

**DISINFORMATION NATION: SOCIAL MEDIA'S ROLE
IN PROMOTING EXTREMISM AND MISINFORMA-
TION**

VIRTUAL JOINT HEARING
BEFORE THE
SUBCOMMITTEE ON COMMUNICATIONS AND
TECHNOLOGY
AND THE
SUBCOMMITTEE ON CONSUMER PROTECTION AND
COMMERCE
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED SEVENTEENTH CONGRESS
FIRST SESSION

MARCH 25, 2021

Serial No. 117-19



Published for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

DISINFORMATION NATION: SOCIAL MEDIA'S ROLE IN PROMOTING EXTREMISM AND
MISINFORMATION

DISINFORMATION NATION: SOCIAL MEDIA'S ROLE IN PROMOTING EXTREMISM AND MISINFORMA- TION

VIRTUAL JOINT HEARING
BEFORE THE
SUBCOMMITTEE ON COMMUNICATIONS AND
TECHNOLOGY
AND THE
SUBCOMMITTEE ON CONSUMER PROTECTION AND
COMMERCE
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED SEVENTEENTH CONGRESS
FIRST SESSION

MARCH 25, 2021

Serial No. 117-19



Published for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
46-925 PDF
WASHINGTON : 2023

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois	CATHY McMORRIS RODGERS, Washington
ANNA G. ESHOO, California	<i>Ranking Member</i>
DIANA DEGETTE, Colorado	FRED UPTON, Michigan
MIKE DOYLE, Pennsylvania	MICHAEL C. BURGESS, Texas
JAN SCHAKOWSKY, Illinois	STEVE SCALISE, Louisiana
G. K. BUTTERFIELD, North Carolina	ROBERT E. LATTA, Ohio
DORIS O. MATSUI, California	BRETT GUTHRIE, Kentucky
KATHY CASTOR, Florida	DAVID B. MCKINLEY, West Virginia
JOHN P. SARBANES, Maryland	ADAM KINZINGER, Illinois
JERRY MCNERNEY, California	H. MORGAN GRIFFITH, Virginia
PETER WELCH, Vermont	GUS M. BILIRAKIS, Florida
PAUL TONKO, New York	BILL JOHNSON, Ohio
YVETTE D. CLARKE, New York	BILLY LONG, Missouri
KURT SCHRADER, Oregon	LARRY BUCSHON, Indiana
TONY CARDENAS, California	MARKWAYNE MULLIN, Oklahoma
RAUL RUIZ, California	RICHARD HUDSON, North Carolina
SCOTT H. PETERS, California	TIM WALBERG, Michigan
DEBBIE DINGELL, Michigan	EARL L. "BUDDY" CARTER, Georgia
MARC A. VEASEY, Texas	JEFF DUNCAN, South Carolina
ANN M. KUSTER, New Hampshire	GARY J. PALMER, Alabama
ROBIN L. KELLY, Illinois, <i>Vice Chair</i>	NEAL P. DUNN, Florida
NANETTE DIAZ BARRAGAN, California	JOHN R. CURTIS, Utah
A. DONALD McEACHIN, Virginia	DEBBIE LESKO, Arizona
LISA BLUNT ROCHESTER, Delaware	GREG PENCE, Indiana
DARREN SOTO, Florida	DAN CRENSHAW, Texas
TOM O'HALLERAN, Arizona	JOHN JOYCE, Pennsylvania
KATHLEEN M. RICE, New York	KELLY ARMSTRONG, North Dakota
ANGIE CRAIG, Minnesota	
KIM SCHRIER, Washington	
LORI TRAHAN, Massachusetts	
LIZZIE FLETCHER, Texas	

PROFESSIONAL STAFF

JEFFREY C. CARROLL, *Staff Director*
TIFFANY GUARASCIO, *Deputy Staff Director*
NATE HODSON, *Minority Staff Director*

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

MIKE DOYLE, Pennsylvania
Chairman

JERRY McNERNEY, California
YVETTE D. CLARKE, New York
MARC A. VEASEY, Texas
A. DONALD MCEACHIN, Virginia
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona
KATHLEEN M. RICE, New York
ANNA G. ESHOO, California
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California, *Vice Chair*
PETER WELCH, Vermont
KURT SCHRADER, Oregon
TONY CARDENAS, California
ROBIN L. KELLY, Illinois
ANGIE CRAIG, Minnesota
LIZZIE FLETCHER, Texas
FRANK PALLONE, JR., New Jersey (*ex officio*)

ROBERT E. LATTA, Ohio
Ranking Member
STEVE SCALISE, Louisiana
BRETT GUTHRIE, Kentucky
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RICHARD HUDSON, North Carolina
MARKWAYNE MULLIN, Oklahoma
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
JOHN R. CURTIS, Utah
CATHY McMORRIS RODGERS, Washington
(*ex officio*)

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

JAN SCHAKOWSKY, Illinois
Chair

BOBBY L. RUSH, Illinois
KATHY CASTOR, Florida
LORI TRAHAN, Massachusetts
JERRY McNERNEY, California
YVETTE D. CLARKE, New York
TONY CARDENAS, California, *Vice Chair*
DEBBIE DINGELL, Michigan
ROBIN L. KELLY, Illinois
DARREN SOTO, Florida
KATHLEEN M. RICE, New York
ANGIE CRAIG, Minnesota
LIZZIE FLETCHER, Texas
FRANK PALLONE, JR., New Jersey (*ex officio*)

GUS M. BILIRAKIS, Florida
Ranking Member
FRED UPTON, Michigan
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
LARRY BUCSHON, Indiana
NEAL P. DUNN, Florida
GREG PENCE, Indiana
DEBBIE LESKO, Arizona
KELLY ARMSTRONG, North Dakota
CATHY McMORRIS RODGERS, Washington
(*ex officio*)

C O N T E N T S

	Page
Hon. Mike Doyle, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	2
Prepared statement	4
Hon. Robert E. Latta, a Representative in Congress from the State of Ohio, opening statement	5
Prepared statement	6
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement	7
Prepared statement	8
Hon. Gus M. Bilirakis, a Representative in Congress from the State of Florida, opening statement	9
Prepared statement	10
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	11
Prepared statement	13
Hon. Cathy McMorris Rodgers, a Representative in Congress from the State of Washington, opening statement	14
Prepared statement	15
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, prepared statement	129

WITNESSES

Mark Zuckerberg, Founder, Chairman, and Chief Executive Officer, Facebook	17
Prepared statement	19
Answers to submitted questions ¹	28
Sundar Pichai, Chief Executive Officer, Alphabet	30
Prepared statement	30
Answers to submitted questions ¹	41
Jack Dorsey, Chief Executive Officer, Twitter	43
Prepared statement	43
Answers to submitted questions ¹	43

SUBMITTED MATERIAL

Letter of March 25, 2021, from Asian Americans Advancing Justice to Mr. Pallone, et al., submitted by Mr. Doyle	130
Letter of March 25, 2021, from Wade Henderson, Interim President and Chief Executive Officer, and LaShawn Warren, Executive Vice President for Government Affairs, Leadership Conference on Civil and Human Rights, to Mr. Doyle, et al., submitted by Mr. Doyle	136
Letter of March 25, 2021, from Koustubh “K.J.” Bagchi, Senior Policy Counsel, and Spandana Singh, Policy Analyst, Open Technology Institute, and reports, “Protecting the Vote How Internet Platforms Are Addressing Election and Voter Suppression-Related Misinformation and Disinformation,” September 2020, and “How Internet Platforms Are Combating Disinformation and Misinformation in the Age of COVID-19,” June 2020, to Mr. Doyle, et al., submitted by Mr. Doyle ²	

¹The witnesses' answers to submitted questions for the record have been retained in committee files and are available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=111407>.

²The information has been retained in committee files and is available at <https://docs.house.gov/meetings/IF/IF16/20210325/111407/HHRG-117-IF16-20210325-SD005.pdf>.

Letter of March 3, 2021, from Donna N. Burns, President, NY Small Farms Ltd., to Mr. Pallone, et al., and report, "Creating Opportunity and Justice with Regenerative Cannabis: A Challenge to New York," December 2020, submitted by Mr. Doyle ³	
Statement of Alphabet Workers Union, March 25, 2021, submitted by Mr. Doyle	143
Letters from David J. Johns, Executive Director, National Black Justice Coalition, to Mr. Doyle, et al., submitted by Mr. Doyle	146
Letter of March 22, 2021, from Gurpatwant Singh Pannun, Legal Advisor, Sikhs for Justice, to Mr. Pallone and Mrs. Rodgers, submitted by Mr. Doyle	150
Letters of March 24, 2021, from William Tong, Attorney General of Connecticut, to Mr. Pallone, et al., and to Jack Dorsey, Chief Executive Officer, Twitter, Inc., and Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook, Inc., submitted by Mr. Doyle	152
Letter of March 24, 2021, from Arthur D. Sidney, Vice President of Public Policy, Computer & Communications Industry Association, to Mr. Doyle, et al., submitted by Mr. Latta	160
Report, "Facebook, From Election to Insurrection: How Facebook Failed Voters and Nearly Set Democracy Aflame," AVAAZ, submitted by Mr. Doyle ³	
Article of March 24, 2021, "Why Section 230 Isn't Really a Good Samaritan Provision," by Neil Fried, DigitalFrontiers Advocacy, submitted by Mr. Latta	163
Letter of March 25, 2021, from American Association of Independent Music, et al., to Mr. Pallone, et al., submitted by Mr. Doyle	168
Letter of March 25, 2021, from Disinfo Defense League to Mr. Pallone, et al., submitted by Mr. Doyle	172
Letter of March 25, 2021, from Laurel Lehman, Policy Analyst, Consumer Reports, et al., to Mr. Doyle, et al., submitted by Mr. Latta	176
Report, "The Disinformation Dozen: Why Platforms Must Act on Twelve Leading Online Anti-Vaxxers," Center for Countering Digital Hate, submitted by Mr. Doyle ³	
Letter of March 25, 2021, from the Coalition for a Secure and Transparent Internet to Mr. Doyle, et al., submitted by Mr. Doyle	184
Statement of the Sikh American Legal Defense and Education Fund, by Kiran Kaur Gill, Executive Director, March 25, 2021, submitted by Mr. Doyle	192
Letter of March 24, 2021, from Meenakshi Bewtra, et al., to Mr. Pallone, et al., submitted by Mr. Doyle	204
Letter of January 21, 2021, from Ms. Eshoo, et al., to Sundar Pichai, Chief Executive Officer, Google, LLC, and Susan Wojcicki, Chief Executive Officer, YouTube, Inc., submitted by Mr. Doyle	206
Letter of January 21, 2021, from Ms. Eshoo, et al., to Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook, Inc., submitted by Mr. Doyle	209
Letter of January 21, 2021, from Ms. Eshoo, et al., to Jack Dorsey, Chief Executive Officer and Founder, Twitter, Inc., submitted by Mr. Doyle	212
Study, "A longitudinal analysis of YouTube's promotion of conspiracy videos," by Marc Faddoul, et al., March 6, 2020, submitted by Mr. Latta	216
Letter of March 18, 2021, from John B. Hertig, President, Board of Directors, Alliance for Safe Online Pharmacies Global, to Mrs. Rodgers, submitted by Mr. Latta	224
Statement of the Technology and Social Change Team, Harvard Shorenstein Center, by Joan Donovan, et al., February 15, 2021, submitted by Mr. Latta	231

³The information has been retained in committee files and is available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=111407>.

	Page
Article of May 26, 2020, “Facebook Executives Shut Down Efforts to Make the Site Less Divisive,” by Jeff Horwitz and Deepa Seetharaman, Wall Street Journal, submitted by Mr. Kinzinger	246
Article of March 17, 2021, “FBI: Surge in Internet Crime Cost Americans \$4.2 Billion,” by Masood Farivar, VOA News, submitted by Mr. Latta	256
Report of the Global Research Project, National Center for Missing & Exploited Children, “A Global Landscape of Hotlines Combating Child Sexual Abuse Material on the Internet and an Assessment of Shared Challenges,” submitted by Mr. Latta ³	
Article of June 11, 2020, “Google Is Not Cracking Down on the Most Dangerous Drug in America,” by Dr. Hany Farid and Mathea Falco, Newsweek, submitted by Mr. Latta	260
Article of March 11, 2021, “How Facebook got addicted to spreading misinformation,” by Karen Hao, MIT Technology Review, submitted by Mr. Latta ³	
Article of October 24 2017, “Bill Gates and Steve Jobs Raised Their Kids Tech-Free—And It Should’ve Been a Red Flag,” by Chris Weller, The Independent, submitted by Mr. Latta	267
Article of February 12, 2021, “Inside the Making of Facebook’s Supreme Court,” by Kate Klonick, The New Yorker, submitted by Mr. Latta	271
Statement of the Coalition for a Safer Web, “Proposal for a Social Media Standards Board,” submitted by Mr. Latta	282
Article of February 7, 2020, “Tech Companies Detect a Surge in Online Videos of Child Sexual Abuse,” by Gabriel J.X. Dance and Michael H. Keller, The New York Times, submitted by Mr. Latta	290
Article of October 5, 2020, “Thank you for posting: Smoking’s lessons for regulating social media,” by Joan Donovan, MIT Technology Review, submitted by Mr. Latta	293
Article of January 2021, “Who Is in Control? The Need to Rein in Big Tech,” by Allum Bokhari, Breitbart News, submitted by Mr. Latta	298
Article of December 2019, “The Dark Psychology of Social Networks,” by Jonathan Haidt and Tobias Rose-Stockwell, The Atlantic, submitted by Mr. Latta	306
Article of June 23, 2020, “Square, Jack Dorsey’s Pay Service, Is Withholding Money Merchants Say They Need,” by Nathaniel Popper, The New York Times, submitted by Mr. Latta	317
Letter of March 24, 2021, from Lauren Culbertson, Head of U.S. Public Policy, Twitter, to Mrs. Rodgers, submitted by Mr. Latta	320
Letter of March 24, 2021, from Mark Isakowitz, Vice President, Government Affairs and Public Policy, Google, to Mrs. Rodgers, et al., submitted by Mr. Latta	329
Letter of March 24, 2021, from Facebook, Inc., to Mrs. Rodgers, submitted by Mr. Latta	339
Article of December 10, 2016, “Twitter says no to law enforcement protest policing tool,” by T. Seppala, engadget.com, submitted by Mr. Latta	348
Letter of March 24, 2021, from Anti-Defamation League, et al., to Mr. Pallone and Mrs. Rodgers, submitted by Mr. Cárdenas	350
Charts, youth suicide trends, submitted by Ms. Castor	
Report of the House Committee on Veterans’ Affairs, “Hijacking Our Heroes: Exploiting Veterans Through Disinformation on Social Media,” submitted by Miss Rice ³	354

³The information has been retained in committee files and is available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=111407>.

DISINFORMATION NATION: SOCIAL MEDIA'S ROLE IN PROMOTING EXTREMISM AND MIS- INFORMATION

THURSDAY, MARCH 25, 2021

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY
JOINT WITH THE
SUBCOMMITTEE ON CONSUMER PROTECTION AND
COMMERCE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittees met, pursuant to notice, at 12:01 p.m., via Cisco Webex online video conferencing, Hon. Michael F. Doyle (chairman of the Subcommittee on Communications and Technology) presiding.

Members present: Representatives Doyle, Schakowsky, Rush, Eshoo, Butterfield, Matsui, Castor, McNearney, Welch, Clarke, Schrader, Cárdenas, Dingell, Veasey, Kelly, McEachin, Soto, O'Halleran, Rice, Craig, Trahan, Pallone (ex officio), Latta (Subcommittee on Communications and Technology ranking member), Bilirakis (Subcommittee on Consumer Protection and Commerce ranking member), Upton, Scalise, Guthrie, Kinzinger, Johnson, Long, Bucshon, Mullin, Hudson, Walberg, Carter, Duncan, Dunn, Curtis, Lesko, Pence, Armstrong, and Rodgers (ex officio).

Also present: Representatives Tonko, Blunt Rochester, Schrier, Burgess, McKinley, Griffith, Crenshaw, and Joyce.

Staff present: AJ Brown, Counsel; Jeffrey C. Carroll, Staff Director; Parul Desai, FCC Detailee; Jennifer Epperson, Counsel; Lisa Goldman, Senior Counsel; Waverly Gordon, General Counsel; Daniel Greene, Professional Staff Member; Tiffany Guarascio, Deputy Staff Director; Perry Hamilton, Clerk; Alex Hoehn-Saric, Chief Counsel, Communications and Consumer Protection; Ed Kaczmarek, Policy Analyst; Zach Kahan, Deputy Director, Outreach and Member Service; Jerry Leverich, Senior Counsel; Dan Miller, Professional Staff Member; David Miller, Counsel; Phil Murphy, Policy Coordinator; Joe Orlando, Policy Analyst; Kaitlyn Peel, Digital Director; Tim Robinson, Chief Counsel; Chloe Rodriguez, Clerk; Andrew Souvall, Director of Communications, Outreach and Member Services; Sydney Terry, Policy Coordinator; Anna Yu, Professional Staff Member; Michael Cameron, Minority Policy Analyst, Consumer Protection and Commerce, Energy, Environment; Nate Hodson, Minority Staff Director; Peter Kiely, Minority General Counsel; Bijan Koohmariae, Minority Chief Counsel;

Tim Kurth, Minority Chief Counsel, Consumer Protection and Commerce; Kate O'Connor, Minority Chief Counsel, Communications and Technology; and Michael Taggart, Minority Policy Director.

Mr. DOYLE. The Subcommittee on Communications and Technology and Subcommittee on Consumer Protection and Commerce will now come to order. Today we will be holding a joint hearing entitled "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation."

Due to the COVID-19 public health emergency, today's hearing is being held remotely. All Members and witnesses will be participating via videoconferencing. As part of our hearing, microphones will be set on mute for the purpose of eliminating inadvertent background noise.

Members and witnesses, you will need to unmute your microphones each time you wish to speak. Additionally, Members will need to be visible on screen in order to be recognized.

Due to the anticipated length of this hearing, the committee will take a 15-minute recess around 3 o'clock to provide witnesses and Members a restroom break.

Finally, documents for the record can be sent to Ed Kaczmarski and Joe Orlando at the email addresses we have provided to your staff. All documents will be entered into the record at the conclusion of the hearing.

The Chair will now recognize himself for 5 minutes.

OPENING STATEMENT OF HON. MIKE DOYLE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Our Nation is drowning in disinformation driven by social media. Platforms that were once used to share photos of kids with grandparents are all too often havens of hate, harassment, and division. The way I see it, there are two faces to each of your platforms.

Facebook has Family and Friends Neighborhood, but it is right next to the one where there is a White nationalist rally every day. YouTube is a place where people share quirky videos, but down the street antivaxxers, COVID deniers, QAnon supporters, and Flat Earthers are sharing videos. Twitter allows you to bring friends and celebrities into your home, but also Holocaust deniers, terrorists, and worse.

Now, it would be one thing if every user chose where to go organically, but almost everything is scripted on social media platforms. Facebook recognizes antisocial tendencies in one user and invites them to visit the White nationalists. YouTube sees another user is interested in COVID-19 and autostarts an antivax video. On Twitter, a user follows the trending conversation never knowing it is driven by bots and coordinated disinformation networks run by foreign agents.

Your platforms have changed how people across the planet communicate, connect, learn, and stay informed. The power of this technology is awesome and terrifying, and each of you has failed to protect your users and the world from the worst consequence of your creations.

This is the first time the three of you have appeared before Congress since the deadly attack on the Capitol on January 6th. That event was not just an attack on our democracy and our electoral process, but an attack on every Member of this committee and in the Congress.

Many of us were on the House floor and in the Capitol when that attack occurred, and we were forced to stop our work of certifying the election and retreat to safety, some of us wearing gas masks and fearing for our lives. We fled as a mob desecrated the Capitol, the House floor, and our democratic process. People died that day, and hundreds were seriously injured.

That attack, and the movement that motivated it, started and was nourished on your platforms. Your platforms suggested groups for people to join, videos they should view, and posts they should like, driving this movement forward with terrifying speed and efficiency.

FBI documents show that many of these individuals used your platforms to plan, recruit, and execute this attack. According to independent research, users on Facebook were exposed 1.1 billion times to misinformation related to the election last year alone despite changes to your policies and claims that you have removed election misinformation.

Our Nation is in the middle of a terrible pandemic. Nearly 550,000 Americans have lost their lives to this deadly disease, more than any other country on the planet. And an independent study found that on Facebook alone, that users across five countries, including the United States, were exposed to COVID disinformation an estimated 3.8 billion times, again despite claims of fixes and reforms.

And now, as the Biden administration is working to implement the American Rescue Plan and get vaccines in people's arms, we are faced with waves of disinformation on social media about the safety and efficacy of these shots. These vaccines are the best chance we have to fight this virus, and the content that your websites are still promoting, still recommending, and still sharing is one of the biggest reasons people are refusing the vaccine.

And things haven't changed. My staff found content on YouTube telling people not to get vaccines, and was recommended to similar videos. The same was true on Instagram, where it was not only easy to find vaccine disinformation, but platforms recommended similar post. The same thing happened on Facebook, except they also had antivax groups to suggest as well. And Twitter was no different. If you go to any of these superspreader accounts that remain up despite the policies meant to curb this antivax content, you will see this content.

Now, understand this. You can take this content down. You can reduce division. You can fix this. But you choose not to. We saw your platforms remove ISIS terrorist content. We saw you tamp down on COVID misinformation at the beginning of the pandemic. And we have seen disinformation drop when you have promoted reliable news sources and removed serial disinformation superspreaders from your platform. You have the means.

But time after time, you are picking engagement and profit over the health and safety of your users, our Nation, and our democracy.

These are serious issues, and to be honest, it seems like you all just shrug off billion-dollar fines. Your companies need to be held accountable. We need rules, regulations, technical experts in government, and audit authority of your technologies. Ours is the committee of jurisdiction, and we will legislate to stop this. The stakes are simply too high.

[The prepared statement of Mr. Doyle follows:]

PREPARED STATEMENT OF HON. MIKE DOYLE

Our Nation is drowning in disinformation driven by social media. Platforms that were once used to share photos of kids with grandparents are all too often havens of hate, harassment, and division.

The way I see it, there are two faces to each of your platforms. Facebook has the family and friends neighborhood but it is right next to the one where there is a White nationalist rally every day.

YouTube is a place where people share quirky videos, but down the street, antivaxxers, COVID deniers, QAnon supporters, and flat earthers are sharing videos. Twitter allows you to bring friends and celebrities into your home, but also Holocaust deniers, terrorists and worse.

Now, it would be one thing if every user chose where to go organically, but almost everything is scripted on social media platforms. Facebook recognizes antisocial tendencies in one user and invites them to visit the White nationalists.

YouTube sees another user is interested in COVID-19 and autostarts an antivax video. On Twitter a user following the trending conversation, never knowing it is driven by bots and coordinated disinformation networks run by foreign agents.

Your platforms have changed how people across the planet—communicate, connect, learn, and stay informed.

The power of this technology is awesome and terrifying—and each of you has failed to protect your users and the world from the worst consequences of your creations.

This is the first time the three of you have appeared before Congress since the deadly attack on the Capitol on January 6th. That event was not just an attack on our Democracy and our electoral process, but an attack on every member of this committee and in the Congress.

Many of us were on the House floor and in the Capitol when that attack occurred and we were forced to stop our work of certifying the election—and retreat to safety—some of us wearing gas masks and fearing for our lives.

We fled as a mob desecrated the Capitol, the House floor, and our democratic process. People died that day, and hundreds were seriously injured.

That attack and the movement that motivated it started and was nourished on your platforms. Your platforms suggested groups for people to join, videos they should view, and posts they should like—driving this movement forward with terrifying speed and efficiency.

FBI documents show that many of these individuals used your platforms to plan, recruit, and execute this attack.

According to independent research, users on Facebook were exposed 1.1 billion times to misinformation related to the election last year alone—despite changes to your policies and claims that you removed election misinformation.

Our Nation is in the middle of a terrible pandemic. Nearly five hundred and fifty thousand Americans have lost their lives to this deadly disease—more than any other country on the planet. An independent study found that on Facebook alone, users across five countries, including the United States, were exposed to COVID disinformation an estimated 3.8 billion times—again despite claims of fixes and reforms.

And now as the Biden administration is working to implement the American Rescue Plan and get vaccines in people's arms, we are faced with waves of disinformation on social media about the safety and efficacy of these shots.

These vaccines are the best chance we have to fight this virus, and the content that your websites are still promoting, still recommending, and still sharing—is one of the biggest reasons people are refusing the vaccine.

And things haven't changed—my staff found content on YouTube telling people not to get vaccines and was recommended similar videos.

The same was true on Instagram, where it was not only easy to find vaccine disinformation—but the platform recommended similar posts. The same thing happened on Facebook except they also had antivax groups to suggest as well.

Twitter was no different, if you go to any of the super spreader accounts that remain up despite policies meant to curb antivax content, you'll see this content.

You **can** take down this content, you **can** reduce division, you **can** fix this—but you choose not to.

We saw your platforms remove ISIS terrorist content; we saw you tamp down on COVID misinformation at the beginning of the pandemic; we have seen disinformation drop when you have promoted reliable news sources and removed serial disinformation super spreaders from your platforms.

You have the means, but time after time, you are picking engagement and profit over the health and safety of your users, our Nation, and our democracy.

These are serious issues, and to be honest—it seems like you all just shrug off billion-dollar fines. Your companies need to be held accountable—we need rules, regulations, technical experts in government, and audit authority of your technologies. Ours is the committee of jurisdiction, and we will legislate to stop this. The stakes are simply too high.

Mr. DOYLE. The Chair will now recognize Mr. Latta, ranking member of the Subcommittee on Communications and Technology, for 5 minutes for his opening statement.

**OPENING STATEMENT OF HON. ROBERT E. LATTA, A
REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO**

Mr. LATTA. Well, I thank the chairman for recognizing me. And I want to thank our witnesses for being with us today, for a conversation that is long overdue in the Energy and Commerce Committee. I am deeply concerned by your decisions to operate your companies in a vague and biased manner, with little to no accountability while using Section 230 as a shield for your actions and their real-world consequences.

Your companies have the power to silence the President of the United States, shut off legitimate journalism in Australia, shut down legitimate scientific debate on a variety of issues, dictate which articles or websites are seen by Americans when they search the internet. When these actions are taken, users have little to no recourse to appeal the decision—if they are aware of your actions. In most cases, we simply don't know.

What does this mean for everyday Americans? We are all aware of Big Tech's ever-increasing censorship of deserving voices and their commitment to serve the radical progressive agenda by influencing a generation of children, who are moving, shutting down, or canceling any news, books, and even now toys, that aren't considered woke. This is fundamentally un-American.

At a recent hearing on disinformation and extremism online, Professor Turley, one of the Nation's foremost experts on constitutional law, testified about the "Little Brother Problem," a problem which private entities do for the government which it cannot legally do for itself.

As of January of this year, Google has a greater than 92 market share in search. Facebook has over 2.7 billion monthly users. And Twitter has 187 million daily users. Your companies have enormous control over whose ideas are seen, read, or heard around the world. This gives you great power. And if misused, as we have seen in recent years, your actions have a ripple effect throughout the world that result in American voices being removed from the marketplace of ideas.

While the Little Brother Problem of censorship is frightening enough, other serious harms are occurring on these platforms that

affect ordinary Americans. Young American children and teenagers are addicted—actually addicted—to their devices and social media. This problem has been exacerbated by the pandemic and will only get worse if children continue to be separated from their peers and cannot learn from their teachers in a classroom.

Your platforms are purposely designed to keep our children hooked to their screens. The use of social media has been linked to increased rates of depression, mental illness, cyberbullying, and suicide among America's youth. Illegal drugs continue to be sold online despite your previous commitment to solve these issues.

Mr. Chairman, I do ask unanimous consent to submit a letter from the National Association of Boards of Pharmacy for the record.

Mr. DOYLE. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. LATTA. Thank you very much.

Serious problems continue to persist, and I wonder how much you are truly dedicating to combating these actions. What actions are you taking to educate Americans about the dangers of using your site, especially the dangers for kids?

As ranking member of the Subcommittee on Communications and Technology, we have oversight of any change made to Section 230 of the Communications Decency Act. Section 230 provides you with liability protection for content moderation decisions made in good faith. Based on recent actions, however, it is clear that in your definition of good faith, moderation includes censoring viewpoints you disagree with and establishing a faux independent appeals process that doesn't make its content moderation decisions based on American principles of free expression. I find that highly concerning.

I look forward to today's hearing as an important step in reconsidering the extent to which Big Tech deserves to retain the significant liability protection. And with that, Mr. Chairman, I yield back the balance of my time.

[The prepared statement of Mr. Latta follows:]

PREPARED STATEMENT OF HON. ROBERT E. LATTA

Good morning to our witnesses, and welcome to this long overdue conversation with the Energy and Commerce Committee.

I am deeply concerned by your decisions to operate your companies in a vague and biased manner, with little to no accountability, while using Section 230 as a shield for your actions and their real-world consequences.

Your companies have the power to silence the President of the United States, shut off legitimate journalism in Australia, shut down legitimate scientific debate on a variety of issues, and dictate which articles or websites are seen by Americans when they search the Internet. When these actions are taken, users have little to no recourse to appeal the decision—if they are aware of your actions. In most cases, we simply do not know.

What does this mean for everyday Americans?

We are all well aware of Big Tech's ever increasing censorship of conservative voices and their commitment to serve the radical progressive agenda by influencing a generation of children and removing, shutting down, or canceling any news, books, and, now, even toys that aren't considered "woke." This is fundamentally un-American.

At a recent hearing on disinformation and extremism online, Professor Turley, one of the Nation's foremost experts on constitutional law, testified about "the little brother problem"—a problem in which private entities do for the Government what

it cannot legally do for itself. As of January of this year, Google has greater than 92% market share in search, Facebook has over 2.7 billion monthly users, and Twitter has over 187 million daily users.

Your companies have enormous control over whose ideas are seen, read, or heard around the world. This gives you great power—and if misused, as we have seen in the recent years, your actions have ripple effects throughout the world that result in American voices being removed from the marketplace of ideas.

While the little brother problem of censorship is frightening enough, other serious harms are occurring on these platforms that affect ordinary Americans.

Young American children and teenagers are addicted, actually addicted, to their devices and social media. This problem has been exacerbated by the pandemic and will only get worse if children continue to be separated from their peers and cannot learn from their teachers in a classroom.

Your platforms are purposely designed to keep our children hooked to their screens. The use of social media has been linked to increased rates of depression, mental illness, cyberbullying, and suicide among America's youth. Illegal drugs continue to be sold online despite your previous commitments to solve these issues [Mr. Chairman, I would like to submit a letter from the National Association Boards of Pharmacy for the record]. Serious problems continue to persist, and I wonder how much you are truly dedicating to combating these actions.

What actions are you taking to educate Americans about the dangers of using your site? Especially the dangers for our kids?

As ranking member on the Subcommittee for Communications and Technology, we have oversight over any change made to Section 230 of the Communications Decency Act. Section 230 provides you with liability protection for content moderation decisions made in "good faith." Based on recent actions, however, it is clear that your definition of "good faith" moderation includes censoring viewpoints you disagree with and establishing a faux independent appeals process that does not make its content moderation decisions based on American principles of free expression. I find that highly concerning.

I look at today's hearing as an important step in reconsidering the extent to which Big Tech deserves to retain their significant liability protection.

I yield back.

Mr. DOYLE. Thank you. The gentleman yields back.

The Chair now recognizes Chair Schakowsky, chair of the Subcommittee on Consumer Protection and Commerce, for 5 minutes for her opening statement.

OPENING STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you. It is a pleasure to cochair this meeting with you.

I want to welcome our witnesses and thank them for coming. It is not an exaggeration to say that your companies have fundamentally and permanently transformed our very culture and our understanding of the world. Much of this is for good, but it is also true that our country, our democracy, even our understanding of what is truth has been harmed by the proliferation and dissemination of misinformation and extremism, all of which has deeply divided us.

What our witnesses today need to take away from this hearing is that self-regulation has come to the end of its road, and that this democracy, this democratic—the people that you see before you, elected by the people, is preparing to move forth with legislation and regulation.

The regulation that we seek should not attempt to limit constitutionally protected freedom of speech, but it must hold platforms accountable when they are used to incite violence and hatred or, as in the case of the COVID pandemic, spread misinformation that costs thousands of lives.

All three of the companies that are here today run platforms that are hotbeds of misinformation and disinformation. And despite all the promises and new policies to match, disinformation was rampant in the 2020 election, especially targeting vulnerable communities. For example, Spanish language ads run by the Trump campaign falsely accused President Biden of being endorsed by Venezuelan President Maduro.

The spread of disinformation fed upon itself until it arrived at the Capitol of the United States on January 6th, which cost five lives. The lives lost in the insurgency were not the first cases of these platforms' failure, nor even the worst. In 2018, Facebook admitted a genocide of the Rohingya people in Myanmar was planned and executed on Facebook.

2020 saw the rise of coronavirus disinformation on Facebook platforms, including the playing of the—they called it “The Plandemic.” This film got 1.8 million views and 150,000 shares before it was removed. Disinformation like “Plandemic” made people skeptical of the need for vaccines and almost certainly cost—contributed to the horrible loss of life during the pandemic. Disinformation also hops platforms to spread viruses. Disinformation also hops from platform to platform. “The Plandemic” actually was first on YouTube before it was on Facebook and Instagram and Twitter.

Misinformation regarding the election dropped 73 percent across social media platforms after Twitter permanently suspended Trump as well as—and also the Capitol insurgency and QAnon.

But the question really is: What took so long? The witnesses here today have demonstrated time and time again that they do not—that self-regulation has not worked. They must be held accountable for allowing disinformation and misinformation to spread. And that is why I will be introducing the Online Consumer Protection Act, which I hope will earn bipartisan support. And thank you. I will yield back.

[The prepared statement of Ms. Schakowsky follows:]

PREPARED STATEMENT OF HON. JAN SCHAKOWSKY

I want to welcome our witnesses and thank them for coming. It is not an exaggeration to say that your companies have fundamentally and permanently transformed our very culture; and our understand of the world.

Much of this is for the good, but it is also true that our country, our democracy, even our understanding of what is truth, has been harmed by the proliferation of disinformation, misinformation, and extremism, all of which has deeply divided us.

What our witnesses need to take away from this hearing is that self-regulation has come to the end of its road, and that this democratically elected body is prepared to move forward with legislation and regulation.

The regulation we seek should not attempt to limit constitutionally protected free speech, but it must hold platforms accountable when they are used to incite violence and hatred—or as in the case of the Covid pandemic—spread misinformation that costs thousands of lives.

All three companies here today run platforms that are hotbeds of misinformation and disinformation.

Despite all the promises and new policies to match, disinformation was rampant in the 2020 election—especially targeting vulnerable communities.

For example, Spanish language ads run by the Trump campaign falsely claimed President Biden was endorsed by Venezuelan President Maduro. The spread of disinformation fed upon itself until it came to a head in the historic assault on our Capitol and our democracy on January 6th, which cost 5 lives.

The lives lost to the Insurrection were not the first casualties of these platforms' failures, nor are they the worst. In 2018, Facebook admitted a genocide of the Rohingya people in Myanmar was planned and executed on Facebook.

2020 saw the rise of coronavirus disinformation on Facebook's platforms including the propaganda film "Plandemic." This film got 1.8 million views and 150,000 shares before it was removed by Facebook.

Disinformation like "Plandemic" made people skeptical of the need for vaccines and almost certainly contributed to the horrible loss of life during the pandemic.

Disinformation also hops platforms to spread virally across the internet. "Plandemic" was first posted on YouTube before taking off on Facebook, Instagram, and Twitter.

Misinformation regarding the election dropped by 73% across social media platforms after Twitter permanently suspended Trump as well as accounts tied to the Capitol Insurrection and QAnon. The question is, what took so long?

The witnesses here today have demonstrated time and again that promises to self-regulate don't work. They must be held accountable for allowing disinformation and misinformation to spread across their platforms, infect our public discourse, and threaten our democracy.

That's why I'll be introducing the Online Consumer Protection Act, which I hope will earn bipartisan support.

Thank you, and I yield back.

Mr. DOYLE. The gentlelady yields back.

The Chair now recognizes Mr. Bilirakis, ranking member for the Subcommittee on Consumer Protection and Commerce, for 5 minutes for his opening remarks.

OPENING STATEMENT OF HON. GUS M. BILIRAKIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it. Thank you for participating in today's hearing, all the witnesses and the Members.

I have been thinking about this hearing since our side first requested this hearing last year. My time in college has provided me enough knowledge about the history of the committee to know what the Telecommunications Act was and, importantly, what it wasn't. Components of that law have been struck down by the courts, while other provisions are interpreted and applied differently than first conceived. This is all a departure from congressional intent.

Regardless of what one thinks of whether all of the Communications Decency Act was the right approach, the same members that voted for Section 230 voted for that entire bill. The statute was meant to protect our society, specifically our children.

To our witnesses today, here lies the problem for you: You don't want the Federal Government telling you what parts of your company you are allowed to operate. So imagine things from our perspective when you pick and choose what parts of the law you want to follow.

I really do admire your ingenuity. You have created something truly remarkable, in my opinion. But with that power, you must also be Good Samaritans, and you have an obligation to be stewards of your platform. If your legal department doesn't believe you are bound to the intent of the law, I would hope your moral compasses will.

Many of my colleagues will raise legitimate concerns about the attack on the Capitol from January, and other colleagues can point to what occurred in our cities last summer. These were all inci-

dents where social media escalated tension, incited chaos, and bred extremism through echo chambers and algorithms.

As a new Republican leader, quite an honor, on the commerce protection and commerce committee—so the Consumer Protection and Commerce committee—I have been digging into how your companies operate. That led me to run a survey of my district following our Big Tech hearing announcement. The conclusion is my constituents simply don't trust you anymore.

With thousands of responses, over 82 percent say they do not trust Big Tech to be good stewards of their platforms or consistently enforce their policies. That includes my constituent who told me, "We were providing information to local families on teen suicide risks on Facebook Livestream. It was blocked by Facebook."

Another constituent said she has seen countless teens be bullied online or simply not able to process a devastating comparison game that they are forced to deal with on social media. Others told me they stopped using your services altogether out of fear and distrust. One even told me they quit social media due to treatment from your companies over their families' Christian views.

Each one of these represents a story of how your companies have failed people. And you will be hearing from my colleagues with more of these stories about how Big Tech has lost its way, highlighting a much larger problem. People want to use your services, but they suspect your coders are designing what they think we should see and hear by keeping us online longer than ever, and all with the purpose to polarize or monetize us, disregarding any consequences for the assault on our inherent freedoms which we hold so dearly.

So I don't want to hear about how changing your current law is going to affect startups because I have heard directly from them, accusing you of anticompetitive tactics. None of us want to damage entrepreneurs. What I do want to hear is what you will do to bring our country back from the fringes and stop the poisonous practices that drive depression, isolation, and suicide, and instead cooperate with law enforcement to protect our citizens.

Our kids are being lost while you say you will try to do better, as we have heard countless time already. We need true transparency and real change. We need, again, not empty promises from you, and we have heard that over and over again. The fear you should have coming into this hearing today isn't that you are going to get upbraided by a Member of Congress. It is that our committee knows how to get things done when we come together. We can do this with you or without you. And we will.

Thank you, Mr. Chairman. I yield back.

[The prepared statement of Mr. Bilirakis follows:]

PREPARED STATEMENT OF HON. GUS M. BILIRAKIS

Thank you for participating in today's hearing. I have been thinking about this hearing since our side first requested it last year.

My time in Congress has provided me enough knowledge about the history of this committee to know what the Telecommunications Act was and importantly what it wasn't.

Components of that law have been struck by the courts, while other provisions are interpreted and applied differently than first conceived. This is all a departure from Congressional intent.

Regardless of what one thinks of whether all of the Communications Decency Act was the right approach, the same Members that voted for Section 230 voted for that entire bill—the statute was meant to protect our society, specifically our kids.

To our witnesses today, here lies the problem for you. You don't want the Federal Government telling you what parts of your company you're allowed to operate. Imagine things from our perspective when you pick and choose what parts of the law you want to follow.

I really do admire your ingenuity. You have created something truly remarkable. But with that power you must also be Good Samaritans, and you have an obligation to be stewards of your platform. If your legal department doesn't believe you are bound to the intent of the law, I would hope your souls and consciences will.

Many of my colleagues will raise legitimate concerns about the attack on the Capitol from January, and other colleagues can point to what occurred in our cities last summer. These were all incidents where social media escalated tension, incited chaos, and bred extremism through echo chambers and algorithms.

As the new Republican leader on the Consumer Protection and Commerce subcommittee, I have been digging into how your companies operate. That led me to run a survey of my district following our Big Tech hearing announcement. The conclusion is my constituents simply don't trust you anymore. With thousands of responses, over 82% said they do not trust Big Tech to be good stewards of their platforms or consistently enforce their policies. That includes my constituent who told me "We were providing information to local families on teen suicide risks on Facebook Livestream, and it was blocked by Facebook." Another constituent said she is seeing "countless teens be bullied online or simply not able to process the devastating comparison game that they are forced to deal with on social media." Others told me they stopped using your services all together out of fear and distrust, one even told me they quit social media due to treatment from your companies over their family's Christian views. Each one of these represents a story of how your companies have failed people, and you'll be hearing from my colleagues with more of these stories about how Big Tech has lost its way, highlighting a much larger problem.

People want to use your services, but they suspect your coders are designing what they think we should see and hear, by keeping us online longer than ever, and all with the purpose to polarize and monetize us, disregarding any consequences for the assault on our inherent freedoms.

So I don't want to hear about how changing current law is going to hurt startups, because I've heard directly from them accusing you of anticompetitive tactics. None of us want to damage entrepreneurs.

What I do want to hear is what you will do to bring our country back from the fringes and stop the poisonous practices that drive depression, isolation, and suicide, and instead cooperate with law enforcement to protect our citizens. Our kids are being lost while you say you will "try to do better" as we've heard countless times already. We need true transparency and real change, not empty promises.

The fear you should have coming into this hearing today isn't that you're going to get yelled at by a Member of Congress, it's that our committee knows how to get things done when we come together. We can do this with you or without you. And we will.

Thank you, I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair now recognizes Mr. Pallone, chairman of the full committee, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Chairman Doyle and Schakowsky, for this very important hearing. We are here today because the spread of disinformation and extremism has been growing online, particularly on social media, where there are little to no guardrails in place to stop it.

And unfortunately this disinformation and extremism doesn't just stay online. It has real-world, often dangerous, and even violent consequences. And the time has come to hold online platforms

accountable for their part in the rise of disinformation and extremism.

According to a survey conducted by Pew earlier this month, 30 percent of Americans are still hesitant or simply do not want to take the COVID-19 vaccine. On January 6, our Nation's Capitol was violently attacked. This month, Homeland Security Secretary Mayorkas identified domestic violent extremism as the "greatest threat" to the United States. And crimes against Asian Americans have risen by nearly 150 percent since the beginning of the COVID-19 pandemic.

Five years ago, during the 2016 Presidential elections Facebook, Google, and Twitter were warned about—but simply ignored—their platforms' role in spreading disinformation. And since then the warnings have continued, but the problem has only gotten worse.

Only after public outrage and pressure did these companies make inadequate attempts to appease critics and lawmakers. But despite the public rebuke, Wall Street continued to reward the companies' strategy to promote misinformation and disinformation by driving their stock prices even higher.

And now, despite repeated promises to seriously tackle this crisis, Facebook, Google, and Twitter instead routinely make minor changes to their policies in response to the public relations crisis of the day. And they will change some underlying internal policy that may or may not be related to the problem. But that is it. The underlying problem remains.

So Mr. Chairman, it is now painfully clear that neither the market nor public pressure will force these social media companies to take the aggressive action they need to take to eliminate disinformation and extremism from their platforms. And, therefore, it is time for Congress and this committee to legislate and realign these companies' incentives.

Today our laws give these companies and their leaders a blank check to do nothing. Rather than limit the spread of disinformation, Facebook, Google, and Twitter have created business models that exploit the human brain's preference for divisive content to get Americans hooked on their platform at the expense of the public interest.

It isn't just that social media companies are allowing disinformation to spread—it is that, in many cases, they are actively amplifying and spreading it themselves. And fines, to the extent they are levied at all, have simply become the cost of doing business.

The dirty truth is that they are relying on algorithms to purposefully promote conspiratorial, divisive, or extremist content so they can take more money in ad dollars. And this is because the more outrageous and extremist the content, the more engagement and views these companies get from their users. And more views equal more money, Mr. Chairman. That is what it is all about, more money.

It is crucial to understand that these companies aren't just mere bystanders—they are playing an active role in the meteoric rise of disinformation and extremism because they make money on it. So when a company is actually promoting this harmful content, I question whether existing liability protections should apply.

Members on this committee have suggested legislative solutions and introduced bills. The committee is going to consider all these options so that we can finally align the interests of these companies with the interests of the public and hold the platforms and their CEOs accountable when they stray.

That is why you are here today, Mr. Zuckerberg, Mr. Pichai, and Mr. Dorsey. You have failed to meaningfully change after your platforms played a role in fomenting insurrection, in abetting the spread of the virus, and trampling Americans' civil liberties.

And while it may be true that some bad actors will shout "Fire!" in a crowded theater, by promoting harmful content your platforms are handing them a megaphone to be heard in every theater across the country and the world. Your business model itself has become the problem.

And the time for self-regulation is over. It is time we legislate to hold you accountable. That is what we are going to do. And I want to thank you, Mr. Chairman, Mr. Doyle, and Ms. Schakowsky because I know that you are very serious about moving forward on legislation, which we will do. I promise everyone.

Thank you, and I yield back.
[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

We are here today because the spread of disinformation and extremism has been growing online, particularly on social media, where there are little to no guardrails in place to stop it. And unfortunately, this disinformation and extremism doesn't just stay online. It has real world, often dangerous and even violent consequences. The time has come to hold online platforms accountable for their part in the rise of disinformation and extremism.

According to a survey conducted by Pew earlier this month, 30 percent of Americans are still hesitant or simply do not want to take the COVID-19 vaccine. On January 6, our Nation's Capitol was violently attacked. This month, Homeland Security Secretary Mayorkas identified domestic violent extremism as the "greatest threat" to the United States. And crimes against Asian Americans have risen by nearly 150 percent since the beginning of the COVID-19 pandemic.

Each of these controversies and crimes have been accelerated and amplified on social media platforms through misinformation campaigns, the spread of hate speech, and the proliferation of conspiracy theories.

Five years ago, during the 2016 Presidential elections, Facebook, Google, and Twitter were warned about—but simply ignored—their platforms' role in spreading disinformation. Since then, the warnings have continued, but the problem has only gotten worse. Only after public outrage and pressure, did these companies make inadequate attempts to appease critics and lawmakers. But despite the public rebuke, Wall Street continued to reward the companies' strategy to promote misinformation and disinformation by driving their stock prices even higher.

And now, despite repeated promises to seriously tackle this crisis, Facebook, Google, and Twitter instead routinely make minor changes to their policies in response to the public relations crisis of the day. They will change some underlying internal policy that may or may not be related to the problem. But that's it. The underlying problem remains.

It is now painfully clear that neither the market nor public pressure will force these social media companies to take the aggressive action they need to take to eliminate disinformation and extremism from their platforms. And, therefore, it is time for Congress and this committee to legislate and realign these companies' incentives to effectively deal with disinformation and extremism.

Today, our laws give these companies, and their leaders, a blank check to do nothing. Rather than limit the spread of disinformation, Facebook, Google, and Twitter have created business models that exploit the human brain's preference for divisive content to get Americans hooked on their platform, at the expense of the public interest. It isn't just that social media companies are allowing disinformation to spread—it's that, in many cases, they are actively amplifying and spreading it them-

selves. Fines, to the extent they are levied at all, have simply become the cost of doing business.

The dirty truth is that they are relying on algorithms to purposefully promote conspiratorial, divisive, or extremist content so they can rake in the ad dollars. This is because the more outrageous and extremist the content, the more engagement and views these companies get from their users. More views equal more money.

It's crucial to understand that these companies aren't just mere bystanders—they are playing an active role in the meteoric rise of disinformation and extremism.

So when a company is actually promoting this harmful content, I question whether existing liability protections should apply.

Members on this committee have suggested legislative solutions and introduced bills. The committee is going to consider all these options so that we can finally align the interests of these companies with the interests of the public and hold the platforms, and their CEOs, accountable when they stray.

That is why you are here today, Mr. Zuckerberg, Mr. Pichai, and Mr. Dorsey. You have failed to meaningfully change after your platforms played a role in fomenting insurrection, in abetting the spread of COVID-19, and trampling Americans civil rights.

And while it may be true that some bad actors will shout fire in a crowded theater, by promoting harmful content, your platforms are handing them a megaphone to be heard in every theater across the country and the world. Your business model itself has become the problem.

The time for self-regulation is over. It is time we legislate to hold you accountable. With that, I yield back.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mrs. Rodgers, the ranking member of the full committee, for 5 minutes for her opening statement.

**OPENING STATEMENT OF HON. CATHY McMORRIS RODGERS,
A REPRESENTATIVE IN CONGRESS FROM THE STATE OF
WASHINGTON**

Ms. RODGERS. Thank you, Mr. Chairman.

Ten years ago, when I joined Big Tech platforms, I thought they would be a force for good. I thought that they would help us build relationships and promote transparency in Congress. I can testify today I was wrong. That is not what has transpired. You have broken my trust. Yes, because you failed to promote the battle of ideas and free speech. Yes, because you censor political viewpoints you disagree with. Those polarizing actions matter for democracy.

But do you know what convinced me Big Tech is a destructive force? It is how you have abused your power to manipulate and harm our children. Your platforms are my biggest fear as a parent. I am a mom of three school-aged kids, and my husband and I are fighting the Big Tech battles in our household every day.

It is a battle for their development, a battle for their mental health, and ultimately a battle for their safety. I have monitored your algorithms. I have monitored where your algorithms lead them. It is frightening. And I know that I am not alone.

After multiple teenage suicides in my community, I reached out to our schools and we started asking questions: What is going on with our kids? What is making them feel so alone, so empty and in despair? And this is what I heard over and over again from parents, pediatricians, school administrators, and teachers: They are all raising the alarm about social media.

A day doesn't go by that I don't talk to friends and other parents who tell me their 14-year-old is depressed, she used to love soccer, now they can't get her to do anything, she never gets off her device or leaves her room. I think about a mom who told me she can't

leave her daughter alone—ever—because she harms herself. Or the family who is recovering after almost losing their daughter to a predator she met online.

These stories are not unique to me or eastern Washington. I recently heard of a young college student who has lost nine friends to suicide. This is unimaginable. The science on social media is becoming clear. Between 2011 and 2018, rates of depression, self-harm, suicides, and suicide attempts exploded among American teens.

During that time, rates of teen depression increased more than 60 percent, with a larger increase among young girls. Between 2009 and 2015, emergency room admissions for self-harm among 10-to-14-year-olds tripled. And suicide substantially increased.

One study found during that time teens who use their devices for 5 or more hours a day were 66 percent more likely to have at least 1 suicide-related outcome compared to those who used theirs for just 1. Other studies found that teens who spend more time online report lower psychological well-being and more feelings of loneliness.

Remember, our kids, the users, are the product. You, Big Tech, are not advocates for children. You exploit and profit off of them. Big Tech needs to be exposed and completely transparent for what you are doing to our children so parents like me can make informed decisions. We also expect Big Tech to do more to protect children, because you haven't done enough. Big Tech has failed to be good stewards of your platforms.

I have two daughters and a son with a disability. Let me be clear: I do not want you defining what is true for them. I do not want their future manipulated by your algorithms. I do not want their self-worth defined by the engagement tools you built to attract their attention. I do not want them to be in danger from what you have created. I do not want their emotions and vulnerabilities taken advantage of so you can make more money and have more power.

I am sure most of my colleagues on this committee who are parents and grandparents feel the same way. Over 20 years ago, before we knew what Big Tech would become, Congress gave you liability protections. I want to know: Why do you think you still deserve those protections today? What will it take for your business model to stop harming children? I know I speak for millions of moms when I say we need answers, and we will not rest until we get them.

Thank you.

[The prepared statement of Mrs. Rodgers follows:]

PREPARED STATEMENT OF HON. CATHY McMORRIS RODGERS

Thank you, Mr. Chairman. 10 years ago—when I joined Big Tech platforms—I thought they would be a force for good.

I thought they would help us build relationships and promote transparency in Congress. I can testify today, I was wrong. That is not what has transpired. You've broken my trust. Yes, because you've failed to promote the battle of ideas and free speech.

Yes, because you censor political viewpoints you disagree with. Those polarizing actions matter for democracy. But, do you know what has convinced me Big Tech

is a destructive force? It's how you've abused your power to manipulate and harm our children.

Your platforms are my biggest fear as a parent. I'm a mom of three schoolaged kids. My husband and I are fighting the Big Tech battles in our household every day. It's a battle for their development, A battle for their mental health and—ultimately—a battle for their safety. I've monitored where your algorithms lead them. It's frightening. I know I'm not alone. After multiple teenage suicides in my community, I reached out to our schools and we started asking questions.

What's going on with our kids? What's making them feel so alone? So empty and in despair? This is what I hear over and over again from parents...pediatricians...school administrators...and teachers.

They all are raising the alarm about **social media**. A day doesn't go by that I don't talk to friends and other parents who tell me: Their 14-year-old is depressed. She used to love soccer. Now, they can't get her to do anything. She never gets off her device or leaves her room.

I think about a mom who told me she can't leave her daughter alone **EVER** because she harms herself. Or the family who is recovering from almost losing their daughter to a predator she met online.

These stories are not unique to me or Eastern Washington. I recently heard of a young college student who has lost 9 friends to suicide. This is unimaginable. The science on social media is becoming clearer.

Between 2011 and 2018, rates of depression, self-harm, suicides, and suicide attempts exploded among American teens. During that time, rates of teen depression increased by more than **SIXTY percent**, with the larger increase among young girls.

Between 2009 and 2015, emergency room admissions for self-harm among 10 to 14-year-old girls tripled and suicides substantially increased.

One study found that during that time, teens who used their devices for 5 or more hours a day were 66 percent more likely to have at least one suicide-related outcome compared to those who used their device for just one. Other studies have found that teens who spend more time online report lower psychological well-being and more feelings of loneliness.

Remember our kids—the users—are the product. You—Big Tech—are **not** advocates for children. You exploit and profit off them.

Big Tech needs to be exposed and completely transparent for what you are doing to our children so parents like me can make informed decisions. We also expect Big Tech to do more to protect children because you haven't done enough. Big Tech has failed to be good stewards of your platforms. I have two daughters and a son with a disability.

Let me be clear, I do not want you defining what is true for them. I do not want their future manipulated by your algorithms. I do not want their self-worth defined by the engagement tools you've built to own their attention. I do not want them to be in danger from what you've created. I do not want their emotions and vulnerabilities taken advantage of so you can make more money and have more power.

I'm sure most of my colleagues on this committee—who are also parents and grandparents—feel the same way. Over 20 years ago, before we knew what Big Tech would become, Congress gave you liability protections.

I want to know why do you think you still deserve those protections today? What will it take for your business model to stop harming children? I know I speak for millions of moms when I say we need these answers and we will not rest until we get them.

Thank you.

Mr. DOYLE. I thank the gentlelady. The gentlelady yields back.

The Chair would now like to remind Members that, pursuant to committee rules, all Members' written opening statements shall be made a part of the record.

I would now like to introduce our witnesses for today's hearing and thank them all for appearing today. First we have Mark Zuckerberg, chairman and chief executive officer of Facebook; Sundar Pichai, chief executive officer of Google; and Jack Dorsey, chief executive officer of Twitter.

We want to thank all three of you for joining us today. We look forward to your testimony. Each of you will have 5 minutes to give your opening statements.

Mr. Zuckerberg, we will start with you. You are recognized for 5 minutes.

STATEMENTS OF MARK ZUCKERBERG, FOUNDER, CHAIRMAN, AND CHIEF EXECUTIVE OFFICER, FACEBOOK; SUNDAR PICHAI, CHIEF EXECUTIVE OFFICER, ALPHABET; AND JACK DORSEY, CHIEF EXECUTIVE OFFICER, TWITTER

STATEMENT OF MARK ZUCKERBERG

Mr. ZUCKERBERG. Chairs Pallone, Schakowsky, and Doyle, ranking members Rodgers, Latta, and Bilirakis, and members of the committee, I am glad that this committee is looking at all the ways that misinformation and disinformation show up in our country's discourse.

There are important challenges here for our society. We have to decide how we want to handle speech that is legal but harmful, and who should be responsible for what people say. Misinformation is not a new problem. It was 200 years ago that a congressman said that a lie would travel from Maine to Georgia while truth was still getting on its boots. And disinformation has often been spread through traditional media too.

But the internet gives everyone the power to communicate, and that certainly presents unique challenges. Now, people often say things that aren't verifiably true but that speak to their lived experiences. I think we have to be careful restricting that. For example, if someone feels intimidated or discriminated against while voting, I believe that they should be able to share their experience even if the election overall was fair.

I don't think anyone wants a world where you can only say things that private companies judge to be true, where every text message, email, video, and post has to be fact-checked before you hit send. But at the same time, we also don't want misinformation to spread that undermines confidence in vaccines, stops people from voting, or causes other harms.

At Facebook, we do a lot to fight misinformation. We have removed content that could lead to imminent real-world harm. We have built an unprecedented third-party fact-checking program, and if something is rated false, then we have warning labels and significantly reduce its distribution. We invest a lot in directing billions of people to authoritative information.

The system isn't perfect. But it is the best approach that we have found to address misinformation in line with our country's values. It is not possible to catch every piece of harmful content without infringing on people's freedoms in a way that I don't think that we would be comfortable with as a society.

Our approach was tested in 2020 when we took extraordinary steps during an extraordinary election. We removed voting misinformation; banned hundreds of malicious and conspiracy networks, including QAnon; labeled posts that prematurely or wrongly declared victory; and directed people to official results. We labeled over 180 million posts. We directed 140 million people to our offi-

cial Voting Information Center. And we helped 4½ million people register to vote.

We did our part to secure the integrity of the election. And then, on January 6th, President Trump gave a speech rejecting the results and calling on people to fight. The attack on the Capitol was an outrage, and I want to express my sympathy to all of the Members and Capitol workers who had to live through this disgraceful moment in our history. And I want to express my gratitude to the Capitol police, who were on the front lines in defense of our democracy.

I believe that the former President should be responsible for his words, and that the people who broke the law should be responsible for their actions. So that leaves the question of the broader information ecosystem. And I can't speak for everyone else—the TV channels, radio stations, news outlets, websites, and other apps—but I can tell you what we did.

Before January 6th, we worked with law enforcement to identify and address threats. During and after the attack, we provided extensive support in identifying the insurrectionists and removed posts supporting violence. We didn't catch everything, but we made our services inhospitable to those who might do harm. And when we feared that he would incite further violence, we suspended the former President's account.

Now, many people are concerned that platforms can ban leaders. I am too. I don't think that private companies should make so many decisions like this alone. We need an accountable process, which is why we created an independent oversight board that can overrule our decisions. And we need democratically agreed rules for the internet.

The reality is, our country is deeply divided right now, and that isn't something that tech companies alone can fix. Now, we all have a part to play in helping to turn things around, and I think that starts with taking a hard look at how we got here.

Now, some people say that the problem is that social networks are polarizing us. But that is not at all clear from the evidence or research. Polarization was rising in America long before social networks were even invented. And it is falling or stable in many other countries where social networks are popular. Others claim that algorithms feed us content that makes us angry because it is good for business, but that is not accurate either.

I believe that the division we see today is primarily the result of a political and media environment that drives Americans apart. And we need to reckon with that if we are going to make progress. I know that technology can help bring people together. We see it every day on our platforms.

Facebook is successful because people have a deep desire to connect and share, not to stand apart and fight. And we believe that connectivity and togetherness are more powerful ideals than division and discord, and that technology can be part of the solution to the challenges our society is facing. And we are ready to work with you to move beyond hearings and get started on real reform. Thank you.

[The prepared statement of Mr. Zuckerberg follows:]

**Hearing Before the United States House of Representatives
Committee on Energy and Commerce
Subcommittees on Consumer Protection & Commerce and Communications & Technology**

March 25, 2021
Testimony of Mark Zuckerberg
Facebook, Inc.

I. Introduction

Chairs Pallone, Schakowsky, and Doyle, Ranking Members McMorris Rodgers, Latta, and Bilirakis, and members of the Committee,

I want to start by extending my deepest condolences to the families of the Capitol police officers who lost their lives in the wake of January 6 and my appreciation to the many officers who put themselves at risk to protect you. Their bravery stands as an example to us all. My heart also goes out to those of you who lived through the awful events of that day. The Capitol attack was a horrific assault on our values and our democracy, and Facebook is committed to assisting law enforcement in bringing the insurrectionists to justice.

I look forward to discussing the role that misinformation and disinformation play in our country's information ecosystem and the work Facebook is doing to reduce harmful content on our platform. Facebook's mission is to give people the power to build community and bring the world closer together. Our services enable more than three billion people around the world to stay connected with friends and family, discover what's going on in the world, and entertain and express themselves. We build products people use to share ideas, have fun, offer support, connect with neighbors, celebrate milestones, promote small businesses and non-profits, and discuss important topics, including family, careers, health, politics, and social issues.

It's important to note that the vast majority of what people see on Facebook is neither political nor hateful. Political posts make up only about 6 percent of what people in the United States see in their News Feed, and the prevalence of hateful content people see on our service is less than 0.08 percent. While we work hard to prevent abuse of our platform, conversations online will always reflect the conversations taking place in living rooms, on television, and in text messages and phone calls across the country. Our society is deeply divided, and we see that on our services too.

We are committed to keeping people safe on our services and to protecting free expression, and we work hard to set and enforce policies that meet those goals. We will continue to invest extraordinary resources into content moderation, enforcement, and transparency.

II. Our Efforts to Combat Misinformation

People want to see accurate information on Facebook, and so do we. That's why we have made fighting misinformation and providing people with authoritative information a priority for the company. We have recalibrated our products and built global partnerships to combat misinformation on a massive scale.

We created an industry-leading fact-checking program. We work with 80 independent third-party fact-checkers certified through the non-partisan International Fact-Checking Network to curb misinformation on Facebook and Instagram. If content is rated false by one of these third-party fact-checkers, we put a warning label on it. And based on one fact-check, we're able to kick off similarity detection methods that identify duplicates of debunked stories. When content is rated false, we significantly reduce its distribution; on average, this cuts future views by more than 80 percent. If people do try to share the content, we notify them of additional reporting, and we also notify people if content they have shared in the past is later rated false by a fact-checker. Group admins are notified each time a piece of content rated false by fact-checkers is posted in their Group, and they can see an overview of this in the Group Quality tool. We use information from fact-checkers to improve our technology so we can identify misinformation faster in the future.

We also work to reduce the incentives for people to share misinformation to begin with. Since a lot of the misinformation that spreads online is financially motivated spam, we focus on disrupting the business model behind it. We take action against Pages that repeatedly share or publish content rated false, including reducing their distribution and, if necessary, removing their ability to monetize. And we've enhanced our recidivism policies to make it harder to evade our enforcement. We've also taken steps to reduce clickbait and updated our products so people see fewer posts and ads in News Feed that link to low-quality websites.

As well as taking steps to fight misinformation, we also use our platform to proactively connect people to authoritative information. We have directed over 2 billion people to our Covid-19 Information Center, and over 140 million people to our Voting Information Center. This is an important component of our work to build a healthier information ecosystem.

As one of the leading platforms where people share information and express themselves, misinformation is an ongoing challenge for us. With millions of Americans using our services every day, there will always be things we miss. However, I believe we do more to address misinformation than any other company, and I am proud of the teams and systems we have built.

Below is an overview of this work in two important contexts: Covid-19 and the 2020 presidential election.

A. Covid-19 and Vaccine Misinformation

Since Covid-19 was declared a global public health emergency, Facebook has been working to connect people to authoritative information from health experts and keep harmful misinformation about Covid-19 from spreading on our apps. As part of our efforts, we have focused on:

- Promoting reliable information by launching a Covid-19 Information Center which we showed at the top of the Facebook News Feed and on Instagram, and that we direct people to when they search for information about Covid-19. We have connected over 2 billion people to authoritative information through this resource.
- Combating Covid-19 misinformation by removing over 12 million pieces of false content, including from foreign leaders; barring entities that have repeatedly shared false information;

removing exploitative ads spreading panic about the virus or mistruths about cures for financial gain; and promoting authoritative and science-based search results.

- Providing aggregated data on symptoms and travel patterns to public health officials, researchers, and nonprofits to help them calibrate the public health response.
- Supporting newsgathering by investing \$100 million to assist local news and journalists and funding a \$1 million grant program to support fact-checkers covering the virus.

In April 2020, we started showing messages in News Feed to people who liked, commented on, or reacted to posts with Covid-19 misinformation that we later removed for violating our policy. We've redesigned these notifications to make them more personalized and to more clearly connect people with authoritative information. Now people will see a thumbnail of the post and more information about where they saw it, how they engaged with it, why it was false, and why we removed it. People will then be able to see more facts in our Covid-19 Information Center and take other actions such as unfollowing the Page or Groups that shared this content.

We are also continuing to improve search results on our platforms. When people search for vaccine or Covid-19 related content on Facebook, we promote relevant, authoritative results and provide third-party resources to connect people to expert information about vaccines.

In the Appendix are some of the alerts people see on Facebook that are designed to keep them informed and limit misinformation about Covid-19.

1. Covid-19 Vaccines

In addition to our work to combat misinformation about Covid-19 generally, we're running the largest worldwide campaign to promote authoritative information about Covid-19 vaccines specifically by:

- Providing \$120 million in ad credits to help health ministries, non-profits, and UN agencies reach billions of people around the world with Covid-19 vaccine and preventive health information.
- Providing training and marketing support to help governments and health organizations move quickly and reach the right people with the latest vaccine information.
- Providing data to inform effective vaccine delivery and educational efforts to build trust in Covid-19 vaccines.
- Helping people find where and when they can get vaccinated, similarly to how we helped people find information about voting during elections.

We're also focused on removing misinformation on Facebook and Instagram about Covid-19 and vaccines. In December, we began removing false claims about Covid-19 vaccines that could lead to imminent harm, including false claims about the safety, efficacy, ingredients, or side effects of the vaccines. Last month, we expanded the list of false claims we will remove to include additional debunked claims about Covid-19 and vaccines following consultations with leading health

organizations, including the World Health Organization. We already reject these claims in advertisements and prohibit any ads that discourage vaccines.

Groups, Pages, and accounts on Facebook and Instagram that repeatedly share these debunked claims may be removed altogether. In some instances, we are also requiring Group admins to temporarily approve all posts from other admins or members who have violated our Covid-19 policies. Claims about Covid-19 or vaccines that do not violate these policies may remain eligible for review by our independent third-party fact-checkers. If a claim is then identified as false, it will be labeled and will be demoted in News Feed.

B. Election Misinformation and Support for the Democratic Process

Facebook stands for giving people a voice, and it was important to us that everyone could make their voice heard during the election. While we were only a small piece of the broader election ecosystem, we announced a series of policies in advance to help protect the integrity of the election and support our democratic process.

As part of this effort, we worked hard to combat misinformation and voter suppression. We partnered with election officials to remove false claims about polling conditions and displayed warnings on more than 150 million pieces of content after review by our independent third-party fact-checkers. We put in place strong voter suppression policies prohibiting explicit or implicit misrepresentations about how or when to vote as well as attempts to use threats related to Covid-19 to scare people into not voting. We also removed calls for people to engage in poll watching that used militarized language or suggested that the goal was to intimidate, exert control, or display power over election officials or voters, and we stopped recommending civic Groups.

As the ballots were counted, we deployed additional measures that we announced in advance of the election to help people stay informed:

- We partnered with Reuters and the National Election Pool to provide reliable information about election results in the Voting Information Center and notified people proactively as results became available. We added labels to posts about voting by candidates from both parties and directed people to reliable information about results.
- We attached an informational label to content that sought to delegitimize the outcome of the election or discuss the legitimacy of voting methods.
- We strengthened our enforcement against militias, conspiracy networks, and other groups to help prevent them from using our platform to organize violence or civil unrest in the period after the election.

Based on what we learned in 2016 about the risk of coordinated online efforts by foreign governments and individuals to interfere in our elections, we invested heavily in our security systems and monitored closely for any threats to the integrity of elections from at home or abroad. We invested in combatting influence operations on our platforms, and since 2017, we have found and removed over 100 networks of accounts for engaging in coordinated inauthentic behavior. We

also blocked ads from state-controlled media outlets in the US to provide an extra layer of protection against various types of foreign influence in the public debate ahead of the election.

Finally, we proactively supported civic engagement on our platform. We ran the largest voting information campaign in American history. Based on conversion rates we calculated from a few states we partnered with, we estimate that we helped 4.5 million people register to vote across Facebook, Instagram, and Messenger—and helped about 100,000 people sign up to be poll workers. We launched a Voting Information Center to connect people with reliable information on deadlines for registering and voting and details about how to vote by mail or vote early in person, and we displayed links to the Voting Information Center when people posted about voting on Facebook. 140 million people visited the Voting Information Center on Facebook and Instagram since it launched. We are encouraged that more Americans voted in 2020 than ever before and that our platform helped people take part in the democratic process.

III. Our Efforts to Address Polarization and Divisive Content

Facebook's mission is to bring people together, and we stand firmly against hate and the incitement of violence. We have industry-leading policies that prohibit such content on our platforms, and we invest billions of dollars and work tirelessly to improve and enforce these policies. We are proud of the work we have undertaken to address harmful content on Facebook, from our robust content review and enforcement program to our industry-leading Community Standards Enforcement Report, which includes hard data that we hope can inform public discourse and policymaking about these issues.

A. Efforts to Keep Hate and Violence Off Our Platform

We have taken major steps to keep our community safe. While our enforcement efforts are not perfect and there is always more work to be done, we have built industry-leading policies, teams and systems to keep hate and violence off our platform.

Our Dangerous Organizations and Individuals policy prohibits content calling for or advocating violence, and we ban organizations and individuals that proclaim a violent mission. We remove language that incites or facilitates violence, and we ban Groups that proclaim a hateful and violent mission from having a presence on our apps. We also remove content that represents, praises, or supports them. We believe this policy has long been the broadest and most aggressive in the industry.

In August 2020, we expanded this policy further to address militarized social movements and violence-inducing conspiracy networks such as QAnon. To date, we have banned over 250 white supremacist groups and 890 militarized social movements, and we have been enforcing our rules that prohibit QAnon and militia groups from organizing on our platform. We have also continued to enforce our ban on hate groups, including the Proud Boys and many others.

Moving quickly to find and remove dangerous organizations such as terrorist and hate groups takes significant investment in both people and technology. That's why we have tripled the size of our teams working in safety and security since 2016 to over 35,000 people. Our team of experts includes 300 professionals who work exclusively or primarily on preventing terrorist and violent

content from appearing on our platform and quickly identifying and removing it if it does. These professionals possess expertise ranging from law enforcement and national security to counterterrorism intelligence and radicalization.

Four years ago, we developed automated techniques to detect content related to terrorist organizations such as ISIS, al Qaeda, and their affiliates. We've since expanded these techniques to detect and remove content related to other terrorist and hate groups. We are now able to detect and review text embedded in images and videos, and we've built media-matching technology to find content that's identical or near-identical to photos, videos, text, and audio that we've already removed. Our work on hate groups focused initially on those that posed the greatest threat of violence at the time; we've now expanded this to detect more groups tied to different hate-based and violent extremist ideologies. In addition to building new tools, we've also adapted strategies from our counterterrorism work, such as leveraging off-platform signals to identify dangerous content on Facebook and implementing procedures to audit the accuracy of our AI's decisions over time.

B. Actions to Address Content That Violates Community Standards in Groups

People turn to Facebook Groups to connect with others who share their interests and to build community. This is particularly important in the midst of the Covid-19 crisis, which makes connecting both more important and more challenging than ever. However, we recognize the importance of keeping violent and hateful content out of Groups and have taken significant steps towards that goal.

We remove Groups that represent QAnon, even if they contain no violent content. And we do not allow militarized social movements—such as militias or groups that support and organize violent acts amid protests—to have a presence on our platform. In addition, last year we temporarily stopped recommending US civic or political Groups, and earlier this year we announced that policy would be kept in place and expanded globally. We've instituted a recommendation waiting period for new Groups so that our systems can monitor the quality of the content in the Group before determining whether the Group should be recommended to people. And we limit the number of Group invites a person can send in a single day, which can help reduce the spread of harmful content from violating Groups.

We also take action to prevent people who repeatedly violate our Community Standards from creating new Groups. Our recidivism policy stops the administrators of a previously removed Group from creating another Group similar to the one removed, and an administrator or moderator who has had Groups taken down for policy violations cannot create any new Groups for a period of time. Posts from members who have violated any Community Standards in a Group must be approved by an administrator or moderator for 30 days following the violation. If administrators or moderators repeatedly approve posts that violate our Community Standards, we'll remove the Group.

Our enforcement effort in Groups demonstrates our commitment to keeping content that violates these policies off the platform. In September, we shared that over the previous year we removed about 1.5 million pieces of content in Groups for violating our policies on organized hate, 91 percent of which we found proactively. We also removed about 12 million pieces of content in

Groups for violating our policies on hate speech, 87 percent of which we found proactively. When it comes to Groups themselves, we will remove an entire Group if it repeatedly breaks our rules or if it was set up with the intent to violate our standards. We took down more than one million Groups for violating our policies in that same time period.

IV. Updating the Rules of the Internet

In my testimony above, I laid out many of the steps we have taken to balance important values including safety and free expression in democratic societies. We invest significant time and resources in thinking through these issues, but we also support updated Internet regulation to set the rules of the road. One area that I hope Congress will take on is thoughtful reform of Section 230 of the Communications Decency Act.

Over the past quarter-century, Section 230 has created the conditions for the Internet to thrive, for platforms to empower billions of people to express themselves online, and for the United States to become a global leader in innovation. The principles of Section 230 are as relevant today as they were in 1996, but the Internet has changed dramatically. I believe that Section 230 would benefit from thoughtful changes to make it work better for people, but identifying a way forward is challenging given the chorus of people arguing—sometimes for contradictory reasons—that the law is doing more harm than good.

Although they may have very different reasons for wanting reform, people of all political persuasions want to know that companies are taking responsibility for combatting unlawful content and activity on their platforms. And they want to know that when platforms remove harmful content, they are doing so fairly and transparently.

We believe Congress should consider making platforms' intermediary liability protection for certain types of unlawful content conditional on companies' ability to meet best practices to combat the spread of this content. Instead of being granted immunity, platforms should be required to demonstrate that they have systems in place for identifying unlawful content and removing it. Platforms should not be held liable if a particular piece of content evades its detection—that would be impractical for platforms with billions of posts per day—but they should be required to have adequate systems in place to address unlawful content.

Definitions of an adequate system could be proportionate to platform size and set by a third-party. That body should work to ensure that the practices are fair and clear for companies to understand and implement, and that best practices don't include unrelated issues like encryption or privacy changes that deserve a full debate in their own right.

In addition to concerns about unlawful content, Congress should act to bring more transparency, accountability, and oversight to the processes by which companies make and enforce their rules about content that is harmful but legal. While this approach would not provide a clear answer to where to draw the line on difficult questions of harmful content, it would improve trust in and accountability of the systems and address concerns about the opacity of process and decision-making within companies.

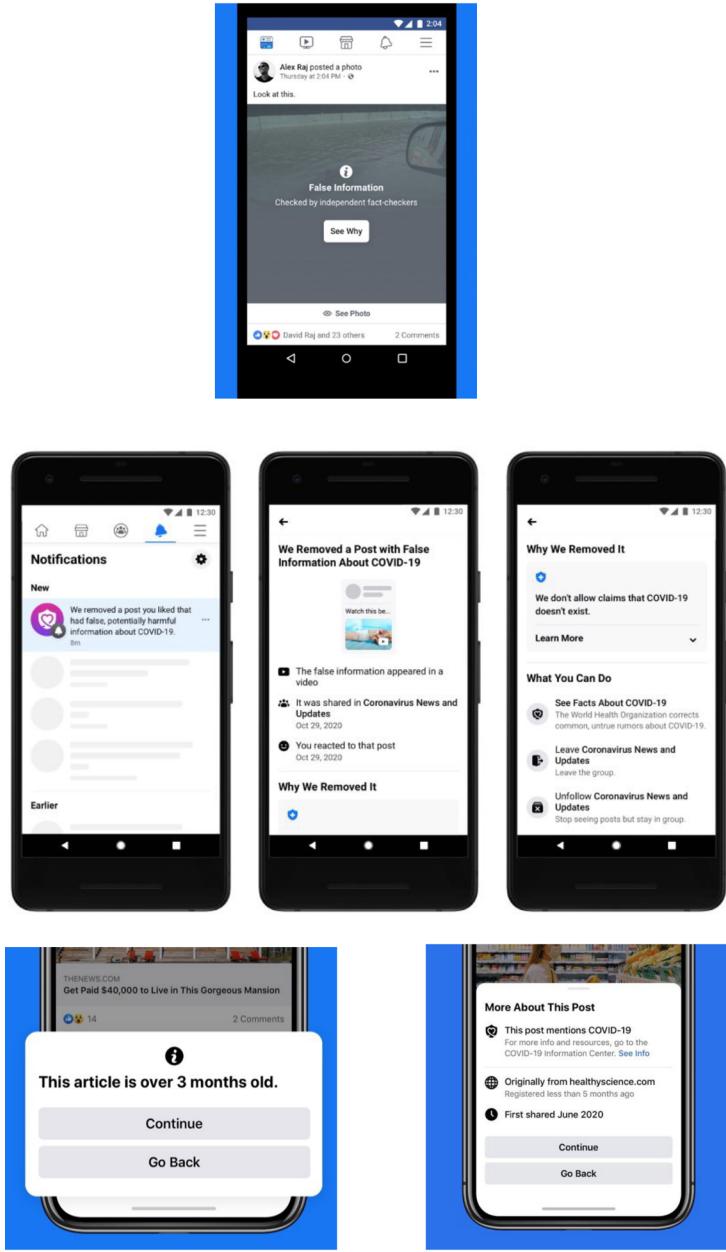
Ultimately it is up to Congress and the new Administration to chart the path forward. Facebook stands ready to be a productive partner in the discussion about Section 230 reform—as well in important and urgent conversations about updating the rules for privacy, elections, and data portability.

V. Conclusion

Every day we see people using our services to come together and do good—forming supportive communities, raising money for good causes, drawing attention to important issues, creating opportunities for themselves, or simply being there for one another in times of need.

Facebook is successful because people around the world have a deep desire to connect and share, not to stand apart and fight. This reaffirms our belief that connectivity and togetherness are ultimately more powerful ideals than division and discord—and that technology can be part of the solution to the deep-seated challenges in our society. We will continue working to ensure our products and policies support this ambition.

APPENDIX: Facebook Efforts to Combat Covid-19 Misinformation



Mr. DOYLE. Thank you, Mr. Zuckerberg.
 Now Mr. Pichai. You are now recognized for 5 minutes.
 Mr. Pichai, are you on mute?
 Mr. PICHAI. Sorry. I had my volume on.

STATEMENT OF SUNDAR PICHAI

Chairman Doyle, Ranking Member Latta, Chairwoman Schakowsky, Ranking Member Bilirakis, full committee Chair Pallone, and full committee Ranking Member McMorris Rodgers, and members of the committee, thank you for the opportunity to appear before you today.

To begin, I want to express my sympathies to those who have lost loved ones to COVID or the recent gun violence in Boulder and Atlanta. In difficult times, we are reminded of what connects us as Americans: the hope that we can make things better for our families and our communities. And we at Google are committed to that work.

I joined Google because I believed the internet was the best way to bring the benefits of technology to more people. Over the past three decades, we have seen how it has inspired the best in society by expanding knowledge, powering businesses, and providing opportunities for discovery and connection.

I am proud that anyone can turn to Google for help, whether they are looking for vaccine information, learning new skills on YouTube, or using digital tools to grow their businesses. In 2020 our products helped 2 million U.S. businesses and publishers generate \$426 billion in economic activity. We are energized by the opportunity to help people at scale and humbled by the responsibility that comes with it.

Thousands of people at Google are focused on everything from cyber attacks to privacy to today's topic, misinformation. Our mission is to organize the world's information and make it universally accessible and useful. The goal to that is providing trustworthy content and opportunities for free expression while combating misinformation.

It is a big challenge without easy answers. Five hundred-plus hours of video are uploaded to YouTube every minute. And approximately 15 percent of Google searches each day are new to us. Eighteen months ago, no one had heard of COVID-19. Sadly, "coronavirus" was the top trending search last year.

Staying ahead of new challenges to keep users safe is a top priority. We saw the importance of that on January 6th, when a mob stormed the U.S. Capitol. Google strongly condemns these violent acts on our democracy and mourns the lives lost.

In response, we raised up authoritative sources across our products. On YouTube, we removed livestreams and videos that violated our Incitement to Violence policies and began issuing strikes to those in violation of our Presidential Elections policy. We removed apps from the Play Store for inciting violence and stopped ads referencing the 2020 election or the Capitol riots as part of our Sensitive Events policy.

We were able to act quickly because we were prepared ahead of the 2020 elections. Our reminders of how to register and vote were

viewed over 2 billion times. YouTube's election results information panels have been viewed more than 8 billion times.

We also worked to keep campaigns safe from cyber attacks and protect platforms from abuse. After the December 8 safe harbor deadline for States to certify elections, we removed content from YouTube that alleged widespread fraud changed the outcome of the election.

This past year, we have also focused on providing quality information during the pandemic. Globally, we have committed over \$550 million in ad grants for COVID-related PSAs to governments, health organizations, and nonprofits. On YouTube, our COVID information panels have been viewed over 400 billion times. We also removed 850,000 videos and blocked nearly 100 million COVID-related ads throughout 2020.

Across all of this work, we strive to have transparent policies and enforce them without regard to politics or point of view. Our ability to provide a range of information and viewpoints while also being able to remove this information is possible only because of legal frameworks like Section 230. It is foundational to the open web, which has been a powerful force for good for so many.

I look forward to sharing more about our approach today and working together to create a path forward for the next three decades. Thank you.

[The prepared statement of Mr. Pichai follows:]

**Written Testimony of Sundar Pichai
Chief Executive Officer, Alphabet**

**United States House Committee on Energy and Commerce
“Disinformation Nation: Social Media’s Role In Promoting Extremism And
Misinformation”
March 25, 2021**

**Chairman Doyle, Ranking Member Latta, Chairwoman Schakowsky, Ranking
Member Bilirakis, Full Committee Chair Pallone and Full Committee Ranking
Member McMorris Rodgers, thank you for the opportunity to appear before you
today.**

This month, the worldwide web turned 32. Over the past three decades, we've seen the web inspire the best in society, by expanding knowledge, powering businesses, and providing opportunities for expression, discovery, and connection—no matter who you are, or where you live.

I joined Google in 2004 because I believed the internet was the best way to bring the benefits of technology to more people, and I believe that still today.

I am proud that Americans can turn to Google for help in moments that matter, whether they're looking for COVID vaccine information on Search and Maps, working and learning from home using Google Workspace or Google Classroom, learning new skills on YouTube, or using our digital tools to grow their businesses. In 2020, our products helped 2 million US businesses, publishers, and others generate \$426 billion

in economic activity. And we helped billions of people find comfort and connection in an otherwise awful year.

Beyond our products, we were proud to announce last week our plans to invest over \$7 billion in data centers and offices across 19 states, and create at least 10,000 full-time Google jobs in the U.S. That's in addition to the 84,000 employees we currently employ across the country. And according to an Oxford Economics report, YouTube's creative ecosystem supported the equivalent of 345,000 full time jobs in 2019.

We are energized by the opportunity to help people at scale, and we are humbled by the responsibility that comes with it. We have thousands of people focused on everything from cyber attacks, to data privacy, to today's topic: misinformation.

Our mission at Google is to organize the world's information and make it universally accessible and useful. Core to that mission is providing trustworthy content and opportunities for free expression across our platforms, while limiting the reach of harmful misinformation.

It's a large, dynamic challenge without easy answers. More than 500 hours of video are uploaded to YouTube every minute, and approximately 15% of the searches on Google each day are new to us. Eighteen months ago most people hadn't heard of COVID-19; sadly, coronavirus was the top trending search of 2020.

Responding to the events of January 6th

Staying ahead of these challenges and keeping users safe and secure on our platforms is a top priority. We saw how high those stakes can be on January 6, 2021, when a mob stormed the U.S. Capitol. This was an unprecedented and tragic event,

and Google strongly condemns these violent attacks on our democracy, and mourns the lives lost.

In response, our teams worked to raise up authoritative news sources across our products. Teams at YouTube quickly took down any live streams or videos that violated our incitement to violence policies, and on January 7th, we began issuing strikes to those in violation of our presidential election integrity policy. In the Play Store, we removed apps for violating our policies on inciting violence. We also prohibited advertisers from running ads that referenced the 2020 election or topics related to the Capitol riots in the scope of our Sensitive Events policy.

Doing our part to contribute to the integrity of the US 2020 election

We were able to act quickly because of the investments we made to prepare for the 2020 elections. Last year, teams across Google and YouTube worked around the clock to contribute to election preparedness, by helping voters find authoritative information about the election; by working with campaigns to equip them with best-in-class security features and helping them connect with voters; and by protecting our platforms from abuse.

Helping voters find authoritative information on our services

This U.S. election cycle saw all-time highs in searches on Google for civics-related topics. Anticipating that need, we worked to launch features that would help people find the information to participate in the democratic process, including how to register and how to vote in their states.

Consistent with our approach to prior election cycles, we showed “how to register” and “how to vote” reminders to all our U.S. users directly on Google Search, Maps and YouTube. These reminders were seen over 2 billion times across our products. As the election neared, we helped people find polling and ballot drop off locations: from

mid-October through Election Day, we added more than 125,000 voting locations in Google Maps. Across our products, these features were seen nearly 500 million times.

Finally, starting on Election Day, we worked with the Associated Press to provide real-time election results for relevant searches on Google. These results had over six times more views in 2020 than in 2016. Similarly, on YouTube, we launched an election results information panel that showed on top of search results and under videos with election-related content. It pointed to our election results page on Google, and over time, we expanded it to include an additional link pointing to a page on the US Cybersecurity and Infrastructure Security Agency (CISA) website that debunked incorrect claims made about the integrity of the elections. Once the safe harbor deadline for state certification passed, we updated this YouTube Election Results Information Panel again to point to the National Archives Office of the Federal Register page of record for the 2020 electoral college vote. Collectively, our election information panels on YouTube have been shown over 8 billion times.

Working with campaigns

We also helped campaigns and elected officials effectively use Google and YouTube products to reach voters and enhance their election security. As part of our Civics Outreach Virtual Training Series, Google held 21 training sessions for over 900 candidates, campaigns, public officials, and nonprofit leaders. Overall, we held 45 group and individual trainings to help more than 2,900 election workers learn to use Google tools to amplify their message and better connect with voters through events like digital town halls, debates and virtual campaign rallies.

In addition, as a part of our Election Cybersecurity Initiative with the University of Southern California's Annenberg School, nearly 4,000 elected officials, secretaries of state, campaign staffers, political party representatives, and state election directors in all 50 states received training on ways to secure their information and protect their

campaigns against cyberattacks.

At the start of the 2020 election season, we partnered with Defending Digital Campaigns (DDC), a nonprofit and nonpartisan organization, to give any eligible federal campaign access to free Titan Security Keys—the strongest form of two-factor authentication. This collaboration is a part of our Advanced Protection Program, which protects high-risk individuals, such as election officials, campaigns, and journalists, who have access to high visibility and sensitive information. In the lead up to the 2020 elections, DDC distributed more than 10,000 Titan Security key bundles to more than 140 U.S. federal campaigns. We recently expanded our support for DDC to provide eligible campaigns and political parties, committees, and related organizations, at both the federal and state levels, with knowledge, training and resources to defend themselves from security threats.

Protecting our platforms from abuse

In the years leading up to the 2020 election, we made numerous enhancements to protect the integrity of elections around the world and better secure our platforms. Among them, we introduced strict policies and processes for identity verification for advertisers who run election-related advertising on our platform; we launched comprehensive political ad libraries in the U.S. and in other countries around the world; we developed and implemented policies to prohibit election-related abuse such as voter suppression and deceptive practices on platforms like YouTube, Google Ads, Google Maps and Google Play; our Threat Analysis Group (TAG) launched a quarterly bulletin to provide regular updates on our work to combat coordinated influence operations across our platforms and flagged phishing attempts against the presidential campaigns; and we worked closely with government agencies, including the FBI's Foreign Influence Task Force, and other companies to share information around suspected election interference campaigns.

On YouTube, throughout 2020, we identified and removed content that was misleading voters about where or how to vote, to help ensure viewers saw accurate information about the upcoming election. After December 8th, which marked the "safe harbor" deadline for states to certify their election, in accordance with our Presidential Election Integrity policy we began to remove content uploaded on or after December 9th that misled people by alleging that widespread fraud or errors changed the outcome of the 2020 U.S. presidential election. In addition, we continued to enforce our broader policies – for instance, from October to December 2020, we removed 13,000 YouTube channels for promoting violence and violent extremism; 89% of videos removed for violating our violent extremism policy were taken down before they had 10 views.

This work was in addition to improvements in the ranking systems we use to reduce the spread of harmful misinformation on YouTube: in January 2019, we announced that we would begin reducing recommendations of borderline content or videos that could misinform viewers in harmful ways but that do not violate YouTube Community Guidelines. Since then, we've launched numerous changes to reduce recommendations of borderline content and harmful misinformation, and we continue to invest in this work: our models review more than 100,000 hours of videos every day to find and limit the spread of borderline content.

Our work is never done, and we continue to learn and improve from one election cycle to the next, and continue to evolve our policies. That principle has guided our approach to new and evolving challenges, including COVID-19 misinformation.

Addressing the challenge of COVID-19 misinformation

This past year we've also focused on providing quality information during the pandemic. Since the outbreak of COVID-19, teams across Google have worked to provide quality information and resources to help keep people safe, and to provide

public health, scientists and medical professionals with tools to combat the pandemic. We've launched more than 200 new products, features and initiatives—including the Exposure Notification API to assist contact tracing—and have pledged over \$1 billion to assist our users, customers and partners around the world.

Today, when people search on Google for information for COVID-19 vaccines in the United States, we present them with a list of authorized vaccines in their location, with information on each individual vaccine from the FDA or CDC, as relevant. We also provide them with information about vaccination locations near them in Google Search and Google Maps, when that information is available. On YouTube, we launched COVID-19 information panels directing viewers to the CDC's information about the virus and, later on, about vaccines. These information panels are featured on the YouTube homepage, and on videos and in search results about the pandemic. Since March 2020, they have been viewed over 400 billion times. And we continue to work with YouTube creators to pair them with health experts who can get the facts to a wide range of audiences – we promote this content in our “ask the experts” feature.

Another way we've been helping is by offering over \$350 million in Ad Grants to help more than 100 government agencies and non-profit organizations around the world run critical public service announcements (PSAs) about COVID-19. Grantees can use these funds throughout 2021 for things like vaccine education and outreach campaigns.

In parallel to our efforts to elevate authoritative information about the pandemic and vaccines, we have worked across our services to combat harmful misinformation about these topics. Across our products, we've had long-standing policies prohibiting harmful and misleading medical or health-related content. When COVID-19 hit, our Trust and Safety team worked to stop a variety of abuses stemming from the pandemic, including phishing attempts, malware, dangerous conspiracy theories, and

fraud schemes. We took quick action to remove content that promoted inaccurate or misleading claims about cures, masks, and vaccines; our teams have removed 850,000 videos related to dangerous or misleading COVID-19 medical information, and in total, we blocked nearly 100 million COVID-related ads throughout 2020. Our teams have also been planning for new threats and abuse patterns related specifically to COVID-19 vaccines. For example, in October, we expanded our COVID-19 medical misinformation policy on YouTube to remove content about vaccines that contradicts consensus from health authorities, such as the Centers for Disease Control or the World Health Organization (WHO).

Developing Clear and Transparent Policies

We were able to act quickly and decisively because of the significant investments we have made over years, not only to make information useful and accessible, but also to remove and reduce the spread of harmful misinformation. Across all of this work, we strive to have clear and transparent policies and enforce them without regard to political party or point of view. We work to raise up authoritative sources, and reduce the spread of misinformation in recommendations and elsewhere. Teams across the company work in a variety of roles to help develop and enforce our policies, monitor our platforms for abuse, and protect users from everything from account hijackings and disinformation campaigns to misleading content and inauthentic activity. And we don't do this work alone; we work closely with experts to stay ahead of emerging threats.

Supporting innovation in journalism and the development of new business models

At Google, we believe that a vibrant news industry is vital to tackling misinformation on a societal scale. We invested millions to support COVID-19 related fact checking initiatives, providing training or resources to nearly 10,000 journalists. In addition to helping journalists tackle misinformation, we have long been committed to supporting

newsrooms and journalists in the United States and abroad. Over the past 20 years, we have collaborated closely with the news industry and provided billions of dollars to support the creation of quality journalism in the digital age.

We share a strong interest in supporting a diverse and sustainable ecosystem of quality news providers. Our products are designed to elevate high quality journalism and connect consumers to diverse news sites — from global media companies to smaller digital startups.

We are proud that our services help people all over the world find relevant, authoritative news about issues that matter to them. Each month, people click through from Google Search and Google News results to publishers' websites more than 24 billion times — that's over 9,000 clicks per second. This free traffic helps new publishers increase their readership, build trust with readers and earn money through advertising and subscriptions. We also recently announced a new investment in Google News Showcase and committed \$1 billion over the next three years to pay publishers to produce editorially curated content experiences and for limited free user access to paywalled content. In less than one year, we have been able to partner with over 500 publications across more than a dozen countries, spanning global, national, regional, metro and local publications.

Our commitment to the future of news extends beyond our products and services. We launched the Google News Initiative to support journalistic innovation and the emergence of new business models. Since 2018, we have committed \$61 million in funding to support more than two thousand news partners across the United States and Canada. As part of this initiative, we have also helped more than 447,200 journalists develop knowledge and skills in digital journalism through in person and online trainings through the Google News Lab. And when the pandemic hit, we turned our resources to support local news organizations and fact-checkers — contributing

\$10.6 million to over 1,800 local newsrooms across the U.S. and Canada through our Journalism Emergency Relief Fund and committing \$6.5 million to combat Covid-19 misinformation. We look forward to continuing this work with our partners in the news industry to ensure a thriving and healthy future for journalism.

The role of Section 230 in fighting misinformation

These are just some of the tangible steps we've taken to support high quality journalism and protect our users online, while preserving people's right to express themselves freely. Our ability to provide access to a wide range of information and viewpoints, while also being able to remove harmful content like misinformation, is made possible because of legal frameworks like Section 230 of the Communications Decency Act.

Section 230 is foundational to the open web: it allows platforms and websites, big and small, across the entire internet, to responsibly manage content to keep users safe and promote access to information and free expression. Without Section 230, platforms would either over-filter content or not be able to filter content at all. In the fight against misinformation, Section 230 allows companies to take decisive action on harmful misinformation and keep up with bad actors who work hard to circumvent their policies.

Thanks to Section 230, consumers and businesses of all kinds benefit from unprecedented access to information and a vibrant digital economy. Today, more people have the opportunity to create content, start a business online, and have a voice than ever before. At the same time, it is clear that there is so much more work to be done to address harmful content and behavior, both online and offline.

Regulation has an important role to play in ensuring that we protect what is great about the open web, while addressing harm and improving accountability. We are,

however, concerned that many recent proposals to change Section 230—including calls to repeal it altogether—would not serve that objective well. In fact, they would have unintended consequences—harming both free expression and the ability of platforms to take responsible action to protect users in the face of constantly evolving challenges.

We might better achieve our shared objectives by focusing on ensuring transparent, fair, and effective processes for addressing harmful content and behavior. Solutions might include developing content policies that are clear and accessible, notifying people when their content is removed and giving them ways to appeal content decisions, and sharing how systems designed for addressing harmful content are working over time. With this in mind, we are committed not only to doing our part on our services, but also to improving transparency across our industry.

I look forward to sharing more about our approach with you today, and working together to create a path forward for the web's next three decades.

Mr. DOYLE. Thank you, Mr. Pichai.
The Chair now recognizes Mr. Dorsey for 5 minutes.

STATEMENT OF JACK DORSEY

Mr. DORSEY. Thank you, members of the Energy and Commerce Committee and its subcommittees for the opportunity to speak with the American people about how Twitter may be used to spread disinformation, and our solutions. My remarks will be brief so we can move to your questions and discussion.

In our discussion today, some of you might bring up specific tweets or examples, and I will probably have an answer like, "My team will follow up with you." I don't think that is useful. I would rather us focus on principles and approaches to address these problems. I will start with ours.

We believe in free expression. We believe in free debate and conversation to find the truth. At the same time, we must balance that with our desire for our service not to be used to sow confusion, division, or destruction. This makes the freedom to moderate content critical to us.

Our process to moderate content is designed to constantly evolve. We observe what is happening on our service. We work to understand the ramifications. And we use that understanding to strengthen our operations. We push ourselves to improve, based on the best information we have.

Much of what we are likely to discuss today are entirely new situations the world has never experienced before and in some unique cases involved elected officials. We believe the best way to face a big, new challenge is through narrowing the problem to have the greatest impact.

Disinformation is a broad concept, and we needed to focus our approach on where we saw the greatest risk if we hope to have any impact at all. So we chose to focus on disinformation leading to offline harm, and three categories to start: manipulated media, public health, and civic integrity.

Many of you will have strong opinions on how effective we are in this work. Some of you will say we are doing too much and removing free speech rights. Some of you will say we are not doing enough and end up causing more harm. Both points of view are reasonable and worth exploring.

If we woke up tomorrow and decided to stop moderating content, we would end up with a service very few people or advertisers would want to use. Ultimately, we are running a business, and a business wants to grow the number of customers it serves. Enforcing policy is a business decision. Different businesses and services will have different policies, some more liberal than others, and we believe it is critical this variety continues to exist. Forcing every business to behave the same reduces innovation and individual choice and diminishes free marketplace ideals.

If instead we woke up tomorrow and decided to ask the government to tell us what content to take down or leave up, we may end up with a service that couldn't be used to question the government. This is a reality in many countries today, and is against the right of an individual. This would also have the effect of putting enormous resource requirements on businesses and services, which

would further entrench only those who are able to afford it. Smaller businesses would not be able to compete, and all activity would be centralized into very few businesses.

So how do we resolve these two viewpoints? One way is to create shared protocols. Social media has proven itself important enough to be worthy of an internet protocol, one that a company like Twitter can contribute to and compete on creating experiences people love to use. We started work on such a protocol, which we call Blue Sky. It intends to act as a decentralized, open-source social media protocol not owned by any single company or organization. Any developer around the world can help develop it, just as any company can access its services.

But does an open protocol address the concerns raised here? Greater transparency is the strongest benefit. Anyone around the world can see everything that is happening in the newsletter, including exactly how it works. One doesn't have to trust a company. Just look at the source code.

Second, since the base protocol is shared, it will increase innovation around business models, recommendation algorithms, and moderation controls, which are in the hands of individuals rather than private companies. This will allow people to experiment in a market-based approach. Finally, it will allow all of us to observe, acknowledge, and address any societal issues that arise much faster. Having more eyes on the problems will lead to more impactful solutions that can be built directly into this protocol, making the network far more secure and resilient.

A decentralized, open-source protocol for social media is our vision and work for the long term. We continue the cycle mentioned earlier of constantly improving our approach to content moderation in the short term. I hope our discussion today will focus on more enduring solutions.

One final note: We are a bunch of humans with a desire to make the world around us better for everyone living today and those that come after us. We make mistakes in prioritization and in execution. We commit to being open about these and doing our best to remedy what we control.

We appreciate the enormous privilege we have in building technologies to host some of the world's most important conversations, and we honor the desire to create better outcomes for everyone who interacts with them.

Thanks for your time, and I look forward to the discussion.

[The prepared statement of Mr. Dorsey follows:]

**WRITTEN TESTIMONY OF TWITTER CEO JACK DORSEY (@JACK)
U.S. HOUSE COMMITTEE ON ENERGY & COMMERCE
MARCH 25, 2021**

Twitter's purpose is to serve the public conversation. While much has changed in the world since we started fifteen years ago, we believe our mission is more important than ever.

Every day Twitter grapples with complex considerations on how to address extremism and misinformation. How do we prevent harm, while also safeguarding free expression and the right of diverse individuals to express a range of views? How do we develop policies that can be built at scale and adapt rapidly, especially given diverse regulatory models around the world? What role should our company play in determining these pivotal questions? What information should we rely on when making decisions? How do we earn the trust of those who use our service?

These are even harder questions in an increasingly polarized world, which has consequently heightened concerns about information sources. Quite simply, a trust deficit has been building over the last several years, and it has created uncertainty — here in the United States and globally. That deficit does not just impact the companies sitting at the table today but exists across the information ecosystem and, indeed, across many of our institutions.

This Committee has expressed interest in what we are doing to combat “falsehoods about the COVID-19 vaccine” and “debunked claims of election fraud.” We have [COVID-19](#) and [vaccine misinformation](#) policies, as well as a [COVID information hub](#). Our [civic integrity](#) and [platform manipulation](#) policies are available on our [Help Center](#), along with information on our bans on [state-controlled media](#) advertising and [political advertising](#). As a follow-up to our [preliminary post-election update](#), we are conducting a review of the 2020 U.S. election, the findings of which we intend to share.

Our efforts to combat misinformation, however, must be linked to earning trust. Without trust, we know the public will continue to question our enforcement actions. I believe we can earn trust by focusing on the following: enhancing transparency, ensuring procedural fairness, enabling algorithmic choice, and strengthening privacy.

Building & Earning Trust

Every day, millions of people around the world Tweet hundreds of millions of Tweets, with one set of rules that applies to everyone and every Tweet. We strive to implement policies impartially and at scale. We built our policies primarily around the promotion and protection of three fundamental human rights — freedom of expression, safety, and privacy.

At times, these rights can conflict with one another. As we develop, implement, and enforce our policies, we must balance these rights. Additionally, our policies must be adaptable to changes in behavior and evolving circumstances. This is why we must be transparent, embrace procedural fairness and choice, and protect privacy.

Transparency

While Twitter has made significant progress with respect to transparency, we know that we can do more to strengthen our efforts. People who use our service should understand our processes — how potential violations of our rules are reported and reviewed, how content-related decisions are made, and what tools are used to enforce these decisions. Publishing answers to questions

like these will continue to make our internal processes both more robust and more accountable to the people we serve.

Twitter's open nature means our enforcement actions are plainly visible to the public, even when we cannot reveal the private details behind individual accounts that have violated our rules. We use a combination of machine learning and human review to assess potential violations of the Twitter Rules. We take a behavior-first approach, meaning we look at how accounts behave before we review the content they are posting. If an account owner breaks our Rules and may be required to delete a Tweet, we have worked to build better in-app notices to communicate with both the account that reports a Tweet and the account that posted it with additional information about our actions. In January, we published our biannual update to the [Twitter Transparency Center](#), with additional data about actions we have taken to disrupt state-backed information operations, to enforce our COVID-19 policy, and take action on Tweets that violate our Rules.

In addition to ensuring transparency around our decisions, we are seeking ways to enhance transparency around how we develop our content moderation policies. In recent months, for example, there have been increased questions about how we should address policy violations from world leaders. As a result, we are currently re-examining our approach to world leaders and are soliciting [feedback](#) from the public. Our feedback period is currently open and our survey will be available in more than a dozen languages to ensure a global perspective is reflected.

Procedural Fairness (Accountability & Reliability)

Twitter is focused on advancing procedural fairness in our decision-making. We strive to give people an easy, clear way to appeal decisions we make that they think are not right. Mistakes in enforcement — made either by a human or an automated system — are inevitable and why we strive to make appeals easier. We believe that all companies should be required to provide those who use their service with straightforward processes to appeal decisions that impact them.

Algorithmic Choice

We believe that people should have transparency or meaningful control over the algorithms that affect them. We recognize that we can do more to provide algorithmic transparency, fair machine learning, and controls that empower people. The machine learning teams at Twitter are studying techniques and developing a roadmap to ensure our present and future algorithmic models uphold a high standard when it comes to transparency and fairness.

We also provide people control over algorithms that affect their core experience on Twitter. We have invested heavily in building systems that organize content to show individuals relevant information that improves their experience. With 192 million people last quarter using Twitter daily in dozens of languages and countless cultural contexts, we rely upon machine learning algorithms to help us organize content by relevance to provide a better experience for the people who use our service.

Privacy

We have always believed that privacy is a fundamental human right. We believe that individuals should understand the personal data that is shared with companies and have the tools to help

them control their information. To help people better understand their options, we have created the [Twitter Privacy Center](#), which acts as a hub for information about our privacy and data protection work.

We are constantly working to improve the controls people have to manage their personal data and experience on Twitter. In addition, we continue to support efforts to pass strong federal privacy legislation to safeguard important privacy rights.

Innovations to Address Misinformation

We also recognize that addressing harms associated with misinformation requires innovative solutions. Content moderation in isolation is not scalable, and simply removing content fails to meet the challenges of the modern Internet. This is why we are investing in two experiments — [Birdwatch](#) and [Bluesky](#). Both are aimed at improving our efforts to counter harmful misinformation.

Birdwatch

In January, we launched the “Birdwatch” pilot, a community-based approach to misinformation. Birdwatch is expected to broaden the range of voices involved in tackling misinformation, and streamline the real-time feedback people already add to Tweets. We hope that engaging diverse communities here will help address current deficits in trust for all. More information on Birdwatch can be found [here](#). We expect data related to Birdwatch will be publicly available at [Birdwatch Guide](#), including the algorithm codes that power it.

Bluesky

Twitter is also funding Bluesky, an independent team of open source architects, engineers, and designers, to develop open and decentralized standards for social media. This team has already created an initial review of the ecosystem around protocols for social media to aid this effort. Bluesky will eventually allow Twitter and other companies to contribute to and access open recommendation algorithms that promote healthy conversation and ultimately provide individuals greater choice. These standards will support innovation, making it easier for startups to address issues like abuse and hate speech at a lower cost. Since these standards will be open and transparent, our hope is that they will contribute to greater trust on the part of the individuals who use our service. This effort is emergent, complex, and unprecedented, and therefore it will take time. However, we are excited by its potential and will continue to provide the necessary exploratory resources to push this project forward.

Conclusion

As we look to the future, I agree with this Committee that technology companies have work to do to earn trust from those who use our services. For Twitter, that means tackling transparency, procedural fairness, algorithmic choice, and privacy. I think that this approach will be a growing trend across all companies and organizations, both big and small. I look forward to your questions.

Mr. DOYLE. Thank you, Mr. Dorsey.

Well, we have concluded witness opening statements. At this time we will move to Member questions. I want to make sure that Members are aware that our witnesses are being assisted by counsel, and during questions our witnesses may briefly mute themselves to seek advice of counsel, which is permitted.

Each Member will have 5 minutes to start asking questions of our witnesses. I ask everyone to please adhere to that 5-minute rule, as we have many people that want to ask questions. I will start by recognizing myself for 5 minutes.

Mr. DUNCAN. Mr. Chairman, a point of order?

Mr. DOYLE. The gentleman—who is speaking?

Mr. DUNCAN. This is Jeff Duncan. Point of order.

Mr. DOYLE. Yes, sir?

Mr. DUNCAN. If the witnesses are advised by counsel and we are not swearing them in, why would they need counsel?

Mr. DOYLE. In previous hearings, we have always permitted witnesses to have counsel. Sometimes you will see them at a hearing just leaning back and talking to their counsel before a question. But it is allowed under our rules, and I just wanted to make Members aware that they may mute themselves while that is going on.

Mr. DUNCAN. They should be sworn in, but I yield back. Thank you.

Mr. DOYLE. OK. Gentlemen, my time is short, and I ask that you make your responses as brief and to the point as possible. If I ask you a yes-or-no question, I am just looking for a yes or no. So please respond appropriately.

I want to start by asking all three of you if your platform bears some responsibility for disseminating disinformation related to the election and the Stop the Steal movement that led to the attack on the Capitol. Just a yes or no answer. Mr. Zuckerberg?

Mr. ZUCKERBERG. Chairman, I think our responsibility is to build systems that can help fight—

Mr. DOYLE. Mr. Zuckerberg, I just want a yes or no answer. OK? Yes or no: Do you bear some responsibility for what happened?

Mr. ZUCKERBERG. Congressman, our responsibility is to make sure that we build effective systems to help fight the spread of—

Mr. DOYLE. OK. The gentleman's preference is not to answer the question.

Mr. Pichai, yes or no?

Mr. PICHAI. We always feel a deep sense of responsibility. But I think we worked hard. This election effort was one of our most substantive efforts.

Mr. DOYLE. Is that a yes or a no?

Mr. PICHAI. Congressman, it is a complex question. We—

Mr. DOYLE. OK. We will move on.

Mr. Dorsey?

Mr. DORSEY. Yes. But you also have to take into consideration a broad ecosystem. It is not just about the technology platforms that are used.

Mr. DOYLE. Thank you. Thank you, and I agree with that.

Mr. Zuckerberg, independent analysis has shown that despite all the things that Facebook did during the election, users still interacted with election misinformation roughly 1.1 billion times

over the last year. The initial Stop the Steal group started on Facebook and gained over 350,000 followers in less than a day, faster than almost any other in your platform's history, and they were immediately calling for violence.

In mid-December, you stopped promoting high-quality news outlets for election content at a time when the disinformation was at its height. And finally, the FBI has released numerous documents showing that many of the insurrectionists used Facebook to coordinate and plan the attack on January 6th.

So my question is: How is it possible for you not to at least admit that Facebook played a central role or a leading role in facilitating the recruitment, planning, and execution of the attack on the Capitol?

Mr. ZUCKERBERG. Chairman, my point is that I think that the responsibility here lies with the people who took the actions to break the law and take—and do the insurrection.

And secondarily, also, the people who spread that content, including the President but others as well, with repeated rhetoric over time saying that the election was rigged and encouraging people to organize. I think that those people bear the primary responsibility as well. And that was the point that I was making.

Mr. DOYLE. I understand that. But your platforms supercharged that. You took what—a thing and magnified it. In 12 hours you got 350,000 people in your site. You gin this up. Your algorithms make it possible to supercharge these kinds of opinions. I think we are here because of what these platforms enabled, how your choices put our lives and our democracy at risk. And many of us just find it just unacceptable.

I want to ask each of you another question: Do you think vaccines that have been approved for COVID-19 work? Just yes or no. Do you think the vaccines that have been approved work? Mr. Zuckerberg?

Mr. ZUCKERBERG. Yes.

Mr. DOYLE. Mr. Pichai?

Mr. PICHAI. Yes. Absolutely.

Mr. DOYLE. Mr. Dorsey?

Mr. DORSEY. Yes. But I don't think we are here to discuss our own personal opinions.

Mr. DOYLE. I just want to know if you think the vaccines work. Yes?

Mr. DORSEY. Yes. However—

Mr. DOYLE. Thank you. OK. So if you think the vaccines work, why have your companies allowed accounts that repeatedly offend your vaccine disinformation policies to remain up? I mean, according to report, just 12 accounts on Facebook, Twitter, and Instagram account for 65 percent of all the vaccine disinformation on your platforms. You are exposing tens of millions of users to this every day. I don't have the stats on YouTube, but my understanding is it is similar.

So my question is: Why, in the midst of a global pandemic that has killed over half a million Americans, that you haven't taken these accounts down that are responsible for the preponderance of vaccine disinformation on your platforms? Will you all commit to taking these platforms down today? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congressman, yes, we do have a policy against allowing vaccine disinformation—

Mr. DOYLE. Oh, I know you have a policy, but will you take the sites down today? You still have 12 people up on your site doing this. Will you take them down?

Mr. ZUCKERBERG. Congressman, I would need to look at the—and have our team look at the exact examples to make sure they violate the policy—

Mr. DOYLE. Look at them today and get back to us tomorrow because those still exist. We found them as early as last night.

Mr. Pichai, how about you?

Mr. PICHAI. We have removed over 850,000 videos and we—

Mr. DOYLE. But have you removed them all? Do you still have people that are spreading disinformation on your platforms? There are about 12 superspreaders.

Mr. PICHAI. We have clear policies and we take down content. Some of the content is allowed if it is people's personal experiences. But we definitely—

Mr. DOYLE. OK. Thank you. Mr. Dorsey? I see my time is getting expired. Mr. Dorsey? Will you take these sites down? You got about 12 superspreaders. Will you take them down?

Mr. DORSEY. Yes. We remove everything against our policy.

Mr. DOYLE. Thank you.

I see my time is expired. I will now yield to the ranking member, Mr. Latta, for his 5 minutes.

Mr. LATTA. I thank my friend for yielding.

Amanda Todd was just 15 years old when she hung herself. Amanda met a man online who took inappropriate screenshots of Amanda and proceeded to follow her around the internet and harass her for years. He found her classmates on Facebook and he would send them the picture he took of her. To cope with the anxiety, Amanda turned to drugs and alcohol. But it became too much for her.

Mr. Zuckerberg, clearly Ms. Todd was underage, so the photo that was shared to harass her was illegal. Do you believe that Facebook bears any responsibility for the role it played in her death? Yes or no?

Mr. ZUCKERBERG. Sorry, I was muted. Congressman, that is a—it is an incredibly sad story. And I think that we certainly have a responsibility to make sure that we are building systems that can fight and remove this kind of harmful content. In the case of child exploitation content, we have been building systems for a long time that use AI, and we have thousands of people working on being able to identify this content and remove it, and I think our systems are generally pretty effective at this. And I think it is our responsibility to make sure that we keep improving them.

Mr. LATTA. My time—my time is pretty short, but would you say yes or no then?

Mr. ZUCKERBERG. Sorry. Can you repeat that?

Mr. LATTA. Well, in the question, yes or no, then? Any responsibility?

Mr. ZUCKERBERG. Congressman, I believe that the responsibility of the platform—

Mr. LATTA. OK. Well, let me move on because I have got—I am very short on time.

Do you believe that Facebook should be held accountable for any role in her death? Yes or no?

Mr. ZUCKERBERG. Congressman, the responsibility that I think platforms should have—

Mr. LATTA. OK.

Mr. ZUCKERBERG [continuing]. Is to build effective systems to moderate this content.

Mr. LATTA. I am going to have to move on. I am going to have to take it that you are just not responding to the question.

Unfortunately, stories like Amanda Todd's are only becoming more common. While we all can talk about how your platforms can be used for good or evil, the evil seems to persevere.

Mr. Zuckerberg, you stated that you support thoughtful changes to Section 230 to ensure that tech companies are held accountable for certain actions that happen on their platforms, such as child exploitation. What specific changes do you support in Section 230?

Mr. ZUCKERBERG. Thanks, Congressman. I would support two specific changes, especially for large platforms—although I want to call out that I think for smaller platforms I think we need to be careful about any changes that we make that remove their immunity, because that could hurt competition. So let me just call on these for larger platforms.

I think, first, platforms should have to issue transparency reports that state the prevalence of content across all different categories of harmful content, everything from child exploitation to terrorism to incitement of violence to intellectual property violations to pornography, whatever the different harms are, and—

Mr. LATTA. Well, let me ask real quick now: Where are those transparency reports you are being reported to, and how often do you think that should be going out?

Mr. ZUCKERBERG. Oh, Congressman, as a model, Facebook has been doing something to this effect for every quarter, where we report on the prevalence of each category of harmful content and how effective our systems are at identifying that content and removing it in advance. And I think the company should be held accountable for having effective systems to do that broadly.

The second change that I would propose is creating accountability for the large platforms to have effective systems in place to moderate and remove clearly illegal content, so things like sex trafficking or child exploitation or terrorist content. And I think it would be reasonable to condition immunity for the larger platforms on having a generally effective system in place to moderate clearly illegal types of content.

Mr. LATTA. Let me interrupt real quick because I am running really short on time. Because I know in your testimony you are talking about that you would—you say that platforms should not be held liable if a particular piece of content evades its detection.

So again, that is one of the areas when you are talking about the transparency and also the accountability I would like to follow up on.

Let me ask you real quick, Mr. Pichai, yes or no: Do you agree with Mr. Zuckerberg's changes to Section 230?

Mr. PICHAI. There are definitely good proposals around transparency and accountability, which I have seen in various legislative proposals as well, which I think are important principles and we would certainly welcome legislative approaches in that area.

Mr. LATTA. OK. Mr. Dorsey, do you agree with Mr. Zuckerberg? Yes or no? On the changes on 230?

Mr. DORSEY. I think the ideas around transparency are good. I think it is going to be very hard to determine what is a large platform and a small platform, and it may incentivize the wrong things.

Mr. DOYLE. OK. The gentleman's time is expired.

Mr. LATTA. Thank you very much. My time is expired, and I yield back.

Mr. DOYLE. The Chair now recognizes Chair Schakowsky, chair of the Subcommittee on Consumer Protection and Commerce, for 5 minutes.

Ms. SCHAKOWSKY. Thank you so much.

Mr. Zuckerberg, immediately after the Capitol insurgency, Sheryl Sandberg did an interview in which she insisted that the siege was largely planned on smaller platforms, that—but the court filings actually show something quite the opposite, that the Proud Boys and Oath Keepers used Facebook to coordinate in real time during the siege.

And so my question for you is: Will you admit today that Facebook groups, in particular, played a role in fomenting the extremism that we saw and that led to the Capitol siege?

Mr. ZUCKERBERG. Congresswoman, thanks for the question on this. In the comment that Sheryl made, what I believe that we were trying to say was—and what I stand behind—is what was widely reported at the time, that after January 6th—

Ms. SCHAKOWSKY. No. But I am sorry to interrupt, as many of my colleagues have had to do because we only have 5 minutes. But would you say that—and would you admit that Facebook played a role?

Mr. ZUCKERBERG. Congresswoman, I think certainly there was content on our services, and from that perspective, I think that there is further work that we need to do to make our services and moderation more effective.

Ms. SCHAKOWSKY. I have heard that. OK. I am going to ask Mr. Pichai a question.

Many companies have used Section 230 as a shield to escape consumer protection laws. And I have a bill that would actually not protect companies that do that. And so, Mr. Pichai, would you agree that that would be proper use, to not allow liability protection for those who violate consumer protection laws?

Mr. PICHAI. Congresswoman, consumer protection laws are very important areas, like we comply with COPPA and HIPAA. I think the right approach is to have legislation in applicable areas and have us—

Ms. SCHAKOWSKY. OK. I am going to have to interrupt again. Is that a yes, that if a law has been broken, a consumer protection law, that it would not—there would not be liability protection under Section 230 for you?

Mr. PICHAI. We rely on the liability protections to actually take strong action in, particularly, new types of content. When the Christchurch shooting happened, within a few minutes our teams had to make decisions about the content to take down. That certainty is what we rely on.

But I agree with you that we should have strong consumer protection laws and be subject to it and have agencies like the FTC have clear oversight over those laws and how we comply with them.

Ms. SCHAKOWSKY. Let me just ask a real—thank you—a real yes or no, quickly. Do you think that when you take money to run advertisements that promote disinformation, that you are exempt from liability? Yes or no? Yes or no?

Mr. PICHAI. Section 230—

Ms. SCHAKOWSKY. Mr. Zuckerberg? Yes or no?

Mr. ZUCKERBERG. Congresswoman, I don't know the legal answer to that. But we don't allow misinformation in our ads. And any ad that has been fact-checked as false, we don't allow it to run as an ad.

Ms. SCHAKOWSKY. OK. And Mr. Dorsey?

Mr. DORSEY. Again, I also would need to review the legal precedent for it. But we would not allow that.

Ms. SCHAKOWSKY. OK. And Mr. Pichai?

Mr. PICHAI. We are subject to FTC's deceptive ad practices, so there are statutes which apply to us. We removed over 3 billion bad ads last year alone.

Ms. SCHAKOWSKY. OK. Let me ask one more question: Do you think that Section 230 should be expanded to trade agreements that are being made, as happened in the U.S. trade agreement with Mexico and Canada? Yes or no? Mr. Zuckerberg.

Mr. ZUCKERBERG. Congresswoman, my primary goal would be to help update Section 230 to reflect the kind of modern reality in what we have learned over 25 years. But that said, I do still think that Section 230 plays a foundational role in the development of the internet and—

Ms. SCHAKOWSKY. I hear you. But I am talking now about trade agreements. Mr. Pichai?

Mr. PICHAI. Congresswoman, I think there is value in it. But if there are evolution of Section 230, that should apply. And so in a flexible way, being able to do that would be good, I think.

Ms. SCHAKOWSKY. Mr. Dorsey?

Mr. DORSEY. I don't fully understand the ramifications of what you are suggesting. So I would have to review any—

Ms. SCHAKOWSKY. I am saying to have a liability shield that would be international and clarify it in trade agreements. And I think it is a bad idea.

Mr. DOYLE. The gentlelady's time has expired.

Ms. SCHAKOWSKY. Thank you. I yield back.

Mr. DOYLE. The Chair now recognizes Mr. Bilirakis, ranking member of the Subcommittee on Consumer Protection and Commerce, for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it.

Mr. Dorsey, you have heard briefly about what I am hearing again my district. My opening remarks, you have heard them. The

other key part with these stories that we are hearing when we conduct these surveys is how we empower law enforcement.

In a hearing last year, we received testimony that since 2016 Twitter has intentionally curtailed sharing threat data with law enforcement fusion centers. Here is the question: You are well aware that on Twitter and Periscope, that traffic has increased from bad actors seeking to groom children for molestation, lure females into sex trafficking, sell illegal drugs, incite violence, and even threaten to murder police officers.

Are you willing to reinstate this cooperation, retain evidence, and provide law enforcement the tools to protect our most vulnerable? Yes or no?

Mr. DORSEY. Well, first, child sexual exploitation has no place on our platform, and I don't believe that is true. We work with local law enforcement regularly.

Mr. BILIRAKIS. So you are saying that this is not true, what I am telling you? Are you willing to reinstate—reinstate; in other words, it is not going on now—reinstate this cooperation with law enforcement to retain evidence and provide law enforcement the tools to protect our most vulnerable?

Mr. DORSEY. We would love to work with you in more detail on what you are seeing. But we work with law enforcement regularly. We have a strong partnership.

Mr. BILIRAKIS. So you are saying that this is not true, what I am telling you?

Mr. DORSEY. I don't believe so. But I would love to understand the specifics.

Mr. BILIRAKIS. Will you commit to doing what I am telling you you are not doing in the future, and work with me on this?

Mr. DORSEY. We will commit to continue doing what we are doing.

Mr. BILIRAKIS. And what is that? You are saying that the—so in other words—

Mr. DORSEY. Working with the local law enforcement.

Mr. BILIRAKIS. OK. Well, let me go on to the next question. But I am going to follow up with this to make sure you are doing this. I mean, our children's lives are in jeopardy here.

Mr. Zuckerberg, we have heard you acknowledge mistakes about your products before. There are now media reports of an Instagram for under-13 being launched. My goodness. Between this and YouTube Kids, you and Mr. Pichai have obviously identified a business case for targeting this age bracket with content, and I find that very concerning, targeting this particular age bracket, 13 and under.

Given these free services, how exactly would you be making money, or are you trying to monetize our children, too, and get them addicted early? And will you be allowing your own children to use this site with the default settings? We are talking about, again, the site that apparently is being launched for children 13 and under, or under 13, actually. Can you please answer that question for me?

Mr. ZUCKERBERG. Congressman, we are early in thinking through how this service would work. There is clearly a large number of people under the age of 13 who would want to use a service

like Instagram. We currently do not allow them to do that. I think the offer—

Mr. BILIRAKIS. What would be beneficial to our children to launch this kind of service?

Mr. ZUCKERBERG. Well, Congressman, I think helping people stay connected with friends and learn about different content online is broadly positive. There are clearly issues that need to be thought through and worked out, including how parents can control the experience of kids, especially kids under the age of 13. And we haven't worked through all of that yet, so we haven't kind of formally announced the plans. But I think that something like this could be quite helpful for a lot of people.

Mr. BILIRAKIS. Excuse me. OK, I will reclaim my time.

Mr. Pichai, your company has had failures to rating content for kids. What advice would you offer your challenge here?

Mr. PICHAI. Congressman, we have invested a lot in a one-of-a-kind product, YouTube Kids. The content there is—we work with trusted content partners. Think Sesame Street as an example of the type of channel you would find there, science videos and cartoons. And we take great effort to make sure—

Mr. BILIRAKIS. I need to reclaim my time. I have one more—one last question for Mr. Zuckerberg.

Do you have concerns with what has appeared on your platform hosted by YouTube? And with regard to your children, about—in general. Do you have concerns, yes or no?

Mr. ZUCKERBERG. Congressman, are you asking me about YouTube?

Mr. BILIRAKIS. Yes. I am asking you about YouTube.

Mr. ZUCKERBERG. Congressman, I use YouTube to watch educational videos with my children, and—

Mr. BILIRAKIS. Do you have concerns? First, for your children and your family personally? Do you have concerns?

Mr. ZUCKERBERG. Well, Congressman, my children are 5 and 3 years old. So when I watch content on YouTube with them, I am doing it and supervising them. So in that context, no, I haven't particularly had concerns. But I think it is important that if anyone is building a service for kids under the age of 13 to use by themselves, that there are appropriate parental controls.

Mr. DOYLE. The gentleman's time is expired.

Mr. BILIRAKIS. Thank you.

Mr. DOYLE. I would ask all Members to try to stick to our 5-minute rule so that we can get out of here before midnight.

The Chair will now recognize Mr. Pallone, the full committee chair, for 5 minutes.

Mr. PALLONE. Thank you, Chairman Doyle. My questions are of Mr. Zuckerberg and Mr. Pichai. But I just want to say, after listening to the two of you's testimony, you definitely give the impression that you don't think that you are actively in any way promoting this misinformation and extremism. And I totally disagree with that.

You are not passive bystanders. You are not nonprofits or religious organizations that are trying to do a good job for humanity. You are making money. And the point we are trying to make today—or at least I am—is that when you spread disinformation,

misinformation, extremism, actively promoted and amplified, you do it because you make more money.

And so I kind of deny the basic premise of what you said. But let me get to the questions. Let me ask Mr. Zuckerberg. According to a May 2020 Wall Street Journal report, a Facebook researcher concluded that Facebook's own recommendation tools were tied to a significant rise in membership in extremist Facebook groups in Germany. I wrote to you last month requesting this research and related documents. I trust you will fully cooperate with the committee's inquiry and provide all requested documents and information.

But my question is, and please yes or no: Were you aware of this research showing that 64 percent of the members in the extremist Facebook groups studied joined because of Facebook's own recommendations to join these extremist groups in Germany? Were you aware of that, yes or no?

Mr. ZUCKERBERG. Congressman, this is something that we study because we want to make sure our products—

Mr. PALLONE. But I am asking whether you were aware of it. It is a simple question. Yes or no: Were you aware of it? That is all I am asking. Were you aware of it?

Mr. ZUCKERBERG. Aware at what time? After we studied that—

Mr. PALLONE. I just asked if you were aware of it, Mr. Zuckerberg. Yes or no? If not, I am going to assume that the answer is yes. OK?

Mr. ZUCKERBERG. Congressman, I have seen the study. It was about a—

Mr. PALLONE. All right. So your answer is yes.

Mr. ZUCKERBERG [continuing]. Contest leading up to the German election. And we have since—

Mr. PALLONE. I appreciate that. Let me go to the final question, which relates to that. You said yes. OK.

The troubling research I mentioned demonstrates that Facebook was not simply allowing disinformation and extremism to spread, it actively amplified it and spread it. This is my point. Nonetheless, Facebook didn't permanently stop recommending political and civil groups to the United States until after the January 6th insurrection, years after it was made aware of this research.

The fact that Facebook's own recommendation system helped populate extremist groups compels us to reevaluate platforms' liabilities. Now, back to that Wall Street Journal article.

Facebook's chief product officer, Chris Cox, championed an internal effort to address division on Facebook and proposed a plan that would have reduced the spread of content by hyperactive users on the far left and far right. The article alleges, Mr. Zuckerberg, that you personally reviewed this proposal and approved it, but only after its effectiveness was decreased to 80 percent.

Is that true? Yes or no, please?

Mr. ZUCKERBERG. Congressman, we have made a lot of measures that—to fight this content, including—

Mr. PALLONE. Did you approve it after its effectiveness was decreased to 80 percent? Yes or no?

Mr. ZUCKERBERG. Congressman, I can't speak to that specific example. But we have put in place a lot of different measures, and I think that they are effective, including—

Mr. PALLONE. Did you review the proposal and approve it?

Mr. ZUCKERBERG. Congressman, we do a lot of work in this area and I review a lot of proposals and we move forward on a lot of steps.

Mr. PALLONE. It is not a difficult question. I am just asking if you reviewed this internal proposal and you approved it. And you won't even answer that. It is so easy to answer that question. It is very specific.

All right. You won't answer. Right? Yes or no?

Mr. ZUCKERBERG. Congressman, that is not what I said. I said I did review that in addition to many other proposals and things that we have taken action on.

Mr. PALLONE. You whether or not—

Mr. ZUCKERBERG. Including shutting off recommendations for civic and political groups.

Mr. PALLONE. Did you approve it with the 80 percent decrease in effectiveness?

Mr. ZUCKERBERG. Congressman, I don't remember that specifically. But we have taken a number of different—

Mr. PALLONE. OK. Let me—

Mr. ZUCKERBERG [continuing]. Steps on this.

Mr. PALLONE. Let me go to Mr. Pichai. Mr. Pichai, according to the New York Times, YouTube's recommendation algorithm is responsible for more than 70 percent of the time users spend on YouTube. In fact, a former design ethicist at Google was quoted as saying, "If I am YouTube and I want you to watch more, I am always going to steer you towards Crazy Town."

Mr. Pichai, is YouTube's recommendation algorithm designed to encourage users to stay on the site? Yes or no? Is it designed to encourage users to stay on the site? Yes or no?

Mr. PICHAI. Content responsibilities are our number one goal, so that trumps everything.

Mr. PALLONE. I am only asking—very simple—whether YouTube's recommendation algorithm is designed to encourage users to stay on the site. Simple question. Yes or no.

Mr. PICHAI. That is not the sole goal, Congressman. That would definitely—

Mr. PALLONE. So the answer is yes. OK. So the bottom line is, simply put, your company's bottom line compels you to amplify extremist and dangerous content. You are not bystanders. And what happens online doesn't stay online. It has real-world consequences. That is why Congress has to act, because you are not bystanders. You are encouraging this stuff.

Thank you, Mr. Chairman.

Mr. DOYLE. The gentleman's time is expired.

The Chair now recognizes Ms. Rodgers, the full committee ranking member, for 5 minutes.

Ms. RODGERS. We tragically lost a number of young people to suicide in my community. In a 3-year period from 2013 to 2016, the suicide rate more than doubled in Spokane County. In the last six months, one high school lost three teens. Right now suicide is the second-leading cause of death in the entire State of Washington for teens 15 to 19 years old.

As I mentioned, it has led to many painful conversations trying to find some healing for broken families and communities. And together we have been asking, what has left our kids with a deep sense of brokenness? Why do children, including kids we have lost in middle school, feel so empty at such a young, vulnerable age?

Well, some studies are confirming what parents in my community already know: Too much time on screens and social media is leading to loneliness and despair. And it seems to be an accepted truth in the tech industry because what we are hearing today: Making money is more important.

Bill Gates put a cap on screen time for his daughter. Steve Jobs once said in a quote, "We limit how much technology our kids use at home." Mr. Zuckerberg, you have also said that your kids—or you don't want your kids sitting in front of screens passively consuming content.

So Mr. Zuckerberg, yes or no: Do you agree too much time in front of screens, passively consuming content, is harmful to children's mental health?

Mr. ZUCKERBERG. Congresswoman, the research that I have seen on this suggests that if people are using computers and social—

Ms. RODGERS. Could you answer yes or no? I am sorry. Could you use yes or no?

Mr. ZUCKERBERG. I don't think that the research is conclusive on that. But I can summarize what I have learned, if that is helpful.

Ms. RODGERS. I will follow up at a later time because I do know that Facebook has acknowledged that passive consumption on your platform is leading to people feeling worse. And you said that going from video to video is not positive. Yet Facebook is designed to keep people scrolling. Instagram is designed to get users to go from video to video.

So I would like to ask you, if you said earlier that you don't want kids sitting in front of the screens passively consuming content, and your products are designed to increase screen time, do you currently have any limitations on your own kids' use of your products, or how do you think that will change as they get older?

Mr. ZUCKERBERG. Sure, Congresswoman. My daughters are 5 and 3, and they don't use our products. Actually, that is not exactly true. My eldest daughter, Max, I let her use Messenger Kids sometimes to message her cousins. But overall, the research that we have seen is that using social apps to connect with other people can have positive mental health benefits and well-being benefits by helping people feel more connected and less lonely.

Passively consuming content doesn't have those positive benefits to well-being but isn't necessarily negative. It just isn't as positive as connecting. And the way we design our algorithms is to encourage meaningful social interactions. So it is a common misconception that our teams—our goals, or even have goals, of trying to increase the amount of time that people spend.

The News Feed team at Facebook and the Instagram team—

Ms. RODGERS. Thank you, Mr. Zuckerberg. I do have a couple more questions.

So do you agree that your business model and the design of your products is to get as many people on the platform as possible and

to keep them there for as long as possible? If you could answer yes or no, that would be great.

Mr. ZUCKERBERG. Congresswoman, from a mission perspective, we want to serve everyone. But our goal is not—we don't—I don't give our News Feed team or our Instagram team goals around increasing the amount of time that people spend. I believe that if we build a useful product which—

Ms. RODGERS. OK. Thank you. Thank you. We all have limited time. I think the business model suggests that it is true.

It was mentioned earlier that you are studying extremism. I would like to ask, yes or no, of all of you, beginning with Mr. Zuckerberg: Has Facebook conducted any internal research as to the effect your products are having on the mental health of our children?

Mr. ZUCKERBERG. Congressman, I know that this is something that we try to study, and I am—

Ms. RODGERS. Can you say yes or no? I am sorry.

Mr. ZUCKERBERG. I believe the answer is yes.

Ms. RODGERS. OK. Mr. Dorsey, has Twitter?

Mr. DORSEY. I don't believe so, but we will follow up with you.

Ms. RODGERS. OK. Mr. Pichai, has Google conducted any research on the effect your products are having on the mental health of children?

Mr. PICHAI. We consult widely with expert third parties on this area, including SAMHSA and other mental health organizations, and invest a lot of time and effort in this area.

Ms. RODGERS. OK. I would like to see that. It sounds like you have studied extremism. Let's get focused on our children.

Mr. DOYLE. The gentlelady's time is expired.

The Chair now recognizes Mr. Rush for 5 minutes.

Bobby, you need to unmute.

There you go.

Nope, you are still muted.

Mr. RUSH. I want to thank you, Mr. Chairman. We all agree that social media sites should not be tools for stoking racial division or exacerbating racial injustice. However, there is a broad finding of research that demonstrates the disproportionate effects of disinformation and White supremacy extremism on women and people of color, especially Black people.

We have seen, and continue to see, that too often social media sites put their earnings before equality. Simply stated, your corporations carelessly put profits over people. Misinformation, outlandish conspiracy theories, and incendiary content targeting minorities remains firmly, and social media companies, your companies, are profiting from hate and racism on these platforms by harnessing data and generating advertising revenue from such content.

There is only one comparison that remotely approaches the avarice and moral discrepancy of your companies, and that is the slavetocracy burden of our Nation's shameful and inhumane and most difficult dark days in the past.

This is the very reason why I ask Mr. Dorsey, I remember you at our 2018 hearing to commit to commissioning an independent third-party civil rights audit of Twitter. This response at the hear-

ing was followed up with a joint letter from Chairman Pallone and myself confirming that commitment.

It is 3 years later, and I am still waiting, Mr. Dorsey, for the results of that audit. Where is that audit, Mr. Dorsey?

Mr. DORSEY. Thank you. We have taken another approach, which is to work with civil rights orgs on a regular basis. We have regular conversations with civil rights orgs multiple times a year.

Mr. RUSH. Mr. Dorsey, where is the audit that Members of Congress, including the chairman of the committee—where is the audit that we asked you and you agreed to forward?

Mr. DORSEY. We don't have it. We sought a different approach with—

Mr. RUSH. I don't have it either, and I thought that you were being very, very disingenuous. As a matter of fact, I thought that you had lied to the committee and you should be condemned for that. And I can't wait until we come up with legislation that will deal with you and your cohorts in a very, very effective way. This was nothing but an empty promise that you made.

You haven't taken this issue seriously, and Mr. Dorsey I as a black man in America, my experiences are different from your experiences. This audit is very, very important to me and to those who are similarly situated just as I am. Facebook, to their credit, has completed an audit. And there is no reason, simply no reason under the sun, that corporation as large as yours should not have completed that audit.

Mr. Dorsey, has Twitter evaluated the disparate impact from COVID-19 misinformation on the African American community, and simply has not even attempted to identify messages to combat COVID-19 misinformation targeted at African Americans and emphasized reliable, trustworthy medical information?

Mr. DORSEY. Yes on both. And we review with civil rights orgs on a regular basis. That is the solution we chose.

Mr. DOYLE. The gentleman's time is expired.

The Chair now recognizes Mr. Upton for 5 minutes.

Mr. UPTON. Thank you, Mr. Chairman.

As I listen to this hearing, like it or not, it sounds like everybody on both sides of the aisle is not very happy. I think we all believe that there is a lot of responsibility that should be shared for some of the issues that we have raised today by the three of you. And I would just offer—or speculate, I guess you could say—that we are going to see some changes in Section 230.

The President, former President Trump, vetoed a pretty big bill, the defense bill, earlier last year over this very issue because he wanted the total repeal and he didn't get it. But I know that the Senate now has got some legislation that is pending that is looking at a couple reforms. And my sense is that we may see something here in the near future as well.

I serve as one of only two House members on the Commission on Combating Synthetic Opioid Trafficking. It is a multi-Federal agency. It is cochaired by David Trone in the House and Tom Cotton in the Senate. And there is a lot of concern that we all have, not only as parents but as community leaders across the country, on opioids and the inability to remove illegal offers of opioids, steroids, even fake COVID-19 vaccines. Very troubling, I think, as we see

some of these platforms push such content to a user in real search of it.

So I guess my first question is to you, Mr. Zuckerberg. The sale of illegal drugs on your platform does violate your policy, yet it does remain a problem on your platforms. Can you explain the resources that you currently have devoted to addressing the issue and whether or not you plan to develop more? And this is an issue that I intend to raise with the Commission as we look forward to this in the next number of months.

Mr. ZUCKERBERG. Thanks, Congressman. I think this is an important area and a good question. We have more than a thousand engineers who work on our what we call integrity systems that basically are AI systems that try to help find content that violates our policies. You are right that that content does violate our policies. And we also have more than 35,000 people who work in content review who basically are either responding to flags that they get from the community or checking things that our AI systems flag for them but are unsure about.

And this is an area—and when we are talking about reforming Section 230—where I think it would be reasonable to expect that large platforms, especially, build effective systems to be able to combat and fight this kind of clearly illegal content. I think that there will be a lot of ongoing debate about how to handle content which people find distasteful or maybe harmful but is legal. But in this case, when the content is illegal, I think it is pretty reasonable to expect that large platforms build effective systems for moderating this.

Mr. UPTON. So we saw earlier this week—of course, we don't know all the facts on this terrible shooting in Boulder, Colorado. It appears, at least some of the initial reports, that the alleged shooter was in fact bullied, and I think I saw some press reports that some of it had happened online as well.

What process do you have that would allow parents or families to be able to pursue antibullying efforts that might be on your platforms?

Mr. ZUCKERBERG. Thanks, Congressman. I think bullying is a really important case to consider for Section 230 because, first of all, it is horrible, and we need to fight it, and we have policies that are against it. But it also is often the case that bullying content is not clearly illegal.

So when we talk about needing the ability under something like Section 230 to be able to moderate content which is not only clearly illegal content but broader, one of the primary examples that we have in mind is making sure that we can stop people from bullying children. And here we work with a number of advocacy groups. We work with law enforcement to help fight this. This is a huge effort and part of what we do, and I think it is extremely important.

Mr. UPTON. And other than taking the approach that you don't want to see any changes to 230, what suggestions might you have for us as we examine this issue?

Mr. ZUCKERBERG. Sorry, Congressman. I am not saying that I don't think that there should be changes. I am saying that I think 230 still broadly is important, so I wouldn't repeal the whole thing.

But the three changes that I have basically suggested are—one is around transparency, that large platforms should have to report on a regular cadence, for each category of harmful content, how much of that harmful content they are finding and how effective their systems are at dealing with it.

The second thing I think that we should do is hold large platforms to a standard where they should have effective systems for handling clearly illegal content, like opioids or child exploitation or things like that.

And the threshold thing that I think is an important principle is that these policies really do need to apply more to large platforms. And I think we need to find a way to exempt small platforms, so that way—when I was getting started with Facebook, if we had gotten hit with a lot of lawsuits around content, it might have been prohibitive for me to get started. And I think none of us here want to see the next set of platforms from being stopped from kind of being able to get started and grow.

Mr. DOYLE. The gentleman's time is expired.

The Chair now recognizes Ms. Eshoo.

Ms. ESHOO. Am I unmuted? Thank you, Mr. Chairman. And good morning—well, it is still—we are Californians, so it is good morning for us.

I want to start by saying that content moderation, like removing posts or banning accounts, is about treating symptoms. And I think that we need to treat symptoms, but I also think that we need to address two underlying diseases. The first is that your products amplify extremism. The second is that your business models of targeted ads enable misinformation to thrive because you chase user engagement at great cost to our society.

So to Mr. Pichai, last month the Anti-Defamation League found that YouTube amplifies extremism. Scores of journalists and researchers agree. And here is what they say happens: A user watching an extremist video is often recommended more such videos, slowly radicalizing the user. YouTube is not doing enough to address recommendations, and it is why Representative Malinowski and myself introduced the Protecting Americans from Dangerous Algorithms Act to narrowly amend Section 230 so courts can examine the role of algorithmic amplification that leads to violence.

And it is also why I, along with 40 of my House colleagues, wrote to each of you about this issue. And Mr. Chairman, I ask that those letters be placed into the record.

[The letters appear at the conclusion of the hearing.]

Ms. ESHOO. So my question to you, Mr. Pichai, is: Are you willing to overhaul YouTube's core recommendation engine to correct this issue? Yes or no?

Mr. PICHAI. Congresswoman, we have overhauled our recommendation systems, and I know you have engaged on these issues before, pretty substantially in pretty much any area.

Ms. ESHOO. Now, Mr. Pichai, yes or no, because we still have a huge problem. And I outlined what they—are you saying that the Anti-Defamation League doesn't know what they are talking about? All these journalists and researchers? There is a lot more to address. And that is why I am asking you if you are willing to over-

haul YouTube's core recommendation engine to correct this. It is serious. It is dangerous. What more can I say about it? Yes or no?

Mr. PICHAI. Congresswoman, if I may explain, we have—

Ms. ESHOO. No. I don't have time to explain. So we—let me just say this to the witnesses. We don't do filibuster in the House. That is something that is done in the Senate. So a filibuster doesn't work with us.

To Mr. Zuckerberg, your algorithms use unseemly amounts of data to keep users on your platform because that leads to more ad revenue. Now, businesses are in business to make money. We all understand that. But your model has a cost to society. The most engaging posts are often those that induce fear, anxiety, anger, and that includes deadly, deadly misinformation.

The Center for Countering Digital Hate found that the Explore and Suggested Posts parts of Instagram are littered with COVID misinformation, election disinformation, and QAnon posts. So this is dangerous, and it is why Representative Schakowsky and I are doing a bill that is going to ban this business model of surveillance advertising.

So are you willing to redesign your products to eliminate your focus on addicting users to your platforms at all costs? Yes or no?

Mr. ZUCKERBERG. Congresswoman, as I said before, the teams that design our algorithm—

Ms. ESHOO. Never mind. I think—let me just say this, and I think it is irritating all of us, and that is that no one seems to know the word "yes" or the word "no." Which one is it? If you don't want to answer, just say, "I don't want to answer." So yes or no?

Mr. ZUCKERBERG. Congresswoman, these are nuanced issues and—

Ms. ESHOO. OK. So I am going to say that is a no.

To Mr. Dorsey, as chairwoman of the Health Subcommittee I think that you need to eliminate all COVID misinformation—and not label or reduce its spread, but remove it. I looked at a tweet this morning. Robert Kennedy, Jr., links the death of baseball legend Hank Aaron to the COVID vaccine even though fact-checkers debunked the story. The tweet has 9,000 retweets.

Will you take this down, and why haven't you? And also, why haven't you banned the 12 accounts that are spewing this deadly COVID misinformation? This could cost lives.

Mr. DORSEY. No, we won't take it down because it didn't violate our policy. So we have a clear policy in place—

Ms. ESHOO. What kind of policy is that? Is it a policy for misinformation?

Mr. DORSEY. No.

Mr. DOYLE. The gentlelady's time is expired.

The Chair recognizes Mr. Scalise. Is Mr. Scalise here?

Mr. SCALISE. Thank you.

Mr. DOYLE. Ah, there we go.

Mr. SCALISE. Yes. Thank you, Mr. Chairman. I want to thank you for having this hearing. I want to thank our three witnesses for coming as well. Clearly, you are seeing a lot of concern being expressed by Members on both sides, both Republican and Democrat, about the way that your social media platforms are run, and

especially as it relates to the fairness and equal treatment of people.

I know I have had a lot of concerns, shared it with some of you individually over the last few years about whether it is algorithms that seem to be designed sometimes to have an antibias against conservatives. But look, we all agree that whether it is illegal activity, bullying, those things ought not to be permeated through social media.

There is a big difference between stopping bullying and violent type of social media posts versus actual censorship of political views that you disagree with. And I want to ask my first question to Mr. Dorsey, because there have been a lot of concerns expressed recently about that unequal treatment. And I will just start with the New York Post article.

I think a lot of people have seen this. This article was censored by Twitter when it was originally sent out. This is the New York Post, which is a newspaper that goes back to 1801, founded by Alexander Hamilton. And for weeks, this very credibly sourced article, right before an election, about Hunter Biden was banned by Twitter.

And then when you contrast that, you have this Washington Post article that was designed to misportray a conversation between President Trump and the Georgia secretary of state that has since been—parts of this have been debunked. And yet this article can still be tweeted out.

I want to ask Mr. Dorsey: First of all, do you recognize that there is this real concern that there is an anticonservative bias on Twitter's behalf? And would you recognize that this has to stop if this has going to be—Twitter is going to be viewed by both sides as a place where everybody is going to get a fair treatment?

Mr. DORSEY. We made a total mistake with the New York Post. We corrected that within 24 hours. It was not to do with the content. It was to do with the hacked materials policy. We had an incorrect interpretation. we don't write policy according to any particular political leaning. If we find any of it, we root it out.

Mr. SCALISE. So we are regarding the Washington Post—

Mr. DORSEY. We will make mistakes. We will make mistakes, and our goal is to correct them as quickly as possible. And in that case, we did.

Mr. SCALISE. And I appreciate you recognizing that was a mistake. However, the New York Post's entire Twitter account was blocked for about 2 weeks where they couldn't send anything out, not just that article. And to censor—we have got a First Amendment too. It just seems like to censor a newspaper that is as highly respected as the New York Post—again, 1801, founded by Alexander Hamilton—for their entire account to be blocked for 2 weeks by a mistake seems like a really big mistake.

Was anyone held accountable in your censoring department for that mistake?

Mr. DORSEY. Well, we don't have a censoring department. But I agree. Like it—

Mr. SCALISE. Well, who made the decision, then, to block their account for two weeks?

Mr. DORSEY. We didn't block their accounts for 2 weeks. We required them to delete the tweet, and then they could tweet it again. They didn't take that action, so we corrected it for them. That was—

Mr. SCALISE. Even though the tweet was accurate. I mean, are you now—look, you have seen the conversations on both sides about Section 230, and there is going to be more discussion about it. But you are acting as a publisher if you are telling a newspaper that they have got to delete something in order for them to be able to participate in your account.

I mean, don't you recognize that that—you are no longer hosting a town square. You are acting as a publisher when you do that.

Mr. DORSEY. It was literally just a process, sir. This was not against them in any particular way. We require—if we remove a violation, we require people to correct it. We changed that based on their not wanting to delete that tweet, which I completely agree with. I see it. But it is something we learned. We learned to—

Mr. SCALISE. OK. Well, let me go to the New York—now let me go to the Washington Post article because this article can still be tweeted. I don't know if it was ever taken down. It contains false information. Even the Washington Post acknowledges that it contains false information. Yet their tweets today on your service that still mischaracterize it in a way where even the Washington Post admitted it is wrong, yet those mischaracterizations can still be retweeted.

Will you address that and start taking those down to reflect what even the Washington Post themselves has admitted is false information?

Mr. DORSEY. Our misleading information policies are focused on manipulated media, public health, and civic integrity. That is it. We don't have a general—

Mr. SCALISE. I would hope that you would go and take that down. And look. I know you said in your opening statement, Mr. Dorsey, that Twitter is running a business, and you said, "A business wants to grow the customers it serves." Just recognize if you become viewed and continue to become viewed as an anticonservatively biased platform, there will be other people that step up to compete and ultimately take millions of people from Twitter. I would hope you recognize that.

And I would yield back the balance of my time.

Mr. DOYLE. The gentleman's time is expired.

The Chair now recognizes Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. Thank you, Mr. Chairman.

Mr. Zuckerberg, last year in response to the police killing of George Floyd, you wrote a post on your Facebook page that denounced racial bias. It proclaimed, "Black Lives Matter." You also announced that the company would donate \$10 million to racial justice organizations.

And Mr. Dorsey, Twitter changed its official bio to a Black Lives Matter tribute, and you pledged \$3 million to an antiracism organization started by Colin Kaepernick. And Mr. Pichai, your company held a companywide moment of silence to honor George Floyd, and you announced \$12 million in grants to racial justice organizations.

The CEO of Google subsidiary YouTube wrote in a blog post, “We believe Black Lives Matter and we all need to do more to dismantle systematic racism.” YouTube also announced it would start a \$100 million fund for black creators.

Now, all of this sounds nice. But these pronouncements, gentlemen, these pronouncements and money donations do not address the way your companies’ own products, Facebook, Twitter, and YouTube, have been successfully weaponized by racists and are being used to undermine social justice movements, to suppress voting in communities of color, and spread racist content and lies.

And so, gentlemen, in my view—in my view your companies have contributed to the spread of race-based extremism and voter suppression. As the New York Times noted last year, “It is as if the heads of McDonald’s, Burger King, and Taco Bell all got together to fight obesity by donating to a vegan food co-op rather than lowering their calories.”

Gentlemen, you could have made meaningful changes within your organizations to address the racial biases built into your products and donated to these organizations. But instead, we are left with platitudes and another round of passing the buck.

America is watching you today. This is a moment that begins a transformation of the way you do business, and you must understand that. Perhaps a lack of diversity within your organizations has contributed to these failures. The Congressional Black Caucus’s Tech 2025 initiative has been working for years to increase diversity and equity in tech companies at all levels, and you know that because we have visited with you in California.

We founded this initiative in 2015 with the hope that by now the tech workforce would reflect the diversity of our country. Here we are, 2021. I acknowledge that you have made some modest advancements, but not enough. There must be meaningful representation in your companies to design your products and services in ways that work for all Americans.

And that requires public accountability. History has shown that you have talked the talk but have failed to walk the walk. It appears now that Congress will have to compel you—compel you, perhaps with penalties—to make meaningful changes.

And I am going to try the yes-or-no answer, and hopefully I will have better results than my colleagues.

Mr. ZUCKERBERG, I will start with you, and please be brief. Yes or no: Would you oppose legislation that would require technology companies to publicly report on workforce diversity at all levels?

Mr. ZUCKERBERG. Congressman, I don’t think so, but I need to understand it in more detail.

Mr. BUTTERFIELD. Well, we will talk about that. And I hope that, if we introduce this legislation, you will not oppose it.

What about you, Mr. Dorsey? Would you oppose a law that made workforce diversity reporting a requirement?

Mr. DORSEY. No, I wouldn’t oppose it. It does come with some complications in that we don’t always have all the demographic data for our employees.

Mr. BUTTERFIELD. Well, thank you for that, and we talked with you in your office some years ago and you made a commitment to work with us, but we need more.

What about you, Mr. Pichai? Are you willing to support—would you be willing to commit to—would you oppose a law that made workforce diversity reporting a requirement? Would you oppose it?

Mr. PICHAI. Congressman, we were the first company to publish transparency reports. We publish it annually. And so, happy to share that with you and take any feedback. But we do today provide, in the U.S., detailed demographic information on our workforce, and we are committed to doing better.

Mr. BUTTERFIELD. Well, gentlemen, for the last 6 years, the Congressional Black Caucus has said to you over and over again we need greater diversity among your workforce from the top to the bottom, and we need for you to publish the data so the world can see it. That is the only way we are going to deal with diversity and equity.

Thank you so very much, Mr. Chairman. I heard you at the beginning of the committee gavel, and I yield back the 10 seconds that I have.

Mr. DOYLE. The gentleman deserves commendation for doing that, and I hope others follow his example.

The Chair now recognizes Mr. Guthrie for 5 minutes.

Mr. GUTHRIE. Thank you, Mr. Chair, and thanks to the witnesses for being here.

And Big Tech decisions have real impact on people, and that is why I ask my constituents, using your platforms, to share their experiences on your platforms with me as their representative. And I am here to advocate on their behalf. I received 450 responses, and one major thing that I heard from my constituents was the experience they have had with sites taking down religious content, which is important because a lot of religious organizations are now streaming their services due to COVID.

I did have one instance where a constituent wrote to me—and this is what she posted—“I am thankful God’s grace is new every morning.” And then Facebook took it down, and then my constituent said she got a notice from Facebook that it violated their policies around hate.

And so I just want to discuss about this. I can ask you yes-or-no questions, Mr. Zuckerberg, on that, but I just want to talk about it a little bit. One is, it seems, I know that we don’t want extreme language on the internet. I am with you on that. And you cannot watch everything. And so you use algorithms to find that, so algorithms will flag things, some that are clearly obvious and some that you would say probably shouldn’t have been flagged.

But it seems to me that it seems to be biased in that direction. And so instead of just giving you a yes-or-no question, I want to read that quote again. And I sort of know a little bit about math, not a lot but a little bit, about within that quote, what in there would get tripped up, with this quote get tripped up and put into the flagged category?

And as it says, “I am thankful God’s grace is new every morning.” And so I guess the question is what word or thought do you think would trip an algorithm for that quote, Mr. Zuckerberg?

Mr. ZUCKERBERG. Congressman, it is not clear to me why that post would be a problem. I would need to look into it in more detail. Sometimes the systems look at patterns of posting, so if some-

one is posting a lot, then maybe our system thinks it is spam. But I would need to look into it in more detail.

Overall, the reality is that any system is going to make mistakes. There is going to be content that we take down that we should have left up, and there is going to be content that we missed that we should have taken down that we didn't catch or that the system has made a mistake on. And at scale, unfortunately, those mistakes can be a large number even if it is a very small percent.

But that is why, when we are talking about things like Section 230 reform, I think it is reasonable to expect large companies to have effective moderation systems but not reasonable to expect that there are never any errors. But I think that transparency can help hold the companies accountable as to what accuracy and effectiveness they are achieving.

Mr. GUTHRIE. OK. Then, well, to your spam comment, I think they did receive a notify it was for the hate policy. And I understand there are going to be gray areas, whatever. But that quote, I don't see where the gray area is as to how it could get caught up in that.

Mr. ZUCKERBERG. I agree.

Mr. GUTHRIE. But I want to move on. Thanks for your answer with that. I want to move on.

So Mr. Dorsey, I want to talk about the RFK, Jr. I didn't see that quote, but you said that didn't violate your policy. And just in the context of that, I know CDC just recently updated its school guidance to make clear science says you can be 3 feet away and still be safe in schools. The issue—things are changing every day because we are learning more and more about this virus.

So how did the RFK comment not violate your policy—RFK, Jr.? And how did—we have an RFK III that we all—and JFK and JPK III I guess we all like as a former colleague. But RFK, Jr., and the policy towards that. And then how do you keep up with what's changing so quickly, Mr. Dorsey?

Mr. DORSEY. We can follow up with you on the exact reasoning. But we have to recognize that our policies evolve constantly, and they have to evolve constantly. So, as has been said earlier in this testimony, we observe what is happening as a result of our policy. We have got to understand the ramifications. And we improve it. And it is a constant cycle. We are always looking to improve our policies and our enforcement.

Mr. GUTHRIE. So Mr. Zuckerberg, Mr. Pichai, just on all that continuously evolving information on COVID because we are learning more and more about it, how do you keep up? We only have about 30 seconds, so if you could—quick answers for each of you, if you can. Mr. Pichai, maybe, since you haven't answered a question.

Mr. PICHAI. Yes. On COVID we have been really taking guidance from CDC and other health experts, proactively removing information. One thing we get to do in YouTube is to recommend higher quality content. We have shown 400 billion information panels on COVID alone last year, including a lot from CDC and other health organizations.

Mr. GUTHRIE. OK. Thank you, and I will yield back 4 seconds, Mr. Chair.

Mr. DOYLE. Thank you, Mr. Guthrie.

The Chair now recognizes Ms. Matsui for 5 minutes.

Ms. MATSUI. Thank you very much, Mr. Chairman, for having this hearing today.

Today we have another opportunity, hearing from the leaders of Facebook, Twitter, and Google, in what has become a concerning pattern. The members of this committee are here to demand answers to questions about social media's role in escalating misinformation, extremism, and violence.

Last week I testified at a House Judiciary Committee hearing about the rise in discrimination and violence against Asian Americans. Horrifically, that hearing came on the heels of a violent attack in Atlanta that left eight people, six of them Asian women, dead.

The issues we are discussing here are not abstract. They have real-world consequences and implementations that are too often measured in human lives. I am worried, as are many watching this hearing, that the companies before us today are not doing enough to prevent the spread of hate, especially when it is targeted against minority communities. Clearly the current approach is not working, and I think Congress must revisit Section 230.

A recent study from the University of San Francisco examined nearly 700,000 tweets in the week before and after President Trump tweeted the phrase "Chinese virus." The results showed two alarming trends: There was a significantly greater increase in hate speech the week after the President's tweet, and that half of the tweets using the hashtag #chinavirus showed an anti-Asian sentiment compared to just one-fifth of the tweets using the hashtag #covid19.

This empirical evidence backs up what the World Health Organization already knew in 2015, saying, "Disease names really do matter. We have seen certain disease names provoke a backlash against members of particularly religious or ethnic communities." Despite this, Facebook and Twitter are still allowing hashtags like #chinavirus, #kungflu, and #wuhanvirus to spread.

Mr. Zuckerberg and Mr. Dorsey, given the clear association between this type of language and racism or violence, why do you still allow these hashtags on your platforms? Anyone answer that, or is that not answerable?

Mr. DORSEY. I think we were waiting for you to call on one of us. We do have policies against hateful conduct, and that includes the trends, so when we see associated with any hateful conduct, we will take action on it. It is useful to remember that a lot of these hashtags, though, do contain counterspeech, and people on the other side of it do own them and show why this is so terrible and why it needs to—

Ms. MATSUI. Can I just take my time back? The fact of the matter is I think you know how to develop algorithms to kind of get rid of this and examine this further.

Mr. Zuckerberg, any comment here?

Mr. ZUCKERBERG. Thanks, Congresswoman. The rise in anti-Asian hate is a really big issue and something that I do think that we need to be proactive about. I agree with the comments that Jack made on this. On Facebook, any of that context, if it is com-

bined with something that is clearly hateful, we will take that down. It violates the hate speech policy.

But one of the nuances that Jack highlighted that we certainly see as well in enforcing hate speech policy is that we need to be clear about when someone is saying something because they are using it in a hateful way versus when they are denouncing it. And this is one of the things that has made it more difficult to operationalize this at scale.

Ms. MATSUI. Well, reclaiming my time, I think this gives us an opportunity to really look at hate speech, what it really means, particularly in this day and age when we have many instances of these things happening. Hate speech on social media can be baked in, and unfortunately this also is a trend that maybe happened years and years ago, which it might have just been a latent situation.

But with social media, it travels all around the world and it hurts a lot of people. And my feeling, and I believe a lot of other people's feeling, is that we really have to look at how we define hate speech. And you all are very brilliant people, and you hire brilliant people. I would think that there is a way for you to examine this further and take it one step lower to see if it is something that is legitimate or not.

And I really feel that this is a time, especially now when we are examining platforms and what you can do and should do, and as we are examining here in this committee and as we write legislation, we really want to have the entire multitude of what can and can't be done.

So with that, Mr. Chairman, I only have 11 seconds left, and I yield back. Thank you.

Mr. DOYLE. Thank you. The gentlelady yields back.

Let's see. The Chair now recognizes Mr. Kinzinger for 5 minutes.

Mr. KINZINGER. Thank you, Mr. Chairman, and thank you all for being here. In all this conversation it is good to have, I think we also have to recognize that we need to—we are lucky to have all these companies located in the United States. When we talked about the issues and concerns, for instance, with TikTok, we can see that a lot of these companies could easily leave here and go elsewhere and then we would have far less oversight.

I think the crackdown on January 6 was correct. I think we need to be careful to not use that as a way to deflect from what led to January 6th, the pushing of this narrative of Stop the Steal. I think there are folks that are concerned, though, that we also need to make sure that those same levels of protection exist when you talk about like Iran, for instance, and what the leaders there tweet. But let me go into specific questions.

Over the years we have obviously seen the rise of disinformation. It is not new. I remember getting disinformation in the 1990s. But we have seen it spread on these platforms. So we live in a digital world where many people get their news and entertainment from the internet, from articles and posts that are often based off algorithms that can cater to what people see and read.

So those constant News Feeds have simply reinforced people's beliefs, or worse, that they can promote disgraceful and utterly ridiculous conspiracy theories from groups like QAnon. Extremism and

violence have grown exponentially as a result, and we know it is true specifically after January 6.

So Mr. Zuckerberg, let me ask you: According to Hany Farid at Berkeley, numerous external studies and some of your own internal studies have revealed that your algorithms are actively promoting divisive, hateful, and conspiratorial content because it engages users to spend more time.

Do you think those studies are wrong? And if not, what are you guys doing to reverse course on that?

Mr. ZUCKERBERG. Sure. Thank you, Congressman. This is an important set of topics.

In terms of groups, we stopped recommending all civic and political groups even though I think a lot of the civic and political groups are healthy, because we were seeing that that was one vector that there might be polarization or extremism, and groups might start off with one set of views but migrate to another place. So we have removed that completely. And we did it first as an exceptional measure during the election; and since the election we have announced that we are going to extend that policy indefinitely.

For the rest of the content in News Feed and on Instagram, the main thing that I would say is I do think that there is quite a bit of misperception about how our algorithms work and what we optimize for. I have heard a lot of people say that we are optimizing for keeping people on the service.

The way that we view this is that we are trying to help people have meaningful social interactions. People come to social networks to be able to connect with people. If we deliver that value, then it will be natural that people use our services more. But that is very different from setting up algorithms in order to just kind of try to tweak and optimize and get people to spend every last minute on our service, which is not how we designed the company or the services.

Mr. KINZINGER. Thanks. I don't mean to interrupt you. I do have another question.

Mr. Chairman, I want to ask unanimous consent to insert for the record an article from the Wall Street Journal titled "Facebook Executives Shut Down Efforts to Make the Site Less Divisive."

[The article appears at the conclusion of the hearing.]

Mr. KINZINGER. Let me move on to the next one. For years I have called for increased consumer protection from companies on fake accounts and bad actors who use them to exploit others. This issue affected me personally. In 2015, a woman from India spent all of her money on a flight to come see me because she claimed to have developed a relationship with me over Facebook.

In 2019 I sent you, Mr. Zuckerberg, a letter highlighting the issue, and your team provided a relatively inadequate response. Since then, I have introduced two pieces of legislation, Social Media Accountability and Account Verification Act, and the Social Media Fraud Mitigation Act, both of which aim to curb this activity.

So Mr. Zuckerberg, the last time you came before us, you stated that Facebook has a responsibility to protect its users. Do you feel that your company is living up to that? And further, what have you done to remove those fake accounts?

Mr. ZUCKERBERG. Thanks. So fake accounts are one of the bigger integrity issues that we face. I think in the first half of—well, in the last half of last year, we took down more than a billion fake accounts, just to give you a sense of the volume, although most of those our systems are able to identify within seconds or minutes of them signing up because the accounts just don't behave in a way that a normal person would in using the service.

But this is certainly one of the highest-priority issues we have. We see a large prevalence of it. Our systems, I think, at this point are pretty effective in fighting it, but they are not perfect, and there are still a few percent that get through. And it is a big issue and one we will continue working on.

Mr. KINZINGER. Thank you. I would love to ask the rest—the others a question, but I don't have time. So I yield back, Mr. Chairman. Thank you for your attention.

Mr. DOYLE. I thank the gentleman.

The Chair now recognizes Ms. Castor for 5 minutes.

Ms. CASTOR. Well, thank you, Mr. Chairman.

Gentlemen, since you were last here in front of the committee, the illegal activities, the expanse of unwitting Americans, the rampant misinformation on your platforms, have gotten worse. Part of the reason for this toxic stew is that you employ manipulative methods to keep people cemented to the platform, often amplifying discord. And it boosts your bottom line. You enjoy an outdated liability shield that incentivizes you to look the other way or take half-measures while you make billions at the expense of our kids, our health, the truth, and now we have seen the very foundation of our democracy.

I have been working for over a year with advocates and other members on an update to the children's protections online. You all know the tracking and manipulation of children under age 13 is against the law, but Facebook, Google, YouTube, and other platforms have broken that law or have found ways around it. Many have been sanctioned for knowingly and illegally harvesting personal information of children and profiting from it.

I have a question for each of you, just a quick yes or no: Did you all watch "The Social Dilemma," where former employees of yours or other Big Tech platforms say they do not allow their kids on social media? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congresswoman, I haven't seen it—

Ms. CASTOR. Yes or—

Mr. ZUCKERBERG [continuing]. But I am obviously familiar with it.

Ms. CASTOR. OK. Mr. Pichai? Yes or no?

Mr. PICHAI. Yes. I have seen the movie.

Ms. CASTOR. And—

Mr. DORSEY. No. No.

Ms. CASTOR. OK. Well, Mr. Zuckerberg, there is a good reason that they have the former execs say that. Are you aware of the 2019 Journal of the American Medical Association pediatric study that the risk of depression for adolescents rises with each daily hour spent on social media? And I am not talking screen time. I am not talking about Facetime or sending text messages to friends. But are you aware of that research?

Mr. ZUCKERBERG. Congresswoman, I am not aware of that research.

Ms. CASTOR. All right. What about the 2019 HHS research that suicide rates among kids aged 10 to 14 increased by 56 percent between 2007 and 2017 and tripled—tripled—for kids between the age of 10 and 14? Yes or no?

Mr. ZUCKERBERG. Congresswoman, I am aware of the issue—

Ms. CASTOR. Yes. So yes. Certainly you are also aware of the research that indicates a correlation between the rise in hospital admissions for self-harm and the prevalence of social media on phones and the apps on platforms that are designed to be addictive and keep kids hooked. Yes?

[No response.]

Ms. CASTOR. Well, how about you, Mr. Pichai? Are you aware of the JAMA pediatric September 2020 study where they tested hundreds of apps used by children aged 5 and under, many of which were in the Google Play Store's family section? The study found 67 percent of the apps tested showed transmission of identifying info to third parties in violation of the COPPA law? Are you familiar?

Mr. PICHAI. Extensively spent time on this area. We introduced a curated set of apps for kids on the Play Store. We give digital well-being tools so that people can take a break, set time patterns, can set time limits for children. So the concept of—

Ms. CASTOR. Let me ask you this, then, Mr. Pichai: How much are you making in advertising revenue from children under the age 13?

Mr. PICHAI. Most of our products other than a specific product designed for kids, YouTube—most of our products are not eligible for children under the age of 13.

Ms. CASTOR. Yes. So you are not going to provide that.

Mr. Zuckerberg, how much advertising revenue does Facebook—do you make from behavioral surveillance advertising targeted towards kids under age 13?

Mr. ZUCKERBERG. Congresswoman, it should be none of it. We don't allow children under the age of 13—

Ms. CASTOR. Are you—

Mr. ZUCKERBERG [continuing]. On the services that run advertising.

Ms. CASTOR. Oh, are you saying that there are no kids on Instagram under the age of 13 right now?

Mr. ZUCKERBERG. Congresswoman, children under the age of 13 are not allowed on Instagram. When we find out that they are there—

Ms. CASTOR. No. That is not the answer. I think, of course, every parent knows that there are kids under the age of 13 on Instagram. And the problem is that you know it, and you know that the brain and social development of our kids is still evolving at a young age. There are reasons in the law that we set that cutoff at 13. But now, because these platforms have ignored it, they have profited off of it, we are going to strengthen the law. And I encourage all of my colleagues to join in this effort. I have heard a lot of bipartisan support here today.

We also need to hold the corporate executives accountable and give parents the tools that they need to take care and protect their kids.

Thank you, Mr. Chairman. I yield back.

Mr. DOYLE. The gentlelady's time is expired.

The Chair recognizes Mr. Johnson for 5 minutes.

Mr. JOHNSON, Thanks, Mr. Chairman.

Over a decade ago, Americans watched Facebook, Twitter, and Google emerge from humble beginnings. We were curious to see how these new, innovative companies would improve our lives. The results are in, and they are deeply concerning.

We have seen a surge in cyberbullying, child porn, radical extremism, human trafficking, suicides, and screen addiction, all of which have been linked to the use of social media. Our Nation's political discourse has never been uglier, and we haven't been this divided since the Civil War.

Yet Big Tech marches on uninhibited. What is their newest target? Children under the age of 13. News outlets this week have reported that Facebook is planning to create an Instagram app designed for children under the age of 13. We have talked about it here already today. Elementary and middle school students.

By allowing Big Tech to operate under Section 230 as is, we will be allowing these companies to get our children hooked on their destructive products for their own profit. Big Tech is essentially handing children a lit cigarette and hoping they stay addicted for life.

In 1994, Democratic Congressman Henry Waxman chaired a hearing with the CEOs of our Nation's largest tobacco companies. During his opening statement, he stated, and I quote, "Sadly, this deadly habit begins with our kids. In many cases they become hooked quickly and develop a lifelong addiction that is nearly impossible to break."

So, Mr. Zuckerberg and Mr. Dorsey, you profit from your company's hooking users to your platforms by capitalizing on their time. So yes or no: Do you agree that you make money off of creating an addiction to your platforms? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congressman, no. I don't agree with that.

Mr. JOHNSON. OK. Thank you. Thank you.

Mr. ZUCKERBERG. What we do is—

Mr. JOHNSON. That is what I needed, a yes or a no, because you do.

Mr. Dorsey?

Mr. DORSEY. No.

Mr. JOHNSON. OK. All right. Let me go on.

Chairman Waxman went on to say, and I quote, "For decades, the tobacco companies have been exempt from the standards of responsibility and accountability that apply to all other American corporations. Companies that sell aspirin, cars, and soda are all held to strict standards when they cause harm, and that we demand that when problems occur, corporations and their senior executives be accountable to Congress and the public. This hearing marks the beginning of a new relationship between Congress and the tobacco companies." That is what Chairman Waxman said in 1994.

So For all three of you, Mr. Zuckerberg, Mr. Dorsey, and Mr. Pichai: Do you agree that the CEOs that—as the CEOs of major tech companies, you should be held accountable to Congress and the public? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congressman, I think we are accountable to Congress and to the public.

Mr. JOHNSON. Do you think you should be held accountable?

Mr. ZUCKERBERG. I am not sure I understand what you mean, but I think so.

Mr. JOHNSON. It is an easy question. Should you be held accountable—

Mr. ZUCKERBERG. Yes.

Mr. JOHNSON [continuing]. To Congress and the public for the way you run your business?

Mr. ZUCKERBERG. Yes. And we are.

Mr. JOHNSON. OK. All right. Thank you.

Mr. Dorsey?

Mr. DORSEY. Yes. Accountable to the public.

Mr. JOHNSON. OK. Accountable—no. I said accountable to Congress and the public. We represent the public. So you agree?

Mr. DORSEY. Yes.

Mr. JOHNSON. OK. Thank you. Mr. Pichai?

Mr. PICHAI. Yes. I am here today because I am accountable to Congress and members of the public.

Mr. JOHNSON. OK. Great. Well, gentlemen, let me tell you this, and I think I have heard it mentioned by several of my other colleagues. There is a lot of smugness among you. There is this air of untouchability in your responses to many of the tough questions that you are being asked.

So let me tell you all this. All of these concerns that Chairman Waxman stated in 1994 about Big Tobacco apply to my concerns about Big Tech today, about your companies. It is now public knowledge that former Facebook executives have admitted that they use the tobacco industry's playbook for addictive products. And while this is not your first hearing in front of Congress, I can assure you that this hearing marks a new relationship between all of us here today. There will be accountability.

Mr. Chairman, I yield back.

Mr. DOYLE. I thank the gentleman. He yields back.

The Chair now recognizes Mr. McNerney for 5 minutes.

Mr. MCNERNEY. I want to thank the chair for organizing this hearing, and I thank the participants. This is a lot of work on your behalf and a long day for you. I appreciate that.

Are you all aware that your platforms are behemoths, and that the Americans are demanding that we step in and rein in your platforms both in terms of how you handle our data and how platforms handle disinformation that causes real harm to Americans and to the democracy itself?

I understand the tension you have between maximizing your profits by engaging to your platforms on the one hand and by the need to address disinformation and real harm it causes on the other hand. Your unwillingness to unambiguously commit to enforcing your own policies and removing the 12 most egregious

spreaders of vaccine disinformation from your platforms gets right at what I am concerned about.

Disinformation is a strong driver for engagement, and consequently you too often don't act even though we know you have the resources to do that. There are real harms associated with this. And my questions—I hope I don't appear to be rude—but when I ask for a yes-or-no question, I will insist on a yes-or-no answer.

Mr. Zuckerberg, yes or no: Do you acknowledge that there is disinformation being spread on your platform?

Mr. ZUCKERBERG. Sorry, I was muted. Yes, there is, and we take steps to fight it.

Mr. MCNERNEY. Thank you. Yes or no: Do you agree that your company has profited from the spread of disinformation?

Mr. ZUCKERBERG. Congressman, I don't agree with that. People don't want to see disinformation on our services, and when we do—

Mr. MCNERNEY. So it is no, then.

Mr. ZUCKERBERG [continuing]. I think it hurts our long-term—

Mr. MCNERNEY. You said you don't agree with that. I appreciate your forthrightness on that. But we all know this is happening. Profits are being generated from COVID-19 and vaccine disinformation, election disinformation, QAnon conspiracy theories, just to name a few things. And it is baffling that you have a negative answer to that question. Approximately—well, let's move on to the next issue.

Mr. Zuckerberg, you talked a lot about relying on third-party fact-checkers to combat the spread of disinformation, but you tell us very little about the process. I wrote you a letter nearly 2 years ago asking about it, and you failed to answer my question.

I asked this question again when an executive from your company testified last year, and she failed to answer. I would like to get an answer today. On average, from the time content is posted to Facebook's platform, how long does it take Facebook to flag suspicious content to third-party fact-checkers to review the content and for Facebook to take remedial action after this review is completed? How long does this entire process take? I am just looking for a quick number.

Mr. ZUCKERBERG. Congressman, it can vary. If an AI system identifies something immediately, it can be within seconds. If we have to wait for people to report it to us and have human review, it can take hours or days. The fact-checkers take as much time as they need to review things, but as soon as we get an answer back from them, we should operationalize that and attach a label if the content is rated false and—

Mr. MCNERNEY. I am paying attention on what you are saying. But what I do know is that this process isn't happening quickly enough, and I am very concerned that you aren't motivated to speed things up, because the most problematic content is what gets the most views, and the longer the content stays up, the more help—the more this helps maximize your bottom line and the more harm that it can cause. It is clear that you are not going to make these changes on your own.

This is a question for all of the participants, panelists: Would you oppose legislation that prohibits placing ads next to what you know

to be or should know to be false or misleading information, including ads that are placed in videos, promoted content, and ads that are placed above, below, or on the site of a piece of content?

Mr. Zuckerberg, would you answer with a yes or no first, please?

Mr. ZUCKERBERG. Congressman, that is very nuanced. I think the questions to determine whether something is misinformation is a process that I think would need to be spelled out well in a law like that.

Mr. MCNERNEY. Well, OK. I appreciate that.

Mr. Dorsey?

Mr. DORSEY. Yes. I would oppose it until we see the actual requirements and what the ramifications are. We need to understand that.

Mr. MCNERNEY. OK. And Mr. Pichai, would you oppose a prohibition like this?

Mr. PICHAI. The principle makes sense. In fact, advertisers don't want anywhere or near to be content like that. And so we already have incentives. You can imagine reputable advertisers, like consumer products advertisers, do not want any ads to appear next to information that could turn off their consumers. So we have natural incentives to do the right thing here.

Mr. MCNERNEY. You all say you want a safe and open platform for everyone. You say it is not in your company's interest to have this information on your platform. So you shouldn't oppose efforts that would prevent harming the American people.

I yield back.

Mr. DOYLE. The gentleman's time is expired. The gentleman yields back.

The Chair now recognizes Mr. Long for 5 minutes.

Mr. LONG. Thank you, Mr. Chairman.

Mr. Pichai, I am going to ask you a yes-or-no question, and just tell me if you know the difference in these two words: yes and no?

Mr. PICHAI. Yes.

Mr. LONG. Mr. Zuckerberg, same question for you. Do you know the difference in yes and no?

Mr. ZUCKERBERG. Yes, Congressman.

Mr. LONG. And Mr. Dorsey, same question for you. Do you know the difference in two words, yes or no?

Mr. DORSEY. Yes.

Mr. LONG. I am sorry?

Mr. DORSEY. Yes.

Mr. LONG. Is that a yes? I didn't—

Mr. DORSEY. Yes. I know the difference.

Mr. LONG. Thank you. I want a steak dinner there from one of my colleagues. They didn't think I could get all three of you to answer a yes-or-no question. I did it.

Mr. Zuckerberg, let me ask you: How do you ascertain if a user is under 13 years old?

Mr. ZUCKERBERG. Congressman, on services like Facebook, we have people put in a birthday when they register.

Mr. LONG. That is handy. So a 13-year-old would never—I mean, an 11-year-old would never put in the wrong birthday by 2 years and say they were 13? Is that kind of your policy?

Mr. ZUCKERBERG. Congressman, it is more nuanced than that. But I think you are getting at a real point, which is that people lie. And we have additional systems that try to determine what someone's age might be, so if we detect that someone might be under the age of 13, even if they lied, we kick them off.

But this is part of the reason why we are exploring having a service for Instagram that allows under-13s on, because we worry that kids may find ways to try to lie and evade some of our systems. But if we create a safe system that has appropriate parent controls, then we might be able to get people into using that instead. We are still early in figuring this out, but that is a big part of the theory and what we are hoping to do here.

Mr. LONG. But currently they are now allowed to use Instagram. Correct?

Mr. ZUCKERBERG. That is correct. Our policies do not allow people under the age of 13 to use it.

Mr. LONG. I am from Missouri, the Show Me State. And just to say that no one under 13 can get on to me doesn't pass the Missouri smell test of "show me." So I was thinking with you, Mr. Zuckerberg, you created the Facebook Oversight Board as a way to help hold Facebook accountable. They are currently looking at Facebook's decision to remove President Trump's Facebook account.

If the oversight board determines that Facebook should have left President Trump's account up, what will you do?

Mr. ZUCKERBERG. Congressman, we will respect the decision of the oversight board, and if they tell us that former President Trump's account should be reinstated, then we will honor that.

Mr. LONG. I don't know why people call Attorney General Ashcroft "Attorney General," but when they speak of President Trump, they call him "former President." But I guess I will leave that for another day.

Sticking with you again, Mr. Zuckerberg, my understanding is that the Facebook Oversight Board is comprised of members from all over the world. As you are well aware, the United States has the strictest protections on free speech than any other country.

Since the decisions of the board are being made by a panel rather than the U.S. court of law, how can you assure members of this committee and the American people that the oversight board will uphold free speech and make their decisions based on American laws and principles?

Mr. ZUCKERBERG. Congressman, the members of the oversight board were selected because of their views on free expression and strong support of it. That is why we created the oversight board, to help us defend these principles and to help us balance the different aspects of human rights, including free expression.

But each of the people on the oversight board was selected because of a strong commitment to free expression, and I think the decisions that the oversight board has made so far reflect that.

Mr. LONG. OK. Let me move on to Mr. Dorsey.

Mr. Dorsey, I know you are from the Show Me State also. Have you been vaccinated against COVID-19?

Mr. DORSEY. Not yet.

Mr. LONG. Mr. Pichai, have you been vaccinated against COVID-19?

Mr. PICHAI. Sorry. I missed the question, Congressman?

Mr. LONG. I know. I bore a lot of people. Have you been vaccinated against COVID-19?

Mr. PICHAI. Congressman, I was very fortunate to have received it last week.

Mr. LONG. So you have one shot. You have another one to go? Or is it just Johnson & Johnson, where you just need one?

Mr. PICHAI. I still have one more shot to go.

Mr. LONG. And Mr. Zuckerberg, same question: Have you been vaccinated against COVID-19?

Mr. ZUCKERBERG. I have not yet, but hope to as soon as possible.

Mr. LONG. OK. It is not a personal preference not to get vaccinated, they just haven't got to your age group?

Mr. ZUCKERBERG. That is correct.

Mr. LONG. OK. Thank you. And I just cannot believe Robert Kennedy, Jr., is out there with his antivax stuff and it is allowed to stay up on Twitter.

With that, I yield back.

Mr. DOYLE. The gentleman yields back.

Let's see who is next. I don't see a name. Can staff show us who is next up?

Mr. Welch, you are recognized for 5 minutes.

Mr. WELCH. Thank you, Mr. Chairman.

What we are hearing from both sides of the aisle are enormous concerns about some of the consequences of the development of social media—the algorithmic amplification of disinformation, election interference, privacy issues, the destruction of local news, and also some competition issues. And I have listened carefully, and each of the executives has said that your companies are attempting to face these issues.

But a concern I have is whether, when the public interest is so affected by these decisions and by these developments, ultimately should these decisions be made by private executives who are accountable to shareholders, or should they be made by elected representatives accountable to voters?

So I really have two questions that I would like each of you, starting with Mr. Zuckerberg and then Mr. Pichai and then Mr. Dorsey, to address.

First, do you agree that many of these decisions that are about matters that so profoundly affect the public interest should they be made exclusively by private actors like yourselves who have responsibilities for these major enterprises?

And secondly, as a way forward to help us resolve these issues or work with them, will you support the creation by Congress of a public agency, one like the Federal Trade Commission or the Securities and Exchange Commission, one that had staff that is expert in policy and technology, that has rulemaking and enforcement authority to be an ongoing representative of the public to address these emerging issues? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congressman, I agree with what you are saying, and I have said a number of times that I think that private companies should not be making so many decisions alone that have to balance these complicated social and public equities.

And I think that the solution that you are talking about could be very effective and positive for helping out because what we have seen in different countries around the world is there are lots of different public equities at stake here—free expression, safety, privacy, competition—and these things trade off against each other. And I think a lot of these questions, and the reason why people get upset with the companies, I don't think it is necessarily because the companies are negligent. I think it is because these are complex tradeoffs between these different equities.

And if you—

Mr. WELCH. Pardon my interruption, but I want to go to Mr. Pichai. But thank you, Mr. Zuckerberg.

Mr. PICHAI. Congressman, if your question is—I just want to make sure. Are you asking about whether there should be another agency? I defer to Congress on that. We are definitely subject to a variety of statutes and oversight by agencies like FTC. We have consent agreements with the FCC. And we engage with these agencies regularly.

Mr. WELCH. Do you believe that it should be up to the public as opposed to private interests to be making decisions about these public effects?

Mr. PICHAI. We definitely think areas where there could be clear legislation informed by the public—I think that definitely is a better approach. I would say the nature of content is so fast-changing and so dynamic, we spend a lot of energy hiring experts, consult with third parties, and that expertise is needed, I think, based on the—

Mr. WELCH. Right. And that is the problem we have in Congress, because an issue pops up and there is no way we can keep up. But you all can barely keep up with it yourself.

Mr. Dorsey, your view on those two questions, please?

Mr. DORSEY. Yes. I don't think the decision should be made by private companies or the government, which is why we are suggesting a protocol approach to help the people make the decisions themselves, have more control themselves.

Mr. WELCH. So does that mean that the creation of an agency that would be intended to address many of these tech issues that are emerging is something you would oppose or—

Mr. DORSEY. I always have an open mind. I would want to see the details of what that means and how it works in practice.

Mr. WELCH. Well, of course. But the heart of it is creating an entity that has to address these questions of algorithmic transparency, of algorithmic amplification of hate speech, of disinformation, of competition, and to have an agency that is dedicated to that, much like the Securities and Exchange Commission was designed to stop the rampant abuse on Wall Street in the 1930s—a public sector entity that is doing this, not just leaving it to private companies.

Mr. DORSEY. Yes. I do think—

Mr. WELCH. Do you agree or not?

Mr. DORSEY. I do think there should be more regulation around the primitives of AI. But we focus a lot of our conversations right now on the outcomes of it. I don't think we are looking enough at the primitives.

Mr. WELCH. Thank you. I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Mr. Bucshon for 5 minutes.

Mr. BUCSHON. Thank you, Mr. Chairman. And first of all, I want to thank the witnesses for being here today. It is going to be a long day, and appreciate your testimony and your answering questions.

I do think it is important to understand history—excuse me—when you look at these situations and you know, when it comes to the political side, when Thomas Jefferson wanted to get out an anti-Adams message even though he was his own vice president, had started his own newspaper because it was pretty clear that the newspapers that were being published weren't going to change their view because there was no competitive reason to do that.

And I think we are looking at potentially a similar situation here. Without competition, things don't change. I mean, it would be interesting to know the conversations with John D. Rockefeller in the early 1900s prior to the breakup of Standard Oil in 1911, and then of course AT&T in 1982.

So I understand that these are businesses. They are publicly held companies. I respect that. I understand that. I am a capitalist. That said, these situations are a little different, I think, because there is some social responsibility here. And I appreciate your answers that your companies are doing what you believe are necessary.

So I want to ask—I am going to take the antitrust area here. And Mr. Pichai, what do you think—what is the situation when you have Google, 92 percent of the searches are Google? You basically can't get on the internet without some sort of Google service. What do you think is going to happen? What do you think we should do about that?

Mr. PICHAI. Congressman, I mean, we definitely are engaged with conversations as well as lawsuits in certain cases. We understand there will be scrutiny here. We are a popular general-purpose search engine, but we compete vigorously in many of the markets we operate in. For example, the majority of revenue comes from product services, and one in two product services originate with Amazon today in the U.S.

So we definitely see a lot of competition by category. There are many areas as a company we are an emerging player, making phones. Or when we are trying to provide enterprise software, we compete with or larger players as well. And if you look at the last year and look at all the new entrants in the market, new companies that have gone public and emerged strongly, in tech shows, the market is vibrant and dynamic.

At Google, we have invested in many startups. Googlers have started over—former Google employees have started over 2,000 companies in the past 15 years. And so I see a highly dynamic, vibrant, competitive tech sector, and we are committed to doing our part.

Mr. BUCSHON. OK. Fair enough.

Mr. Zuckerberg, do you have some comments on that subject?

Mr. ZUCKERBERG. Congressman, I would echo Sundar's comments. I think that this is a highly competitive market. I mean, if this is a meeting about social media, not only do you have the dif-

ferent companies that are here today that all offer very big services that compete with each other, but you have new entrants that are growing very quickly, like TikTok, which is reaching a scale of hundreds of millions or billions of people around the world and I think is growing faster than any of our services of the companies that are up here today, and certainly competitive with us. And that is just naming a few, right? I mean, obviously there's Snapchat and a bunch of other services as well.

So it is a very competitive marketplace.

Mr. BUCSHON. And do you think—I will ask you this, Mr. Zuckerberg. I think you have commented that some of the privacy things that maybe the Europeans did would kind of solidify your dominance as a company. So what should we do in the United States on this? Because—it is a different subject, but similar—to not do something that would stymie innovation and competition, and further—in my view, further create a monopolistic or at least a perceived monopolistic environment.

Mr. ZUCKERBERG. Well, Congressman, I do think that the U.S. should have Federal privacy legislation because I think we need a national standard. And I think having a standard that is across the country that is as harmonized with standards in other places would actually create clearer expectations of industry and make it better for everyone.

But I think the point that you are making is a really important one, which is, if we ask companies to lock down data, then that to some degree can be at odds with asking them to open up data to enable, whether it is academic research or competition.

So I think that when we are writing this privacy regulation we just should be aware of the interaction between our principles on privacy and our principles on competition. And that is why I think a more holistic view, like what Congressman Welch was just proposing, I think is perhaps a good way to go about this.

Mr. BUCSHON. OK. Quickly, Mr. Dorsey, do you have any comments on that?

Mr. DORSEY. One of the reasons we are suggesting more of a protocol approach is to enable as many new entrants as possible. We want to be a client on that.

Mr. BUCSHON. OK. I want to—

Mr. DOYLE. The gentleman's time is expired.

Mr. BUCSHON. With that, I will yield back.

Mr. DOYLE. The Chair recognizes Ms. Clarke for 5 minutes.

Ms. CLARKE. Thank you, Mr. Chairman. I thank you, the chairs, and the ranking members for today's hearing. I also thank our witnesses for appearing.

In January, I called for public comment for the discussion draft of my bill, the Civil Rights Modernization Act of 2021, a narrowly focused proposal to protect historically marginalized communities from the harms of targeted advertising practices.

These harms can and have infringed on the civil rights of protected classes, and I am proud to formally introduce this bill next week to diminish inequities in the digital world.

For time's sake, I ask our witnesses to please answer the questions as succinctly as possible.

The first question goes to Mr. Zuckerberg. Facebook currently provides their advertisers with insight on how to get their ads in front of people who are most likely to find their ads relevant by utilizing tools to use criteria like consumer's personal interest, geography, to fine-tune thought targeting.

This has often used code that target or avoid specific races or other protected classes of people. Let me add that I am aware of the updates to your special ad audience. However, why does Facebook continue to allow for discrimination in the placement of advertisements that can violate civil rights laws?

Mr. ZUCKERBERG. Congresswoman, we have taken a number of steps to eliminate ways that people can target different groups based on racial affinity and different ways that they might discriminate, because this is a very important area. And we have active conversations going on with civil rights experts as to the best ways to continue improving these systems, and we will continue doing that.

Ms. CLARKE. Mr. Dorsey, Twitter allows advertisers to use demographic targeting to reach people based on location, language, device, age, and gender. In July, your company made changes to your ad targeting policies to advise advertisers to "not wrongfully discriminate against legally protected categories of users."

What did Twitter mean by the phrase "wrongfully discriminate"? Are some kinds of discriminatory advertising permitted on Twitter? If so, would you please explain?

Mr. DORSEY. No. None at all.

Ms. CLARKE. I am sorry. I didn't get that answer.

Mr. DORSEY. No. None at all.

Ms. CLARKE. OK. And so can you explain what you meant by "won't wrongfully discriminate"?

Mr. DORSEY. We mean that you shouldn't use our ad systems to discriminate.

Ms. CLARKE. Oh, OK.

Mr. Pichai, Google has recently announced a new approach in their targeting system called FLOC, or Federal Learning of Cohorts—excuse me, Federated Learning of Cohorts—to allow an ad targeting to groups of people with similar characteristics. The new system will utilize machine learning to create these "cohorts" for the consumers' visits to websites.

Given the potentially biased and disparate impact of machine learning algorithms, how has Google addressed the potential discriminatory impact of this new FLOC system?

Mr. PICHAI. Congresswoman, it is an important area. We recently announced a joint collaboration with HUD to ban ads that would target age, gender, family status, ZIP code, in addition to race, which we have long disallowed. So we will bring similar prohibitions, particularly when we are using machine learning.

And by the FLOC—it is early, we haven't implemented it yet. We will be publishing more technical proposals on it, and they will be held to our AI principles, which prohibit discrimination based on sensitive categories, including race. And we will be happy to consult and explain our work there.

Ms. CLARKE. I appreciate that.

Gentlemen, I just want you to be aware that the longer we delay in this, the more that these systems that you have created bake discrimination into these algorithms. I think that it is critical that you get in there and that you do what is in the best interest of the public of the United States of America and undo a lot of the harm that has been created with the bias that has been baked into your systems.

With that, Mr. Chairman, I yield back 23 seconds. And I thank you for this opportunity.

Mr. DOYLE. And I thank the gentlelady for that.

The Chair now recognizes Mr. Walberg for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chair. And thanks to the panel for being here. What I have listened to so far today, I would have to say that based upon what many of us in Congress say about the best legislation, when both sides don't like it, it is probably good. And you have certainly hit that today, I think from both sides. You have been attacked for various reasons.

But I have to say the platforms that you have developed are amazing and they have huge potential. And they indeed have enabled us to go directions—the information, the communications, relationships—that can be very positive and are amazing in what has been accomplished.

I think we get down to how that is controlled and who controls it. Going back to our foundations as our country, it was our second President, John Adams, who said that our constitution was meant for a moral and religious people and is wholly inadequate for any other.

I think we are seeing a lot of the problems that you are frustrated with as a result of parents and families, churches, schools, that aren't taking the primary responsibility. I get that. So it comes down to the choice that is left for the people is really between conscience and the constable.

We are either going to have a conscience that self-controls and, as you have said, Mr. Zuckerberg—in fact, what you said, I wouldn't mind my 3- and 5-year-old granddaughters coming to your house. I am not asking for the invitation, but I think they would be safe there relative to the online capabilities, from what you have said. But that is conscience versus constable.

But what I have heard today is that there will be some constable, and I am not sure that we will have success in moving forward. So I guess, Mr. Chairman, unfortunately we have been here before. We have been here many times. A few years ago, when Mr. Zuckerberg was here before this committee, I held up a Facebook post by a State senator in Michigan whose post was simply announcing his candidacy as a Republican for elected office, and yet it was censored as shocking and disrespectful or sensational in content.

Just a few months ago I posted my resolution that would add teachers to the vaccine priority list on Twitter, and it was labeled as "sensitive content" and encouraged to be changed. Well, hiding behind Section 230, all of you have denied that there is any bias or inequitable handling of content on your platforms.

And yet Pew Research Center found that—and this is where I have my problem—not so much with the platform or even the ex-

tent of what is on the platform, but they found that 72 percent of the public thinks it is likely that social media platforms actively censor political views that Big Tech companies find objectionable.

Further, and I quote, “By a 4-to-1 margin, respondents were more likely to say Big Tech supports the views of liberals over conservatives than vice versa.” Probably equaled only by higher education. That was my statement. And yet every time this happens, you fall back on blaming glitches in the algorithms.

It was former—Greg Coppola, a former Google insider, who said, before he was suspended by Google, he said, “Algorithms don’t write themselves. We write them to do what we want them to do.” That is my concern. Whether it is censoring pro-life groups like Life Action or pro-Second Amendment groups like the Well-Armed Women, your platforms continually shut down law-abiding citizens in constitutional discussions and commerce that don’t align with Big Tech views and the worldview, and this includes the First and Second Amendments that causes me to be concerned that you don’t share the same freedom and constitutional concerns.

It is not often I find myself agreeing with Bernie Sanders, but in an interview earlier this week, and I quote, he said, “If you are asking me do I feel particularly comfortable that the President of the United States should not express his views on Twitter, I don’t feel comfortable about that,” he went on to say, “because yesterday was Donald Trump who is blamed, and tomorrow it could be somebody else.”

Mr. Zuckerberg or Mr. Dorsey, do you believe the law should allow you to be the arbiters of truth, as they have under Section 230? Mr. Zuckerberg first.

Mr. ZUCKERBERG. Congressman, I think that it is good to have a law that allows platforms to moderate content. But as I have said today, I think that there—that we would benefit from more transparency and accountability.

Mr. WALBERG. Mr. Dorsey?

Mr. DORSEY. I don’t think we should be the arbiters of truth, and I don’t think the government should be, either.

Mr. WALBERG. Gentlemen, I agree.

Mr. DOYLE. The gentleman’s time is expired.

Mr. WALBERG. I yield back.

Mr. DOYLE. The Chair now recognizes Mr. Cárdenas for 5 minutes.

Mr. CÁRDENAS. Thank you very much, Mr. Chairman and ranking members, for having this important hearing. I would like to submit to the record a National Hispanic Media Coalition letter against Spanish-language disinformation on social media. If we could submit that for the record, I would appreciate that.

[The letter appears at the conclusion of the hearing.]

Mr. CÁRDENAS. Also, my first question is to you, Mr. Zuckerberg. In 2020, Facebook brought in approximately \$86 billion revenue in 2020. Is that about right, give or take?

Mr. ZUCKERBERG. Congressman, I think that is about right.

Mr. CÁRDENAS. OK. Thank you. Good. How much of that revenue did Facebook invest in identifying misinformation, disinformation, and that portion of your business?

Mr. ZUCKERBERG. Congressman, I don't know the exact answer. But we invest billions of dollars in our integrity programs, including having more than a thousand engineers working on this and 35,000 people doing content review across the company.

Mr. CÁRDENAS. OK. And how many people do have full-time equivalents, in your company overall?

Mr. ZUCKERBERG. Congressman, I don't know the exact number, but I think it is around 60,000.

Mr. CÁRDENAS. OK. So you are saying over half of the people in your company are doing the portion of content review, et cetera, which is the main subject we seem to be talking about today?

Mr. ZUCKERBERG. No, Congressman, because you asked about full-time employees, and some of the content reviewers are contractors.

Mr. CÁRDENAS. Oh, OK. All right. Well, there seems to be a disparity between the different languages that are used on your platform in America. For example, there was a study published in April, and over 100 items of misinformation on Facebook in six different languages was found, and 70 percent of the Spanish-language content analyzed had not been labeled by Facebook as compared to 30 percent of the English-language misinformation that had not been labeled. So there seems to be a disparity there.

What kind of investment is Facebook making on the different languages to make sure that we have more of an accuracy of flagging those disinformation and misinformation?

Mr. ZUCKERBERG. Congressman, thanks. We have an international fact-checking program where we work with fact-checkers in more than 80 countries and a bunch of different languages.

In the U.S. specifically, we have Spanish-speaking fact-checkers as well as English-speaking fact-checkers. So that's on the misinformation side. But also, when we create resources with authoritative information, whether it is around COVID information or election information, we translate those hubs so that way they can be available in both English and Spanish. And we make it so people can see the content in whatever language they prefer.

Mr. CÁRDENAS. Thank you. So basically you are saying it is extensive?

Mr. ZUCKERBERG. Congressman, this is certainly something that we invest a lot in. And it will be something that we continue to invest more in.

Mr. CÁRDENAS. OK. I like the last portion. I do believe, and would love to see you invest more.

My 70-plus-year-old mother-in-law, who is primarily a Spanish speaker, commented to me the other day that her friends who communicate mainly in Spanish—and they do use the internet, they use some of your platforms, gentlemen—that they were worried about the vaccine and that somebody is going to put a chip in their arm.

For God's sakes, I mean, that to me just was unbelievable that they would comment on that. But they got most of that information on the internet, on various platforms. Clearly, Spanish language disinformation is an issue, and I would like to make sure that we see all of your platforms address these issues, not only in English but in all languages.

I think it is important for us to understand that a lot of hate is being spewed on the internet, and a lot of it is coming through many of your platforms. For example, there are 23 people dead in El Paso because somebody filled this person's head with a lot of hateful nonsense, and he drove to specifically kill Mexicans along the Texas-Mexican border.

Eight people are dead in Atlanta because anti-Asian hatred and misinformation has been permitted to spread and allowed on these platforms unchecked, pretty much unchecked. The spread of hatred and incitement of violence on platforms is a deadly problem in America, and we need to see that it stops.

Mr. Zuckerberg, do you believe that you have done enough to combat these kinds of issues?

Mr. ZUCKERBERG. Congressman, I believe that our systems—and that we have done more than basically any other company. But I think that there is still a problem and there is still more that needs to be done.

Mr. CÁRDENAS. OK. That is good. You would like to do more. Thank you.

I only have 15 seconds so I am going to ask this question to all three of you: Do you think that each one of your organizations should have an executive-level individual in charge of this department reporting directly to the CEO? Do you think you agree that that should be the case? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congressman, we have an executive-level person who is in charge of the integrity team that I talked about. He is on my management team.

Mr. CÁRDENAS. Reports directly to you?

Mr. ZUCKERBERG. Congressman, he does not. I only have a few direct reports. A lot of people on the management team report to them.

Mr. CÁRDENAS. OK. Thank you. To the other two witnesses, very quickly?

Mr. PICHAI. Congressman, we have senior executives, including someone who reports directly to me, who oversees trust and safety across all of these areas.

Mr. CÁRDENAS. Thank you. Mr. Dorsey?

Mr. DORSEY. We do. We do.

Mr. CÁRDENAS. Thank you so much. I yield back the balance of my time.

Mr. DOYLE. The gentleman's time is expired.

The Chair now recognizes Mr. Carter for 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman. And thank all of you for being here.

Mr. Zuckerberg, I would like to start with you. And I wanted to ask you, you are aware, as all of us are, of the disaster that we have at the Southern border [audio disruption] indicate that human smugglers have been using social media, including Facebook, WhatsApp, and Instagram, to coordinate their operations in transporting illegal immigrants into the United States—things like, what to say to authorities, transportation tips, and other forms of information that are being traded on your platform to evade authorities and contribute to the crisis, this disaster at the border.

Mr. Zuckerberg, do you feel complicit in any way that your platform is assisting in this disaster?

Mr. ZUCKERBERG. Congressman, first let me say that what is happening at the border is—

Mr. CARTER. I am not—we know what is happening at the border. I am asking you specifically about your platform. Do you feel complicit in what your platform is doing to assist in this disaster?

Mr. ZUCKERBERG. Congressman, we have policies and we are working to fight this content. We have policies against scams in pages, groups, and events like the content that you are talking about. We are also seeing the State Department use our platform to share factual information with people about—

Mr. CARTER. I am not talking about facts. I am talking about—I am talking about coyotes who are using your platform to spread this kind of information to assist in this illegal activity that is resulting in horrible conditions for these people who are trying to come across that border.

Mr. ZUCKERBERG. Congressman, that is against our policies, and we are taking a lot of steps to stop it. And again, let me just say that I think the situation at the border is really serious and we are taking it very seriously.

Mr. CARTER. Well, and I hope you will look into this, these reports that your platform is being used by these traffickers. This is something we need your help with. I hope you feel the sense of responsibility, sir, to help us with this, because we certainly need it.

Let me ask you something. You dedicated a lot of your written testimony to election issues. And even today, during this hearing, you have been very public in pushing back about the election claims in November. Yet when Facebook has been essentially silent on the attempted theft of the certified election in Iowa of Representative Miller-Meeks. Why is that? Why are you silent on that, yet you are not silent on other elections?

Mr. ZUCKERBERG. Congressman, I think what we saw leading up to January 6 was unprecedented in American history, where you had a sitting President trying to undermine the peaceful transfer of power—

Mr. CARTER. You determined which one is important and which one is not. This seat to these people who elected this duly certified representative, this is the most important thing to them as well.

Mr. ZUCKERBERG. Congressman, I think part of what made the January 6th events extraordinary was not just that the election was contested, but that you got folks like the President—

Mr. CARTER. What—OK. Let me ask you this: What is it that makes this particular issue irrelevant, that you are not even covering it?

Mr. ZUCKERBERG. Congressman, I didn't say that it is irrelevant. But on January 6th, we had insurrectionists storm the Capitol, leading to the death of multiple people.

Mr. CARTER. My time is—Mr. Zuckerberg, I am aware of that. I was there. I understand what happened. But again, will you commit to treating this as a serious election concern? What is going on—

Mr. ZUCKERBERG. Congressman, we—I will commit to that. And we apply our policies to all situations. And I think that this is dif-

ferent from what happened on January 6th, but we apply our policies equally in these cases.

Mr. CARTER. Mr. Dorsey, you, too, have been very silent on this issue on your platform. Will you commit to treating this as a serious concern, the attempted theft of the certified seat in Iowa?

Mr. DORSEY. Yes. We are looking for all opportunities to minimize anything that takes away from integrity of elections.

Mr. CARTER. OK. Mr. Dorsey, while I have got you, let me ask you: You have started a new program. It is called the Bird Watch, and it allows people to identify information in tweets that they believe is misleading. And they write notes to provide context in an effort to stop misleading information from spreading.

Have you seen—we have seen mobs of Twitter users cancel others. And even when the information they share is accurate, why do you think Bird Watch is going to work, given the culture that you created on your platform?

Mr. DORSEY. Well, it is an experiment. We wanted to experiment with a more crowdsourced approach than us going around and doing all this work.

Mr. CARTER. Don't you think that is kind of a dangerous experiment, when you are taking off true information?

Mr. ZUCKERBERG. No. It is an alternative. And I think—

Mr. CARTER. An alternative.

Mr. DORSEY. I think we need to experiment as much as possible to get to the right answers. I think it states—

Mr. CARTER. OK. Well, that is fine as long as you are not the one being experimented on, as long as you are not the one that the information is going—

Mr. DOYLE. The gentleman's time is expired.

The Chair announces that we are going to take a recess now for 15 minutes. So the committee will stand in recess until 3:18, and then we will come back promptly. I call the committee in recess.

[Recess.]

Mr. DOYLE. OK. I will call the committee back to order and ask all Members and witnesses to come back online.

[Pause]

Mr. DOYLE. We will get started. The Chair recognizes Mrs. Dingell for 5 minutes.

Mrs. DINGELL. Thank you, Mr. Chairman. Thanks for having this hearing, and to everyone for testifying today.

We can all agree that social media companies have a responsibility to reduce and eliminate the impact of disinformation on their platforms. Mr. Zuckerberg, in the fall of 2020 you made numerous assurances to Congress that you had a handle on militia and conspiracy networks. We know, however, that Facebook private groups and the algorithms that recommend them have assisted in radicalizing users and facilitated terrorism, violence, and extremism against individuals, including the Governor of my State of Michigan. Racial and ethnic minorities, including Muslims and, recently, Asian Americans, are facing growing racist hate online and violence offline. Last year I sent you multiple letters about these issues, so I know you are aware of them.

In October of 2020, Facebook temporarily decided to stop recommending political or civic groups on its platforms, a change it has

now made permanent. But to be honest, despite what you did in October, we had an insurrection that stormed the Capitol on January 6.

I seriously question Facebook's commitment to actually stopping extremism. In a recent investigative report, a former Facebook AI researcher said he and his team conducted study after study confirming the same basic idea: Models that maximize engagement increase polarization. And you yourself have said that the more likely content is to violate Facebook community standards, the more engagement it generally receives. Engagement is the key to Facebook's growth and success, and the stock markets rewarded you for it even as you have been criticized for promoting extremism and racist content, including in a 2020 Facebook civil rights audit. The two seem to go hand in hand. As Facebook was also the most cited social media site in charging documents that the Justice Department filed against the Capitol insurrectionists.

Mr. Zuckerberg, do you still maintain that the more likely user content is to violate Facebook community standards, the more engagement it will receive? Yes or no?

Mr. ZUCKERBERG. Congresswoman, thanks for raising this because I think that there has been a bunch of inaccurate things about this shared today.

Mrs. DINGELL. OK.

Mr. ZUCKERBERG. There seems to be a belief——

Mrs. DINGELL. Yes or no?

Mr. ZUCKERBERG. Sorry. This is a nuanced topic. So if you are OK with it, I would like to——

Mrs. DINGELL. You have to keep it short. But I will give it a second since I want to——

Mr. ZUCKERBERG. Sure. So——

Mrs. DINGELL [continuing]. That is a victim of this hate.

Mr. ZUCKERBERG. People don't want to see misinformation or divisive content on our services. People don't want to see clickbait and things like that. While it may be true that people might be more likely to click on it in the short term, it is not good for our business or our product or our community for this content to be there. It is not what people want, and we run the company for the long term with a view towards 10 or 20 years from now.

And I think that we are highly aligned with our community in trying to not show people the content that is not going to be meaningful to them.

Mrs. DINGELL. OK, Mr. Zuckerberg. I am going to—I only have 2 minutes left. Do you still agree with the statement in Facebook's most recent 10-K filing that the first risk related to your product offerings is "our ability to add and retain users and maintain levels of user engagement with our products"? Just a yes or no, please.

Mr. ZUCKERBERG. Congresswoman, I think that that is generally right. I mean, for any product, the ability to build something that people like and use is something that is a risk if we can't do that.

Mrs. DINGELL. OK. So do you still agree with the statement of your CFO on a recent earnings call that the changes to group recommendations so far wouldn't affect your engagement? Yes or no?

Mr. ZUCKERBERG. Congresswoman, there are so many different parts of the service that I think it is probably right—

Mrs. DINGELL. Can I just—

Mr. ZUCKERBERG [continuing]. That not recommending political or civic groups probably isn't going to meaningfully decrease engagement. But we have taken a lot of HR steps, including reducing viral videos by about 50 million hours of watching a day, which have had a meaningful impact on engagement. But we do that because it helps make the service better and helps people like it more, which I think will be better for both the community and our business over the long term.

Mrs. DINGELL. OK. Mr. Zuckerberg, I am sorry to have to do this in 5 minutes. But given your promises in the fall, the events that transpired on January 6, and your two incentives that you yourself admit, I find it really difficult to take some of these assurances you are trying to give us today seriously.

I believe that regulators and independent researchers should have access to Facebook and other large social media platforms' recommendation algorithms, not just for groups but for any relevant feature that can be exploited or exploit private user data collected by the company to support extremism. And I support legislation to do so.

Mr. Zuckerberg, given your inability to manage your algorithms or your unwillingness to reduce controversial content, are you opposed to a law enabling regulators to access social media algorithms or other information technology that result in the promotion of harmful disinformation and extremist content?

Mr. ZUCKERBERG. Well, Congresswoman, while I don't necessarily agree with your characterization, I do think that giving more transparency into the systems is an important thing. We have people working on figuring out how to do this.

One of the nuances here in complexity is that it is hard to separate out the algorithms versus people's data which kind of goes into that to make decisions, and the data is private. So it is tough to make that public and transparent. But I do think that this is an important area of study on how to audit and make algorithms more transparent.

Mr. DOYLE. OK. The gentlelady's time is expired.

The Chair recognizes Mr. Duncan for 5 minutes.

Mr. DUNCAN. Thank you, Mr. Chairman. Let me first say that Democrats repeating disinformation about the motives of the murderer in Atlanta during a hearing on disinformation is irony at its worst. The murderer admitted that he was a sex addict. The problem was addiction, mental illness. While my thoughts and prayers go out to the families who were impacted by this hideous crime, it was not a hate crime, and to say so is disinformation.

Mr. Dorsey, is it OK for a white male to tweet a picture of a KKK Klansman hood to a black woman?

Mr. DORSEY. No. That would go against our hateful conduct policy.

Mr. DUNCAN. Just this week, black conservative commentator Candice Owens was sent a tweet from a white liberal depicting a KKK hood. And your support center said that that racist harass-

ment of a conservative didn't violate your terms of service. What do you have to say about that?

Mr. DORSEY. We removed that tweet.

Mr. DUNCAN. OK. Thank you for doing that. Also this week, Syrian refugee Ahmad Al Aliwi Alissa, a Biden-supporting Muslim, allegedly murdered 10 people at a grocery store in Boulder, Colorado. Your support center told Newsweek that referring to this gentleman as a white Christian terrorist wasn't a violation of your misinformation policy. What do you have to say about that?

Mr. DORSEY. I don't know that case, but we can follow up with you on that.

Mr. LATTA. Thank you. Your promises from the last hearing that you will work on this or make it better rang completely hollow sometimes, so I ask that you do.

You have censored and taken down accounts of conservatives, Christian, and even pro-life groups. At the same time, liberals, tyrants, and terrorists continue to have unfettered access on Twitter. You were able to take down the account of a sitting United States President while he was still President. But you continue to allow State sponsors of terror to use Twitter as a platform, including the Ayatollah Khoumeini, Javad Zarif of Iran, or even Bashar al-Assad of Syria.

You act like judge and jury and continue to hide behind the liability protections in Section 230 of the Communications Decency Act, which Congress set up to foster a free and open internet. You think you are above the law because, in a sense, Congress gave you that power, but Congress gave you that liability shield to one end: that was the protection of innocent children. Catherine McMorris Rodgers knocked it out of the park today, hammering the point where children are vulnerable.

But let's look at the John Doe vs. Twitter case that is ongoing right now. According to the National Center on Sexual Exploitation, a teenage boy, a victim of child sex trafficking, had images of his abuse posted on Twitter. One of those videos went viral, and he became the target of bullying to the point of being suicidal. He contacted you to alert you that his sex abuse images were on your platform. You failed to take them down. His mother contacted you to alert you, and again you failed to take them down.

They called the police and they followed up with you with a police report. Your support center told the family that, after review, the illegal video was not a violation of your terms of service. In the meantime, the illegal video accrued over 167,000 views.

It took a threat from a Homeland Security agent to get Twitter to take down the video. Even then you took no action against the accounts that were sharing it and continue to share sexually explicit videos of minors in clear violation of the law and in clear violation of your duties under Section 230 of the Communications Decency Act, as they were passed.

So in the eyes of Twitter, it is better to be a pedophile pornographer, a woke racist, or a state sponsor of terror than it is to be a conservative, even a conservative President. You have abused the Section 230 liability shield we gave you to protect children and used it to silence conservatives instead.

As we have heard today, your abuses of your privilege are far too numerous to be explained away and far too serious to ignore. So it is time for your liability shield to be removed—your immunity shield and the immunity shield of other woke companies who choose to score political points with their immunity shields rather than protect children.

My colleagues have been asking you if you deserve to continue to receive immunity under Section 230. Let me answer the question for you: No, you don't. You all think you do, but you don't because you continue to do a disservice to that law and its intent.

The United States Constitution has the First Amendment, and that should be your guide. Protecting the speech of users of your platform instead of trading them in like hostages and forcing things through algorithms to lead them down a path.

The American people really are tired of you abusing your rights, abandoning their values. So one of the Christian leaders that you banned, Mr. Dorsey, had as her last post a Scripture verse that you took down. And I want to leave it here today, Psalm 34:14. "Depart from evil and do good; seek peace and pursue it." Rather than silence that wise advice, I strongly suggest that you follow it.

Now, I have heard a lot of stuff on this hearing today about 230 protections. I challenge my colleagues to really get serious about doing something about this liability shield so that we do have a fair and free internet and people aren't censored.

With that, Mr. Chairman, I yield back.

Mr. DOYLE. The gentleman's time is expired.

The Chair recognizes Ms. Kelly for 5 minutes.

Ms. KELLY. Thank you, Mr. Chair. Thank you to the witnesses who are testifying today.

The business model for your platforms is quite simple: Keep users engaged. The more time people spend on social media, the more data harvested and targeted ads sold. To build that engagement, social media platforms amplify content that gets attention. That can be cat videos or vacation pictures, but too often it means content that is incendiary, contains conspiracy theories or violence.

Algorithms in your platforms can actively funnel users from the mainstream to the fringe, subjecting users to more extreme content, all to maintain user engagement. This is a fundamental flaw in your business model that mere warning labels, temporary suspension of some accounts, and even content moderation cannot address. And your company's insatiable desire to maintain user engagement will continue to give such content a safe haven if doing so improves your bottom line.

I would like to ask my first question of all the witnesses. Do each of you acknowledge that your company has profited off harmful misinformation, conspiracy theories, and violent content on your platform? Just say yes or no. Starting with Mr. Dorsey, yes or no?

Mr. DORSEY. No. That is not our business.

Ms. KELLY. Mr. Zuckerberg?

Mr. ZUCKERBERG. No, Congresswoman. I don't think we profit from it. I think it hurts our service.

Ms. KELLY. Mr. Pichai?

Mr. PICHAI. Congresswoman, it is certainly not our intent, and we definitely do not want such content. And we have clear policies against it.

Ms. KELLY. Well, since you all said no, can you please provide to me in writing how you manage to avoid collecting revenue from ads either targeted by or served on such content? So I will be expecting that.

There is a difference between a conversation in a living room and one being pumped out to millions of followers, from discouraging voting and COVID-19 misinformation to encouraging hate crimes. The harms are real and disproportionate.

Do you acknowledge that such content is having especially harmful effects on minorities and communities of color? Yes or no again? I don't have a lot of time, so yes or no? Mr. Dorsey?

Mr. DORSEY. Yes.

Ms. KELLY. Mr. Pichai?

Mr. PICHAI. Yes.

Ms. KELLY. Mr. Zuckerberg?

Mr. ZUCKERBERG. Yes. I think that's right.

Ms. KELLY. Thank you. If your financial incentive is that human psychology leads to the creation of a system that promotes emotionally charged content that is often harmful, do you believe that you can address the—do you believe that you will always need to play Whac-a-mole on different topics? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congressman, I do think that we can take systematic actions that help to reduce a large amount of this. But there will always be some content that gets through those systems that we will have to react to.

Ms. KELLY. Mr. Dorsey?

Mr. DORSEY. That is not our incentive, but I agree with Mark. Our model is to constantly integrate. We are going to miss some things, and we will go too far in some cases.

Ms. KELLY. Mr. Pichai?

Mr. PICHAI. I agree largely with what Mark and Jack said. And we—a lot of channels, we remove thousands of misleading election videos. There are many involving threats, and we are very vigilant.

Ms. KELLY. OK. More transparency and research into the AI models you use is needed. I understand that they are constantly evolving and proprietary. However, those obstacles must not be insurmountable. Would you agree to some type of test bed to evaluate your procedures and technology for disparate impacts? And would you welcome minimal standards set by the government? I only have 44 seconds.

Mr. DORSEY. I will go. You are not calling us. But we—yes, we are interested in opening all this up and going a step further in having a protocol. I don't think that should be government-driven, but it should be open and transparent that the government can look at it and understand how it works.

Mr. ZUCKERBERG. I agree that this is an area where research would be helpful. And I think some standards, especially amongst the civil rights community, would be helpful guidance for the companies.

Mr. PICHAI. Congresswoman, we work with many third parties. I just mentioned the HUD collaboration we had. Definitely would

be open to conversations about minimum standards. It is an important area.

Ms. KELLY. Thank you. I yield back.

Mr. DOYLE. The gentlelady's time is expired.

The Chair now recognizes Mr. Dunn for 5 minutes.

Mr. DUNN. Thank you very much, Mr. Chairman.

Many of the questions today deal with personal arms. But there are long-term economic and security arms to our country I would like us to keep in mind as well.

I represent Florida's 2nd Congressional District, which is proud to host a large presence of the U.S. military, including civilian support companies. One of these is Applied Research Associates, which is doing great work with our military in the field of artificial intelligence and machine learning.

I agree with our Nation's top national security experts on the critical importance of the United States maintaining its competitive edge in AI. And I share the concern of former Google CEO Eric Schmidt, who warned just a few weeks ago of the grave consequences should we lose that edge to China.

Leader Rodgers led a bipartisan bill enacted last year, the American Compete Act, to lay out clear AI strategy. We all recognize that China is not a good place to do business, evidenced by the fact that all of your respective main products and services are banned there. It is clear that the influence of the Chinese Communist Party permeates the entire corporate structure in China. Xi Jinping himself stated his goal of integrating the party's leadership into all aspects of corporate governance.

Let's be clear with each other. It is impossible to do business in China without either directly or indirectly aiding the Chinese Communist Party. It is also important to state for the record that each of your business models involve collecting data from individuals who use your product and then using that data for some other purpose.

Mr. Pichai, I am deeply concerned with Google's pursuit of and investment in artificial intelligence research in China, widely reported over the last few years. First and foremost, can you assure Americans that their personal data, regardless of how you think you have de-identified it—data you collect when they use Google and which is central to your algorithms—is not used in your artificial intelligence collaboration with the Chinese Government?

Mr. PICHAI. Congressman, I want to correct any misperceptions here. We do not have an AI research center in China now. We had a limited presence working on open source projects, primarily on open source projects and around K through 12 education with a handful of employees. We don't have that anymore. Compared to our peers, we don't offer our core services in China, products like search, YouTube, Gmail, et cetera.

Mr. DUNN. I am going to have to reclaim my time because it is limited. But I want your team to follow up with me because I am honestly somewhat skeptical. I think you had three centers there in China. And I want to know more about what they are doing and also what material they are using.

And I want to be clear. I am not just suggesting that simply doing business in a country means that you endorse all their poli-

cies. As a former businessman myself, I know the politics all too often get in the way of what we are trying to do. However, Google's own list of artificial intelligence principles states that it will not collaborate on technologies to gather or use information for surveillance, violating international accepted norms or contravenes widely accepted principles of international law and human rights.

We know that the Chinese Communist Party is using artificial intelligence technology to spread misinformation and suppress the prodemocracy movement in Hong Kong as well as using that technology in its genocidal crimes against the Uyghurs, including murdering them for their organ harvesting.

Once again, can you be sure that none of the work you are doing in collaboration with the Chinese Government is not aiding them in this ability?

Mr. PICHAI. Congressman, happy to follow up and clarify the limited work on AI we undertake. It is primarily around open source projects. And very happy to engage and very specifically follow up on what we do.

Mr. DUNN. Well, I think that is great. And I know I am running out of time here, but I ask that we continue this dialogue. And I think Google would be very well served by promoting greater transparency in all of its actions regarding artificial intelligence in China. Your customers have a right to know about this.

In 2018, Diane Greene, former CEO of Google Cloud, noted, "We believe the uses of our cloud and artificial intelligence will prove to be overwhelmingly positive for the world. But we also recognize we cannot control all downstream uses of our technology."

Well, a good place to start would be to end this dangerous artificial intelligence research relationship with China. So with that, Mr. Pichai, thank you. Thank you, all the members of the witness panel.

And Mr. Chairman, I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Mr. McEachin for 5 minutes.

Mr. MCEACHIN. Thank you, Mr. Chairman. And to you and Chairman Pallone and Chairwoman Schakowsky, thank you for convening today's hearing and for our witnesses for joining us.

In July of last year, I led more than 30 of my colleagues, including several on this committee, in a letter to your companies asking what you were doing to halt the spread of climate change disinformation on your platforms. As my colleagues and I clearly expressed in our letter, climate change is a real and urgent threat, and the spread of disinformation on your platforms is underlining that fact.

For instance, the World Health Organization estimates that climate change causes 150,000 deaths annually, a number that will only increase in the coming years. All this begs a simple question: Why do your platforms not treat climate change disinformation with a sense of immediacy and alarm?

Mr. Zuckerberg, Facebook recently implemented the Climate Change Information Center, which directs users to a landing page with climate change facts from researchers and organizations. Are you able to share data on how widespread a problem climate

change disinformation is on your platform and how much the Climate Change Information Center has reduced it?

Mr. ZUCKERBERG. Sure. Thanks, Congressman. Our approach to fighting misinformation—of which climate misinformation, I think, is a big issue, so I agree with your point here. We take a multipronged approach. One is to try to show people authoritative information, which is what the Climate Information Center does.

But then we also try to reduce the spread of misinformation around the rest of the service through this independent third-party fact-checking program that we have in which one of the fact-checkers is specifically focused on science feedback and climate feedback type of issues.

Overall, I would be happy to follow up and share more details on what we have seen across those. But this is certainly an area that I agree is extremely important and needs multiple tactics to address.

Mr. MCEACHIN. Well, thank you. And it is my understanding that this climate center was modeled after your COVID-19 Information Center. However, different standards still apply for both organic content and paid-for advertising for climate change versus COVID-19.

Why does Facebook not apply the same standards of fact-checking on climate change that it does on COVID-19 content?

Mr. ZUCKERBERG. Congressman, you are right that the Climate Information Center was based off our work on the COVID Information Center and Election Information Center. In terms of how we treat misinformation overall, we divide the misinformation into things that could cause imminent physical harm—of which COVID misinformation that might lead someone to get sick or hurt or vaccine misinformation falls in the category of imminent physical harm—and we take down that content.

Then other misinformation are things that are false but may not lead to imminent physical harm. We label and reduce their distribution but leave them up. So that is the broad approach that we have, and that sort of explains some of the differences between some of the different issues and how we approach them.

Mr. MCEACHIN. Mr. Pichai—and I hope I am pronouncing that correctly, sir—YouTube has employed contextualization tools linking viewers to similar sources as Facebook's Climate Center. That being said, you restricted but have not removed some repeat offenders from your platform such as Prager University, a nonaccredited university producing climate change denial content.

Are you not concerned that by restricting those videos and not removing repeat offenders, that people who are determined to find those videos to validate their fears will indeed find them and share them with others?

Mr. PICHAI. Congressman, it is an incredibly important area. In general, in these areas we rely on raising authoritative information, both by showing information panels as well as raising scientific content, academic content, and journalistic content so our algorithms rank those types of content higher for an area like climate change, similar to election integrity and COVID.

And obviously it is an area where there is a range of opinions people can express. We have clear policies, and if it is violative, we

remove. If it is not violative but if it is not deemed to be of high quality, we don't recommend the content. And that is how we approach it, and we are committed to this area as a company.

We lead in sustainability. We have committed to operating 24/7 on a carbon-free basis by 2030. And it is an area where we are investing significantly.

Mr. MCEACHIN. Well, thank you. I have run out of time. Mr. Dorsey, I apologize to you. Perhaps we will have an opportunity to have a conversation.

Mr. Chairman, I give you my 2 seconds.

Mr. DOYLE. I thank the gentleman. The gentleman yields back.

The Chair now recognizes Mr. Curtis for 5 minutes.

Mr. CURTIS. Thank you, Mr. Chairman. And thank you to our witnesses.

My first comment is to point out that in her 2019 Presidential campaign, Senator Elizabeth Warren, Democrat, called for the breaking up of your companies. Several weeks ago, in a speech at CPAC, Senator Josh Hawley, Republican, also said that Big Tech companies should be broken up. I don't think I need to point out the irony of Josh Hawley validating Elizabeth Warren at CPAC.

There seems to be a train wreck coming. Unfortunately, the very few tools that we have in our tool bag are regulation and breaking up. Mr. Zuckerberg, I read through your terms of service, including the dense community standards document. In your terms of service, you state that you cannot control and do not take responsibility for content posted on your platform.

The community standards document, which is frequently cited as why content is or is not censored, says you sometimes make content moderation decisions based off what is considered best for the public interest or public discourse.

I know in your testimony you said that companies need to earn their liability protections. That is great. But that doesn't address the concerns people understandably share about your past or current views on what is or is not acceptable.

How do you claim you cannot take responsibility and therefore should maintain your liability protections for content posted on your site, but at the same time state that your platform or monitored content based off what is in the public's best interest? That appears to be two-sided.

Mr. ZUCKERBERG. Congressman, thanks. People use our services to share and send messages billions of times a day. And it would be impossible for us to scan or understand everything that was going on, and I don't think that our society would want us to take the steps that would be necessary to monitor every single thing. I think that we would think that that would infringe on our freedoms.

So broadly, I think it is impossible to ask companies to take responsibility for every single piece of content that someone posts, and that, I think, is the wisdom of 230. At the same time, I do think that we should expect large platforms to have effective systems for being able to handle, broadly speaking, categories of content that are clearly illegal.

So we have talked today about child exploitation and opioids and sex trafficking and things like that. And I think it is reasonable to

expect that companies have systems that are broadly effective, even if they are not going to be exactly perfect, and there are still going to be some pieces of content that inevitably get through, just like no police department in the city is able to eliminate all crime.

Mr. CURTIS. I am going to jump in only because we are out of time. I would love to spend more time on that with you.

Let me also ask you. Utah is known for Silicon Slopes, our startup community. You have called for government regulation, but some view this with skepticism because larger companies tend to deal with regulation much better than small companies.

If you think back to your college days, the early startup phase of Facebook, what challenges do you see for startups to compete and what cautions should Congress consider as we look at regulations that potentially could be a barrier for companies that might be your future competition?

Mr. ZUCKERBERG. Thanks. I think that this is a really important point whenever we are talking about regulation. And I want to be clear that the recommendations that I am making for Section 230 I would only have applied to larger platforms.

I think it is really critical that a small platform, the next student in a dorm room or in a garage, needs to have a relatively low—as low as possible regulatory burden in order to be able to innovate and then get to the scale where they can afford to put those kind of systems in place. So I think that that is a really important point to make.

But I think that that goes for the content discussions that we are having around 230. It probably also applies to the privacy law that I hope that Congress will pass this year or next year to create a Federal U.S. privacy standard. And I also think that we should be exploring proactively requiring things like data portability that would make it easier for people to take data from one service to another.

Mr. CURTIS. I want to thank you. I have got just a few seconds left. And Mr. Pichai, this is a little bit off topic so I am simply going to ask this question and submit it for the record and not ask for a response.

Almost a decade ago your company started Google Fiber. You introduced Kid Speed and free internet to all the residents of my home city, Provo, Utah. Sadly, it seems like your efforts to do this across the country were slowed down or even stopped by excessive government regulations. I would love you to share off the record—and I will submit it for the record—why government is making it so hard to expand internet across the country.

Thank you, Mr. Chairman, and I yield my time.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Mr. Soto for 5 minutes.

Mr. SOTO. Thank you, Mr. Chairman.

When television, radio, traditional newspapers, political blogs, and even private citizens spread lies, they can be sued and held liable for damages or FCC fines. But pursuant to 230, you all can't be sued. You have immunity. But it ain't 1996 anymore, is it? Meanwhile, lies are spreading like wildfire through platforms. Americans are getting hurt or killed. And the reason is your algorithms.

I want you to all know I was held captive in the gallery during the Capitol insurrection. I was surrounded by domestic terrorists that killed a Capitol police officer, ransacked the Capitol, and almost disrupted a Presidential election. And many of these domestic terrorists plotted on your platforms. I think we all understand by now this violence is real. And so this is why we are here today, in the committee of jurisdiction, with power to protect our fellow Americans.

Mr. Zuckerberg had mentioned effective moderation systems. So now we know you have systems that can prevent many of these harms. Thank you for your statements supporting accountability today, and even for championing support of accountability now.

So the question is: What specific changes to Section 230 do you support to ensure more accountability? Mr. Zuckerberg just mentioned categories of content that are clearly illegal, U.S. privacy standards, and data portability as three standards we should be looking at.

Mr. Pichai, should we be creating these standards and then holding platforms accountable if they violate them under 230?

Mr. PICHAI. Congressman, first of all, there are many ways and there are many laws today which do hold us liable. FTC has oversight, we have a consent decree with the FCC, COPPA, HIPAA, et cetera, and for example areas where there are privacy laws, and we have called for Federal privacy legislation, but in Europe, the GDPR. In California, we have privacy State legislation. We are both accountable as well as we are subject to private plaintiff action against these statutes.

Mr. SOTO. So Mr. Pichai, you agree with these categories that were just outlined by Mr. Zuckerberg. Is that correct?

Mr. PICHAI. I definitely think what Mark is talking about around lines of transparency and accountability are good proposals to think through. There are various legislative proposals, among those—

Mr. SOTO. Excuse me. My time is—Mr. Dorsey, do you think we should be establishing categories of content that are clearly illegal, U.S. privacy standards, and data portability, as well as penalties for violation of those standards?

Mr. DORSEY. I believe, as we look upon 230 and evolutions of it, inputting upon it, I think we need more transparency around content moderation practices, not just policies. I think we need more robust appeals processes. And I think the real issue is algorithms and giving people more choice around algorithms, more transparency around algorithms. So if there is any one I would pick, it would be that one. It is a tough one, but it is the most impactful.

Mr. SOTO. Thank you, Mr. Dorsey.

Mr. Zuckerberg, political misinformation spread rampantly, unfortunately, in Spanish in Florida's Hispanic community on Facebook in the 2020 Presidential election even with the political ad ban. How do you think this happens? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congressman, it is—I do still think that there is too much misinformation across all of these media that we have talked about today. How did it happen? I mean, it is—I think we have talked to a lot today about algorithms. I actually think a lot of this stuff happens in what we refer to as deterministic products

like messaging, right? Someone sends a text message to someone else. There is no algorithm there determining whether that gets delivered. People can just send that to someone else.

A lot of this stuff, I think, unfortunately was amplified on TV and in traditional news as well. There was certainly some of this content on Facebook, and it is our responsibility to make sure that we are building effective systems that can reduce the spread of that. I think a lot of those systems performed well during this election cycle. But it is an iterative process, and there are always going to be new things that we will need to do to keep up with the different threats that we face.

Mr. SOTO. Mr. Zuckerberg, will you commit to boosting Spanish-language moderators and systems on Facebook, especially during election season, to help prevent this from happening again in Spanish language?

Mr. ZUCKERBERG. Congressman, this is already something that we focus on. We already beefed up and added more capacity to Spanish language fact-checking and Spanish language authoritative information resources. And that is certainly something that we hope to build on in the future. So the answer to your question is yes.

Mr. DOYLE. The gentleman's time is expired.

The Chair now recognizes Mrs. Lesko for 5 minutes.

Mrs. LESKO. Thank you, Mr. Chair, and thank you to the witnesses.

I represent constituents in the great State of Arizona, and most of my constituents just want to be treated fairly, equitably, impartially, and they want to make sure that their private information stays private.

Mr. Pichai, does Wikipedia influence Google's search results?

Mr. PICHAI. We do index, and Wikipedia is in our index. And for certain queries, if an answer from Wikipedia rises to the top of our ranking, yes, we do rely on it.

Mrs. LESKO. Thank you.

Mr. Dorsey, did you personally decide to ban President Trump from your platform?

Mr. DORSEY. We have a process that we go through to get there, and that came after a warning.

Mrs. LESKO. And did you make the final decision?

Mr. DORSEY. Ultimately, I have final responsibility.

Mrs. LESKO. Thank you.

And Mr. Pichai, in July 2018 the Wall Street Journal reported that Google let hundreds of outside developers scan the inboxes of millions of Gmail users. Mr. Pichai, do Google employees review and analyze Gmail users' content?

Mr. PICHAI. Congresswoman, we take privacy very seriously. We don't use the data from Gmail for advertising, and our employees generally do not access it, only in narrow cases, either to troubleshoot with the right consent and permissions. There are prohibitions with enough checks and balances.

Mrs. LESKO. So I think what you are saying is occasionally your Google employees do review and analyze.

I have another question regarding that. Does Google share Gmail users' emails or analysis of your emails with third parties?

Mr. PICHAI. We do not sell any data. I think what you are referring to is users could give API access to third-party developers—for example, there are applications which could give travel-related information. So this is a user choice, and it is an API on top of the platforms. We have done numerous steps to make sure users have to go through multiple steps before they would give consent to a third party.

Mrs. LESKO. And so I have looked through your Google Privacy Statements and User Content, and I still have concerns about that. I am very concerned. I have Gmail accounts, just like millions of people, and I don't know if you are looking at them. I don't know who is looking at them. I don't know who is sharing them. I don't know what you are doing with them.

Mr. PICHAI. If I—

Mrs. LESKO. You make me concerned. Mr.—I only have—

Mr. PICHAI. If I could clarify one thing I said there?

Mrs. LESKO. Yes.

Mr. PICHAI. Only if a user asks us to troubleshoot an account, with that user's permission. But we do not look into users' email contents, and we do not share the contents with anyone else without the user's asking us to do so.

Mrs. LESKO. However, the Wall Street Journal had this article saying that hundreds of developers were reviewing the email contents. So I have to move on to another question because I only have a short time.

Mr. Dorsey, Twitter denied the Center for Immigration Studies the ability to promote four tweets that contained the phrases "illegal alien" and "criminal alien," even though those are the correct legal terms. Mr. Dorsey, if there is a warning posted related to a border threat, how will Twitter algorithms react to the use of the word "illegal" versus "undocumented"?

Mr. DORSEY. Well, it isn't about our algorithms. It is interpretation against our policy and if there are violations. But we can follow up with you on how we handle situations like that.

Mrs. LESKO. Well, this is the legal term, is "illegal alien." That is in law, in legal terms. I don't understand why you would not allow that. That is the legal, factual term. And with that, I am going to ask another question.

Mr. Zuckerberg, this has been brought up before. Do you believe that your platform harms children?

Mr. ZUCKERBERG. Congresswoman, I don't believe so. This is something that we study and we care a lot about. Designing products that improve people's well-being is very important to us. And what our products do is help people stay connected to people they care about, which I think is one of the most fundamental and important human things that we do, whether that is for teens or for people who are older than that.

And again, our policies on the main apps that we offer generally prohibit people under the age of 13 from using the services.

Mr. DOYLE. The gentlelady's time is expired.

The Chair now recognizes Mr. O'Halloran for 5 minutes.

Mr. O'HALLORAN. Thank you, Mr. Chairman. I am enlightened. Thank you to the panel today.

I am enlightened by what I have heard today: three of the most knowledgeable business people in the word, with beautiful profit centers, business models, a sense of the future direction that your companies want to go in, standards that are in many cases reliable but others not very much so, and a very big concern by the Congress of the United States on the direction you want to go in versus what is good for our Nation in total.

Mr. Zuckerberg, last October Facebook announced it removed a network of 202 accounts, 54 pages, and 76 Instagram accounts for violating your coordinated inappropriate behavior policy. A really forged network was based in [audio disruption] Arizona and ran its disinformation operation from 2018 to 2020 by creating fake accounts and commenting on other people's content about the 2018 midterm election, the 2020 Presidential election, COVID-19, and criticism and praise of creation of certain political parties and Presidential candidates. Sadly, Facebook only acted after a Washington Post investigation reported its findings.

While your testimony states since 2017 Facebook has removed over 100 networks of accounts for engaging in coordinated, inauthentic behavior, where did Facebook fail by not finding this network over the course of a number of years? Mr. Zuckerberg,

Mr. ZUCKERBERG. Well, Congressman, we have a team of—I think it is more than 300 people who work on counterterrorism at this point, and basically trying to work with law enforcement and across the industry to basically find these networks of fake accounts and authentic accounts that are trying to spread behavior.

And I think we have gotten a lot more effective at this. I can't say that we catch every single one, but certainly I think we have gotten a lot more effective, including just this week we announced that we took down a network of Chinese hackers that were targeting Uyghur activists outside of China.

So we have gotten more sophisticated at this. Sometimes when we start finding a lead, we need to wait to kind of see the full extent of the network so we can take down the whole network. So that is a tradeoff that sometimes we are able to discuss with law enforcement and other times not, in terms of how we do enforcement. But overall, I think this effort has gotten a lot more sophisticated over the last 4 years.

Mr. O'HALLORAN. So you are happy with the amount of personnel that you have working on these issues?

Mr. ZUCKERBERG. Congressman, I think we have one of the leading teams in this area. We went from more than—

Mr. O'HALLORAN. Are you happy with—the question was: Are you happy with the amount of people you have working, the capacity that you have to take care of these issues?

Mr. ZUCKERBERG. Congressman, I think that the team is well-staffed and well-funded. We spend billions of dollars a year on these kind of content and integrity and security issues across the company. So I think that that is appropriate to meet the charge. And there are always things that we are going to want to do to improve the tactics of how we find this, and a lot of that over the last several years has been increasing the work that we do with law enforcement and the intelligence community—

Mr. O'HALLORAN. I am going to move on to another question, Mr. Zuckerberg. Thank you very much. I do want to say that, again, you are a bright, intelligent CEO. You know in advance what you want. Your algorithms are created by your company and the other companies. You have control over those algorithms.

And so the idea that you have to work maybe in this direction, Mr. Zuckerberg, Facebook's most recent community standards enforcement report states that 2.5 million pieces of content related to suicide and self-injury were removed in the fourth quarter of 200 due to increased reviewer capacity.

You can do this if you want to do all this stuff. Very briefly explain what policies Facebook put in place to reviewer capacity, not just on that issue but across the—how much over time has this occurred that you continue to increase reviewer capacity?

Mr. ZUCKERBERG. Sure, Congressman. The biggest thing that we have done is automated a lot of this by building AI tools to identify some of this. So now, for example, more than 98 percent of the hate speech that we take down is done by an AI and not by a person. I think it is 98 or 99 percent of the terrorist content that we take down is identified by an AI and not a person. And you mentioned the suicide content as well, which I think a high 90s percent is identified by AI rather than—

Mr. O'HALLORAN. Mr. Zuckerberg, I am over my time. I want to thank the chair, and I also want to state very briefly that you have a lot of work to do, you and your other cohorts on this panel. Thank you.

Mr. DOYLE. The gentleman's time is expired.

The Chair recognizes Mr. Pence for 5 minutes.

Mr. PENCE. Thank you, Chairs Doyle and Schakowsky and Ranking Members Latta and Bilirakis, for holding this joint subcommittee meeting hearing. And thank you to the witnesses for appearing before us today.

The extent to which your platforms engulf our lives is reminiscent to the all-encompassing entities we have seen over the past century. In the early 1900s, Standard Oil had a monopoly on over 90 percent of our country's refining business. By the 1970s, if you used a telephone it was going to be Ma Bell's system.

In each instance, you could choose not to use either product. But participation in society demanded that you use both. In a similar sense, it is difficult if not impossible to participate in society today without coming across your platforms and using them. We could choose not to use them, but like oil and telecommunications, it is considered essential, and so many other people do use it.

Even the government has become an equal contributor. Each Member of Congress and every Senator is all but required to use your platforms to communicate with their constituents while we are in Washington, DC. I know you understand that your platforms have a responsibility to act in good faith for Hoosiers and all Americans.

Unfortunately, regularly my Facebook and Twitter accounts, like many of my peers and other people I know, are littered with hateful, nasty arguments between constituents that stand in complete opposition to the ideas of civil discourse that your platforms claim to uphold and that you have referenced today.

I am sure you are aware that official government accounts have restrictions that significantly limit our ability to maintain a platform that is a productive resource of information to the public. They have essentially become a micro town hall without a moderator on social media.

I agree with all your testimonies that a trust deficit has been growing over the past several years. And as some of you have suggested, we need to do something about it now. The way in which you manage your platforms in an inconsistent manner, however, has deepened this distrust and devolved the public conversation.

My constituents in southeast Indiana have told me they are increasingly mistrustful of your platforms, given how you selectively enforce your policies. There are just a few examples of how this has occurred. Members of the Chinese Communist Party have verified Twitter accounts to regularly peddle false and misleading claims surrounding the human rights violations we know are occurring in northern China.

Twitter gives the Supreme Leader of Iran a megaphone to proclaim derogatory statements endorsing violence against the U.S. and Western culture. Twitter accounts associated with the Supreme Leader have called Israel a “cancerous tumor” and called for the eradication of the Zionist regime. This happens as he also bans the service for his own people to restrict their free expression.

Mr. Dorsey, clearly you need to do more to address content that violates your policies. I have two questions for you. Why is the Chinese Communist Party allowed to continue the use of your platform after pushing propaganda to cover up human rights abuses against Muslims in Northern China? And two, why does the Supreme Leader of Iran still half a platform to make threats against Israel and America?

Mr. DORSEY. So first and foremost, we do label those Chinese accounts so that people have context as to where they are coming from. That is on every single tweet, so people understand the source. We think that is important.

We are reviewing our world leaders policy. We are actually taking public comment review right now. So we are enabling anyone to give us feedback on how—

Mr. PENCE. If I may interrupt you quickly, Mr. Dorsey. On that very point, Iran has been supporting Hezbollah, and it is not just saber-rattling, as you have made the statement, or your company has made the statement. They have done serious damage to whole countries and people, and as I served in the military, they killed hundreds of Marines many years ago. So I don't know what you have to study about this.

Mr. Chairman, I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Miss Rice for 5 minutes.

Miss RICE. Thank you, Mr. Chairman.

Mr. Dorsey, what is winning, Yes or No, on your Twitter account poll?

Mr. DORSEY. Yes.

Miss RICE. Hmm. Your multitasking skills are quite impressive.

In December of 2020, the House Committee on Veterans' Affairs released a report entitled, “Hijacking Our Heroes: Exploiting Vet-

erans Through Disinformation on Social Media." I ask unanimous consent, Mr. Chairman, that this report be submitted for the record.

Mr. DOYLE. So ordered.¹

Miss RICE. Thank you. I bring up the report today because it is very—deeply disturbing, the investment of our veterans and military service members in the violence that took place on January 6. It is estimated that 1 in 5 people charged in connection with the attack have served or are currently serving in the U.S. military.

It should come as no surprise to those testifying today that for years nefarious actors have learned how to harness the algorithms on all of your platforms to introduce content to veterans and military service members that they did not actively seek out for themselves. Veterans and military service members are particularly targeted by malicious actors online in order to misappropriate their voices, authority, and credibility for the dissemination of political propaganda.

We have to do better for those who have served our country. Mr. Zuckerberg, do you believe that veterans hold a special status in our communities and have military training, making them prime targets for domestic terrorists and our adversaries seeking to foment insurrection?

Mr. ZUCKERBERG. Congresswoman, I certainly believe that veterans hold a special place in our society. I haven't seen much research—

Miss RICE. Did you see on the National Mall and at the Capitol there were rioters who arrived in combat gear who were armed with tactical equipment? Did you see those images, yes or no?

Mr. ZUCKERBERG. Yes.

Miss RICE. OK. Have you personally talked to the Iraq and Afghanistan Veterans of America, IAVA, about disinformation campaigns targeting veterans?

Mr. ZUCKERBERG. No, Congresswoman, I have not personally, although our team certainly is in contact with a number of these groups as we set up our policies.

Miss RICE. Have you talked to the Vietnam Veterans of America about disinformation campaigns targeting veterans?

Mr. ZUCKERBERG. Congresswoman, I can get back to you on whether our team has consulted with them specifically. But broadly, what our teams—

Miss RICE. Please do. Do you believe that veterans and military service members are just like other Americans in that they are susceptible to the impulses in human psychology that Facebook exploits to drive engagement? Do you believe that they are susceptible in that way? Yes or no?

Mr. ZUCKERBERG. Congresswoman, there is a lot in your characterization there that I disagree with.

Miss RICE. No, no. It is a question of do you think they are susceptible to that kind of information coming at them? Yes or no?

Mr. ZUCKERBERG. Congresswoman, I believe that—

¹The report has been retained in committee files and is available at <https://docs.house.gov/meetings/IF/IF16/20210325/111407/HHRG-117-IF16-20210325-SD028.pdf>.

Miss RICE. OK. So given your answers, I am not convinced that you have the appropriate resources devoted to the problem of mitigating the real-world effects of content that is designed to mislead and radicalize your users, especially those who are veterans and military service members.

Would you support legislation that would require you to create an Office of Veterans' Affairs that reports to the CEO and works with outside veterans service organizations to ensure our enemies don't gain ground trying to radicalize our brave men and women who serve in our military? Would you support that legislation?

Mr. ZUCKERBERG. Congresswoman, I think the details matter a lot. So I would be happy to follow up with you or have our team follow up with your team to discuss this. But in general, I do think that—

Miss RICE. We will take you up on that, Mr. Zuckerberg. It is just a broad stroke: Do you believe that you could find your way to support legislation that would have as its goal the protection of our military active duty and veterans? In principle?

Mr. ZUCKERBERG. I think in principle, I think something like that could certainly make sense.

Miss RICE. So I wrote to you, Mr. Zuckerberg, last month requesting information about Facebook's efforts to curb disinformation campaigns that specifically targeted American service members and victims. I am just curious if you know how many public groups with the word "veteran" or public pages with the word "veteran" did you remove from your platform after January 6th in association with misinformation about the 2020 election or the attack on the Capitol?

Mr. ZUCKERBERG. Congresswoman, I don't know the answer off the top of my head, but I would be happy to get back to you with that.

Miss RICE. Thank you. We believe that you should be tracking that information. Your platform was in fact a crime scene after January 6, and we need that information and data to understand how the attack happened.

I want to thank all three of you for coming here today and spending so much time with us. I yield back, Mr. Chairman. Thank you.

Mr. DOYLE. The gentlelady yields back.

The Chair recognizes Mr. Armstrong for 5 minutes.

Is Mr. Armstrong here? You need to unmute, Kelly.

Mr. ARMSTRONG. All right. Sorry about that. Can you hear me?

Mr. DOYLE. Yes. We can hear you.

Mr. ARMSTRONG. All right. Thank you.

No other industry receives such bipartisan scrutiny—disinformation, content moderation, deplatforming, antitrust, privacy, and the list continues to grow. We discuss these things too often in isolation, but they are all related, and it starts with the fact that your users aren't your customers. They are the product. More specifically, the data that you collect from your users is the product.

You are incentivized to collect and monetize user data for behavior advertising. This results in the collection of even more user data. And data is unique as a business asset. It doesn't deplete. Data is perpetual and reinforcing. Data begets more data. Massive

data collection expands your market share, which harms competition.

That is why censorship is so concerning to all of us. Your platforms have a stranglehold on the flow of modern communication, and I think we absolutely have to resist the urge of content moderation and censorship. In 1927, Justice Brandeis wrote: "The remedy to apply is more speech, not enforced silence." I think that statement still holds true today.

Yet your platforms don't simply silence certain speech. Your algorithms are designed to reinforce existing predispositions because you profit by keeping users locked into what they already enjoy. This leads to information siloes, misinformation, extremism on both sides, and even more data collection, which repeats the cycle.

Mr. Pichai, you testified before the House Judiciary Committee last year, and at that hearing I raised several examples of Google's consolidation of the ad tech stack. Your answers large reiterated the privacy justifications, which I understand and support. However, my question was whether Google's consolidation of both the buy and sell sides of digital advertising would further harm competition.

Since then I have reviewed Google's privacy sandbox and the FLoC proposal, which is an alternative group identifier to replace third-party cookies. Again, I understand and I appreciate the privacy justification. But—and this is my question: How will these actions not further entrench Google's digital advertising market share and harm competition?

Mr. PICHAI. Congressman, as you rightfully point out, privacy is really important, and we are trying to get that correct. Users are giving clear feedback in terms of the direction they would like to take. Advertising allows us to provide services to many people who wouldn't otherwise be able to use services, and we are trying to provide relevant ads, protecting their privacy. And that is what FLoC is working on. We will—

Mr. ARMSTRONG. I am going to move on because I understand the privacy. I understand the privacy. And I understand the rationale of eliminating individual-level tracking in favor of cohorts and the potential privacy benefits of user data in CRO method device level.

But this is still eliminating competitors' access to user data at a time when you already control 60 percent of the browser market. I have real concerns that FLoC will incentivize more first-party data collection, which will not actually benefit user privacy. Instead of spreading it amongst a lot of different companies, it will just all be with you. And so I guess my point is Congress needs to conduct careful oversight as the privacy sandbox and FLoC are introduced. And we need to ensure that the user privacy increases and that competition is not stifled further.

But I do have one question, and it is important. I am going to ask all three of you. When we are conducting competition analysis in the tech industry, should nonprice factors like privacy be considered? And I will start with you, Mr. Pichai.

Mr. PICHAI. I think so. I think privacy is very important, and we have called for comprehensive Federal privacy legislation. And to clarify, Google doesn't get any access to FLoC data. It is protected. And then we will publish more papers on it.

Mr. ARMSTRONG. All right. And I understand completely. But you are forcing—I mean, you are forcing advertisers into the ad stack. I mean, that is—I don't discount it increases privacy. That is not—I think this is a real problem because I think they are in conflict with each other.

But Mr. Dorsey, do you think when we are conducting competition analysis in the tech industry, nonprice factors should be considered?

Mr. DORSEY. Not sure exactly what you mean, but open to further discussion on it.

Mr. ARMSTRONG. All right. How about you, Mr. Zuckerberg?

Mr. ZUCKERBERG. Yes, Congressman. My understanding is that the law already includes the quality of products in addition to price.

Mr. ARMSTRONG. And I will just say I appreciate you talking about the difference between big platforms and small platforms because I think in our history of trying to regulate big companies, Congress has already done a really good job at harming the smaller companies worse.

And with my last 6 seconds because this isn't the appropriate hearing, but I am going to ask: Please all do a better job of making sure artists get paid for their work on your platforms. And with that, I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Mr. Veasey for 5 minutes.

Mr. VEASEY. Thank you, Mr. Chairman.

It has often been said that lies travel faster than truth, and we have seen that play out with devastating consequences on social media platforms today. This concerns me greatly, not just as a father or a lawmaker but as someone ready to see the past divisions that have dominated our country for the past several years, and really decades, really.

But it is hard to see how this can change when the CEOs of the largest social media platforms repeatedly say they will fix their ways, only to keep spreading harmful lies and misinformation. I want to give you an example.

Last August here in the Dallas/Fort Worth area, the North Texas Poison Control Center felt the need to warn people against ingesting bleach or other disinfecting products as a cure to prevent COVID-19. Despite efforts of your companies to take down such harmful mis- or disinformation calls to the North Texas Poison Control Center about disinfectant, ingestion rates were much higher than usual and statewide calls about bleach products were up over 70 percent compared to the year before. The North Texas Poison Center pointed this out largely to misinformation online as the cause for these increases.

And as we know, in the lead-up to the last elections Black communities were specifically targeted for disinformation campaigns designed to suppress the vote, especially in battleground States. And right now there are sites up that are discouraging Black people from getting the COVID-19 vaccination. I know a lady that was put in Facebook jail for 30 days because all she did was repost one of the faulty posts saying Black folks aren't falling for this business, and she was put in Facebook jail for 30 days.

Now, even if these posts were eventually taken down or otherwise labeled as false, again, lies travel a lot faster than truths. Your companies have been largely flat-footed when it comes to getting out ahead of these issues, and it is time for something to change.

That is why I am exploring legislation that would establish an independent organization of researchers and computer scientists who could help by identifying and warn about misinformation trends before they become viral. This early-warning system would help social media sites, the public, and law enforcement so that when dangerous conspiracies or disinformation is spreading, they can be on alert and hopefully slow its effect.

Mr. Zuckerberg, would you support legislation that would alert all Facebook or Instagram users of harmful disinformation and conspiracy theories spreading across your platforms?

Mr. ZUCKERBERG. Congressman, I think we need to look into that in more detail to understand the nuances. But in general, I agree that it is our responsibility to build systems that can help slow the spread of this kind of misinformation. And that is why we have taken all the steps that I have outlined today, from building in an unprecedented independent fact-checking program to taking down content that could cause imminent physical harm to the work in the COVID Information Center and the Voting Information Center and the Climate Information Center to promote authoritative information across our services. So I certainly think that there is a lot to do here.

Mr. ARMSTRONG. Mr. Dorsey, would you support legislation for an early-warning system across Twitter?

Mr. DORSEY. I would be open to reviewing the details. I just don't think it will be effective. And it will be very much Whac-a-mole. I think that the more important thing is to, as I said in my opening remarks, get much more of an open standard and protocol that everyone can have access to and review.

Mr. ARMSTRONG. And Mr. Pichai? For Google and YouTube and that? I have a 14-year-old at home that watches YouTube. What about you for those platforms?

Mr. PICHAI. Already today in many of these areas, we show, proactively, information panels. So for example on COVID, we have showed a lot of information from CDC and other experts, and we had views of over 400 billion. And so conceptually, showing proactive information, including information panes, I think makes sense to me.

Mr. ARMSTRONG. OK. Well, thank you. I appreciate the time, Mr. Chairman. I am worried. I think that we need to act quickly and that we are running out of time and that we need these companies to take affirmative action on addressing some of these issues.

I yield back my time. Thank you.

Mr. DOYLE. I thank the gentleman. The gentleman yields back.

The Chair now yields 5 minutes to Ms. Craig.

Ms. CRAIG. Thank you so much, Mr. Chair.

Mr. Zuckerberg, thank you so much for joining us today. As co-chair of the LGBTQ Equality Caucus in the U.S. Congress, I would like to ask you a few questions about an incident that occurred several weeks ago now. And I would appreciate a simple yes-or-no an-

swer. Most of these have absolutely no room for nuance. These aren't trick questions. I would just like to clarify a few facts.

So on February 25th, Facebook took down a video hosted by my colleague Representative Marie Newman in which she places the transgender flag outside her office. Is that correct, to your knowledge? Yes or no?

Mr. ZUCKERBERG. Congresswoman, I am not aware of this.

Ms. CRAIG. You are not aware of this?

Mr. ZUCKERBERG. No.

Ms. CRAIG. Well, the answer is yes. Facebook took her video down. According to Representative Newman, the reason Facebook gave for taking down the video was that it violated Facebook's community standards on hate speech and inferiority. Does that seem right to you, that if someone put up a trans flag and took a video of it and posted it on your platform, that it should be put down?

Mr. ZUCKERBERG. Congresswoman, no. That doesn't seem right to me. But I would need to understand the specifics of the case in more details.

Ms. CRAIG. Yes. Thank you. The answer is no, it is absolutely not right.

Meanwhile, across the hall, Representative Marjorie Taylor Greene from Georgia posted a video to Facebook. Her video showed her putting up a transphobic sign so that Representative Newman, the mother of a trans child, could "look at it every time she opens her door." Facebook allowed Representative Greene's video to remain online. Is that right? Yes or no?

Mr. ZUCKERBERG. Congresswoman, I am not aware of the specifics. But as I have said a number of times today, we do make mistakes, unfortunately, in our content moderation, and we hope to fix them as quickly as possible—

Ms. CRAIG. Reclaiming my time, reclaiming my time. The answer was yes, Representative Greene's video was allowed to remain online. Representative Newman reached out to Facebook, and a few hours later her video was restored with a perfunctory apology. But Representative Greene's video was never taken down. I am not even going to ask you if I am getting that right, as I was, because you obviously don't know.

Are you aware that Facebook has repeatedly flagged the transgender flag as hate speech and that trans-positive content ends up being taken down while transphobic content, like Representative Greene's video, is not taken down and is often shared widely? Yes or no?

Mr. ZUCKERBERG. Congresswoman, I am now aware of that specifically, but this is an instance of a broader challenge in identifying hate speech, which is that there is often a very nuanced difference between someone saying something that is racist versus saying something to denounce something that someone else said that was racist.

And we need to build systems that handle this content in more than 150 languages around the world, and we need to do it quickly. And, unfortunately, there are some mistakes in trying to do this quickly and effectively.

Ms. CRAIG. Mr. Zuckerberg, I am going to give you your nuance this one time.

As it exists today, do you think your company is going to get these content moderation decisions right on the first try eventually?

Mr. ZUCKERBERG. Congresswoman, if what you are asking is are we ever going to be perfect, the answer is no. I think that there will always be some mistakes, but I think we will get increasingly accurate over time. So for example, a few years back, we identified—

Ms. CRAIG. Mr. Zuckerberg, I only have a couple of minutes, or 1 minute left, so I am going to continue here.

As has been mentioned repeatedly throughout today, we just don't have faith that your companies have the proper incentives to proactively contemplate and address basic human rights. With that in mind, would you support legislation requiring social media companies to have an Office of Civil Rights reporting to the CEO, and that would mean you would have to reconsider your corporate structure, including the civil rights and human rights of the trans community?

Mr. ZUCKERBERG. Congresswoman, we took the unprecedented step of hiring a VP of civil rights, and I think we are one of the only companies that has done something similar to what you are saying.

Ms. CRAIG. Well, I hope that you do better, then, because this example I am giving you was completely unacceptable. This panel has done something truly rare in Washington these days: It has united Democrats and Republicans. Your industry cannot be trusted to regulate itself.

And with that, I yield back.

Mr. DOYLE. The gentlelady yields back.

The Chair now recognizes Mrs. Trahan for 5 minutes.

Mrs. TRAHAN. Thank you, Mr. Chairman.

I would like to turn the focus back to our children. My husband and I have five. Our oldest is 27, our youngest is 6, and over the years I have noticed how technology has been increasingly designed to capture their attention. The more time my first-grader spends scrolling through an app, the less time she is playing outside or enjoying face-to-face interactions with us.

Google and Facebook are not only doing a poor job of keeping our children under 13 off of YouTube and Instagram, as my colleagues have already mentioned today, but you are actively onboarding our children onto your ecosystems with apps like YouTube Kids, Facebook Messenger Kids, and now we are hearing Instagram for Kids. These applications introduce our children to social media far too early and include manipulative design features intended to keep them hooked.

Mr. Pichai, when a child finishes a video on YouTube or YouTube Kids, does the next video automatically play by default? And I think this one is a yes or no.

Mr. PICHAI. Sorry, I was muted. Congresswoman, I have children, too. I worry about the time they spend online, and I agree with you it is an important issue.

Mrs. TRAHAN. Yes.

Mr. PICHAI. We design YouTube—

Mrs. TRAHAN. The autoplay function by default? That is a yes—

Mr. PICHAI. On the main app, it is there, and for each video there is an easy on/off toggle. Users have preference to select—

Mrs. TRAHAN. But the default setting is yes. When a user who is predicted to be a teen is watching a YouTube video, are the number of likes displayed by default? Yes or no, please?

Mr. PICHAI. On all videos, I think we do have—across all videos we have.

Mrs. TRAHAN. Right. And Mr. Zuckerberg, will the recently reported Instagram app for kids have endless scroll enabled? Yes or no?

Mr. ZUCKERBERG. Sorry. Congresswoman, we are not done finalizing what the app is going to be. I think we are still pretty early in designing this. But I just want to say that—

Mrs. TRAHAN. Are you not sure or are you not sharing features or—and look, another feature of concern is the filter that adds an unnatural but perfect glow for my 10-year-old to apply to her face. Is that feature going to be part of Instagram for Kids?

Mr. ZUCKERBERG. Congresswoman, I don't know. I haven't discussed this with the team yet.

Mrs. TRAHAN. Well, look, please expect my office and many others to follow up, given what we know about Instagram's impact on teen mental health. We are all very concerned about our younger children.

And I just want to speak mother to father for a moment, fathers, because leading experts all acknowledge that social media sites pose risks to young people—inappropriate content, oversharing of personal information, cyberbullying, deceptive advertising—the list goes on. And those risks are exacerbated with more time children spend in these apps.

Mr. Pichai, you mentioned that you have children, and I have also read you limit their screen time. What do you say when one of your children doesn't want to put their phone down?

Mr. PICHAI. Congresswoman, the struggle is the same, particularly through COVID. It has been hard to moderate it. And I do take advantage of the parental controls and the digital well-being tools. We can limit the time on their apps. And so we have prohibitions in place.

Mrs. TRAHAN. I don't mean to cut you off, Mr. Pichai. But the last thing overworked parents need right now—especially right now—are more complex to-dos, which is what parental controls are. They need childcentric design by default.

Mr. Zuckerberg, I understand your children are younger. But when they start using social media, what will you say when they are craving their tablet over spending time face to face with you or with friends?

Mrs. TRAHAN. Well, Congresswoman, we haven't gotten to that point yet. But we are designing all of these tools—we designed Messenger Kids that the parents are in control. I think we have proven that that can be a good and safe experience. And I think that was one of the things that made us think that we should consider doing this for Instagram as well, by having it so that we have

a parent-controlled experience and, as you say, childcentric experience for people under the age of 13—

Mrs. TRAHAN. I am going—I am going to reclaim my time, only because. Connecting with others is one thing. Adding filters, no breaks for kids to take, and manipulating the design of these apps for our children is another. Look, this committee is ready to legislate to protect our children from your ambition.

What we are having a hard time reconciling is that, while you are publicly calling for regulation—which, by the way, comes off as incredibly decent and noble—you are plotting your next frontier of growth, which deviously targets our young children and which you all take great strides, with infinitely more resources, in protecting your own children.

This playbook is familiar. As some of my colleagues have pointed out, it is the same tactic we saw from alcohol companies and Big Tobacco: Start 'em young and bank on them never leaving, or at least never being able to. But these are our children, and their health and well-being deserve to take priority over your profits.

Mr. DOYLE. The gentlelady's time is expired.

The Chair now recognizes Mrs. Fletcher for 5 minutes.

Mrs. FLETCHER. Thank you, Chairman Doyle. And thanks to you and Chairwoman Schakowsky and Ranking Members Latta and Bilirakis for holding this hearing today. I agree with my colleagues. There is a broad consensus on a range of issues, and I appreciate the discussion.

As we have discussed extensively today, one of the big challenges of this rise of dangerous disinformation is that it denies us a basic set of shared facts to enable an informed debate like what we are having here today. And it is absolutely vital that we take charge and that we address this.

What we have seen is that countries whose interests are not aligned with ours, extremist organizations and others, have used online social media platforms to engage and to amplify extremist content and disinformation, from the COVID-19 pandemic to the January 6 insurrection, both of which we have talked about extensively.

We have seen that the real-world cost of this unchecked spread of disinformation is in lies. And like my colleagues, I worry that the structure of many social media companies, including those we have before us today, prioritize engagement, including engagement with provocative or extremist content, over responsible corporate citizenship.

So one of my greatest concerns regarding how extremist content and disinformation is allowed to spread on your platform is the lack of data transparency when it comes to independent analysis. Now, everyone has claimed they have an internal system, that it is about the systems, that you need good systems to remove and delete disinformation and extremist content.

But we have no way to verify how effective those systems are. And that is a huge part of the challenge before us. I think we all would agree that we need data and information to make good policy and to write good legislation which will be coming out of this committee.

So that brings me to a followup on my colleague Miss Rice's questions about data. As she mentioned, and it is my understanding that all three of your platforms chose to remove content that was posted regarding the Capitol insurrection on January 6. And I think we can all understand some of the reasons for that. But as a result, it is unavailable to researchers and to Congress.

So my question for each of you is: Will you commit to sharing the removed content with Congress to inform our information of the events of January 6 and also the issues before us today about how to respond to extremist and dangerous content online?

And I will start with Mr. Zuckerberg.

Mr. ZUCKERBERG. Thanks, Congresswoman. When we take down content that might be connected to a crime, I think we do, as a standard practice, try to maintain that so that we can share it with law enforcement if necessary. And I am sure our team can follow up to discuss that with you as well.

Mrs. FLETCHER. Sure. I appreciate that. And I understand that you have a legal obligation to cooperate with authorities and law enforcement in these cases. And I think that what I am talking about is also sharing it with us in Congress, and I appreciate your response there.

Mr. Dorsey?

Mr. DORSEY. We would like to do this, actually. We have been thinking about a program for researchers to get access to actions that we had to take. But all of this is subject to local laws, of course.

Mrs. FLETCHER. Well, and that may be something that we can help craft here. So I think that it is consistently something we have heard from researchers as well. It is a real area of challenge in not having the data. So I appreciate that.

And Mr. Pichai? Do you also agree?

Mr. PICHAI. Congresswoman—sorry, I was muted—we are working with law enforcement, and happy to connect with your office. And we cooperate as allowed by law while balancing the privacy of the people involved.

Mrs. FLETCHER. Well, thank you. So I appreciate all of your willingness to work with us and to assist Congress in addressing this attack on our Capitol and our country.

Another idea that I would like to touch base with you on in the time I have left, just over a minute, is the difference we see in how your platforms handle foreign extremist content versus domestic content. By all accounts, your platforms do a better job of combating posts and information from foreign terrorist organizations, or FTOs, like ISIS or al-Qaeda and others, where the posts are automatically removed, depending on keywords and phrases, et cetera.

The FTOs are designated by the State Department. There are rigorous criteria to identify groups that wish to cause harm to Americans. Currently there is no legal mechanism or definition for doing the same for domestic terror and hate groups.

Would a Federal standard for defining a domestic terror organization similar to FTOs help your platforms better track and remove harmful content from your sites? Mr. Zuckerberg?

Mr. ZUCKERBERG. Congresswoman, I am not sure. I think domestically we do classify a number of white supremacist organizations and militias and conspiracy networks like QAnon as the same level of problematic as some of these other organizations that are able to take decisive action.

I think where this ends up being more complicated is where the content is—

Mrs. FLETCHER. I hate to cut off, but I am going to run out of time. So your answer was, “I am not sure.” Could I just get a quick yes or no from Mr. Dorsey and Mr. Pichai?

Mr. DOYLE. Yes, but very quickly because your time is expired. Very quickly.

Mr. DORSEY. We need to evaluate it. We need to understand what that means.

Mrs. FLETCHER. Mr. Pichai?

Mr. PICHAI. We as domestic agencies focus on that, I think we are happy to work and cooperate there.

Mr. DOYLE. OK. The gentlelady’s time is expired.

Mrs. FLETCHER. Well, thank you very much, Mr. Chairman. I yield back.

Mr. DOYLE. It is my understanding we have—let’s see—eight Members who were requesting to waive on for the hearing. I believe we have given all members of the subcommittees their opportunity to speak. So we will now start to recognize the Members waiving on. And first on the list here I see Mr. Burgess.

Doc Burgess, are you with us?

Mr. BURGESS. Yes. Sorry. I couldn’t find my cursor.

Mr. DOYLE. OK. You are recognized for 5 minutes.

Mr. BURGESS. Thank you, Mr. Chairman. And thanks to our witnesses for spending so much time with us. This is clearly a very important issue to every member of this committee regardless of which political party they identify with.

I guess, Mr. Zuckerberg, let me just ask you a question because it strikes me, listening to your answers to both our colleague Jeff Duncan and our colleague Angie Craig—both coming at the issue from different directions—but the concern is that there was the exercise of editorial authority over the postings that were made on your website. Is that a fair assessment?

Mr. ZUCKERBERG. Congressman, I am not sure what you mean. But I think content moderation and enforcing standards, I don’t think that that is the same kind of editorial judgment that, for example, a newspaper makes when writing a post.

Mr. BURGESS. Yes. But maybe it is, because Mr. Duncan eloquently pointed out there was restriction of conservative speech. And our colleague, Angie Craig, eloquently pointed out how there was restriction of trans-affirming speech. So that strikes me that we are getting awfully close to the line of exercising editorial discretion.

And forgive me for thinking that way, but if that is—and I am sure I am not alone in this—it does call into question, then, the immunity provided under Section 230. Maybe it is not a problem with the law itself, Section 230. Maybe the problem is that the mission has changed in your organization and other organizations.

Mr. ZUCKERBERG. Congressman, I am not sure what you mean. But we have clear standards against things like terrorist content, child exploitation, incitement of violence, intellectual property violations, pornography—things that I would imagine that you agree with. And we can enforce—

Mr. BURGESS. All spelled out in the plain language of Section 230. But again, you are putting restrictions on conservative speech. Mr. Duncan eloquently pointed out how that is occurring. Angie Craig eloquently pointed out how you are putting restrictions on trans-affirming speech. None of those fall into any of the other categories that you are describing.

Because to the casual observer, it appears that you are exercising editorial authority, and as such maybe you should be regulated as a publisher as opposed to simply someone who is carrying—who is indifferent to the content that they are carrying.

Mr. ZUCKERBERG. Congressman, I think one of the virtues of Section 230 is it allows companies to moderate things like bullying that are not always clearly illegal content but that I think you and I would probably agree are harmful and bad.

So I think it is important that companies have the ability to go beyond what is legally required. I do not think that that makes these internet platforms the same thing as a news publisher who is literally writing the content themselves. I do think we have more responsibility than maybe a telephone network, where—

Mr. BURGESS. Let me interrupt you in the interest of time because I want to pose the same question to Mr. Dorsey.

Mr. Dorsey, every Presidential tweet that I read following the election had an editorial disclaimer appended to it by you. How does that not make you someone who is exercising editorial discretion on the content that you are carrying?

Mr. DORSEY. Our goal with our labels was simply to provide connection to other data and provide context.

Mr. BURGESS. Yes. But you don't do that routinely with other tweets. It seemed to be a singular assignment that someone had taken on, to look at whatever the President is publishing. "We are going to put our own spin on that." And again, that strikes me as an editorial exercise.

And the only reason I bring this up and we are going to have these discussions, I recognize that smaller companies just starting out, the protection of Section 230 may be invaluable to them. But you all are no longer just starting out. You are established. You are mature companies. You exercise enormous control over the thought processes of not just an entire country but literally the entire world. You are exercising editorial discretion. I do think we need to revisit Section 230 in the terms of, have you now become actual publishers as opposed to simply carriers of information?

Thank you, Mr. Chairman. I will yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Mr. Tonko for 5 minutes.

Mr. TONKO. Thank you, Mr. Chair. Thank you for allowing me to waive on.

Gentlemen, thank you for being with us today. While there are many issues I would like to raise with you, my most pressing unresolved questions revolve around what I saw and experienced on

January 6, when I had to dive for cover in the House gallery as violent insurrectionists attempted to break down the doors and take the chamber.

The rioters who breached the Capitol building were propelled by at least one bully that the election had been stolen from former President Donald Trump. They reached this false and dangerous conclusion, yet somehow in massive numbers. Their assault was not disorganized or isolated, and it was not coincidence.

So Mr. Zuckerberg, you and your colleagues have downplayed the role Facebook played in helping the rioters mobilize on January 6. In light of growing evidence that suggests otherwise, including the fact that Facebook was the most cited social media in charging documents the Department of Justice filed against insurrectionists, do you still deny that your platform was used as a significant megaphone for the lies that fueled the insurrection?

Mr. ZUCKERBERG. Congressman, to be clear, I think part of the reason why our services are very cited in the charging docs is because we worked closely with law enforcement to help identify the people who were there. So I don't view that that collaboration with law enforcement should be seen as a negative reflection on our services.

And as I have said a number of times to today, there was content on our services from some of these folks. I think that that was problematic. But by and large, I also think that by putting in place policies banning QAnon, banning militias, banning other conspiracy networks, we generally made our services inhospitable to a lot of these folks. And that had the unfortunate consequence of having those folks not use Facebook and use other places as well.

So there is certainly more for us to do. But I stand behind the work that we have done with law enforcement on this and the systems that we have in place.

Mr. TONKO. Thank you.

Mr. Pichai, can you affirmatively state that YouTube did not recommend videos with Stop the Steal content, white supremacy content, and other hate and conspiracy content that was seen by rioters at the Capitol?

Mr. PICHAI. Congressman, we had clear policies and we were vigorously enforcing this area. Just leading up to the election, we had removed hundreds of thousands of videos, and we had terminated 8,000 channels. And on the day of the riot, we were successfully able to take down inappropriate livestreams. We gave precedence to journalistic organizations covering the event. And that is the content we raised up on YouTube that day. And since then we have been cooperating with law enforcement as well.

Mr. TONKO. So you're indicating that you did not recommend videos with Stop the Steal?

Mr. PICHAI. We were rigorously enforcing. We had clear policies around content that undermined election integrity. Once the States certified the election on December 8th, we introduced a Sensitive Events policy and we did take down videos which were violative. And so we have been monitoring it very closely.

Mr. TONKO. Thank you.

And Mr. Dorsey, are you confident that the conspiracy theorists or other purveyors of electoral misinformation and Stop the Steal on Twitter were not recommending to others?

Mr. DORSEY. I can't say that I was confident, but I know we did work really hard to make sure that if we saw any amplification that went against the terms of service, which this would, we took an action immediately. We didn't have any up-front indication that this would happen, so we had to react to it quite quickly.

Mr. TONKO. All right. Thank you. And who and what content your platforms recommend have real-world consequences, and the riot caused five deaths and shook our democratic foundations. And I believe that your platforms are responsible for the content you promote, and look forward to working with my colleagues to determine how to hold you accountable.

Mr. Pichai, Google and YouTube often slip under the radar as a source of disinformation. But in the last election, bad actors used ads on Google Search to scam people looking for voting information, and YouTube failed to remove videos that spread misinformation about the 2020 vote results.

So Mr. Pichai, when journalists pointed out in November that election misinformation was rampant on Google's YouTube, the company said it was allowing discussions of election processes and results. A month later YouTube said it would remove new content alleging widespread voter fraud in the 2020 election. Why did YouTube wait a month to take action on election misinformation?

Mr. PICHAI. If I could clarify here, we were taking down videos leading up to the election. There is obviously a month from the date of election till there are due processes, co-challenges, and we waited till this—we consulted with CISPA and Association of Secretaries of State. And on December 8, when the States certified the election, we started enforcing newer policies on December 9th.

To be very clear, we were showing information from the Associated Press, and we were proactively showing information high up in our search results to give relevant information throughout this election cycle.

Mr. DOYLE. The gentleman's time is expired.

Mr. TONKO. Thank you. Mr. Chair, I yield back.

The Chair recognizes Mr. McKinley for 5 minutes.

Mr. MCKINLEY. Thank you, Mr. Chairman, and this panel. You all have to be exhausted after being grilled all day long like this.

So my questions are to Mr. Zuckerberg.

When you came before our committee in 2018, you acknowledged that Facebook had used what you just said, "clear standards," preventing the sale of illegal drugs on your site. But you were shown examples of active posts that traffickers were still using that platform unlawfully to sell prescription opioids. You did apologize and confirm that "social media companies need to do a better job of policing these posts."

Now, 3 years later it appears a shell game is emerging. Facebook seems to have cleaned up its act, but you are now allowing Instagram, one of your subsidiaries, to become the new vehicle. Even though Instagram has the same policies against the sale of illegal substances, you are still allowing bad actors to push pills on your site.

It didn't take long for our staff to find numerous examples. For example, here is oxycodone that is being sold on your site. Here is Ritalin that is being sold on your site. Here is Xanax and Adderall that is being sold on your site. So these posts have—they are not new. They have been active since last fall.

If we can find posts this easily, shame on you for not finding them for yourself. Apparently you are not taking the warnings of Congress seriously. After drug manufacturers dumped millions of pills in our community, killing thousands, ravaging families, and destroying livelihoods, Congress responded by passing laws to hold them liable.

If a retail store is selling cigarettes to underage kids, that store is held liable. So why shouldn't you be held liable as well? Do you think you are above the law? You are knowingly allowing this poison to be sold on your platform into our communities, to our children, to our vulnerable adults.

Look. I have read Scott Galloway's book "The Four." I encourage all the members on this committee to read his book. It is a perfect depiction of the arrogance of Big Tech companies like Facebook, Google, Apple, and Amazon. He develops a very compelling argument as to why Big Tech companies should be broken into smaller companies, much like that occurred to AT&T in 1984.

Maybe it is time for Congress to have an adult conversation about this loss of liability protection and the need to reform our antitrust laws. I don't think Congress wants to tell you how to run your company, but maybe it should.

So Mr. Zuckerberg, let me close with this one question: Don't you think you would find a way to stop these illegal sales on your platforms if you were held personally liable?

Mr. ZUCKERBERG. I keep on getting muted.

Congressman, we don't want any of this content on our platforms, and I agree with you that this is a huge issue. We have devoted a lot of resources and have built systems that are largely quite effective at finding and removing the content. But I just think that what we all need to understand is that at the scale that these communities operate, where people are sharing millions or, in messages, billions of things a day, it is inevitable that we will not find everything, just like a police force in a city will not stop every single crime.

Mr. MCKINLEY. I agree.

Mr. ZUCKERBERG. So I think that we should—

Mr. MCKINLEY. But I ask you the question very directly, Mark. Should you not be held liable when people are dying because your people are allowing these sales to take place? We did it with manufacturers. We do it to the stores. Why aren't we doing it to the salesman that allows this to take place?

Mr. ZUCKERBERG. Well, Congressman, I don't think we are allowing this to take place. We are building systems that take the vast majority of this content off our systems. And what I am saying—

Mr. MCKINLEY. We have been dealing with this for 3 years, Mark. Three years this has been going on. And you said you were going to take care of it last time, but all you do is switch from Facebook over to Instagram. They are still doing it now. And you are saying "We need to do more."

Well, how many more families are going to die? How many more children are going to be addicted while you still study the problem? I think you need to be held liable.

Mr. ZUCKERBERG. Congressman, we are not sitting and studying the problem. We are building effective systems that work across both Facebook and Instagram. But what I am saying is that I don't think that we can expect that any platform will find every instance of harmful content. I think we should hold the platforms to be responsible for building generally effective systems at moderating these kinds of content.

Mr. DOYLE. The gentleman's time is expired.

Mr. MCKINLEY. I am not going to get an answer, Mike. Thank you.

Mr. DOYLE. The gentleman yields back. The Chair recognizes Ms. Blunt Rochester for 5 minutes.

Ms. BLUNT ROCHESTER. Thank you, Mr. Chairman, for allowing me to waive onto this important hearing. And thank you to the witnesses.

I want to focus on two areas: first, a consumer protection and safety issue, and second, more broadly, manipulation and privacy of our data.

On consumer protection and safety, earlier this year two infants from two different families ended up in the intensive care unit in Wilmington, Delaware, after being fed homemade baby formula based on instructional videos viewed on YouTube. One infant suffered from cardiac arrest that resulted in brain damage.

For years, the American Academy of Pediatrics has warned parents against homemade baby formulas because it puts infants at risk of serious illness and even death. And since at least 2018, the FDA has recommended against the use of homemade formula. Even as recent as 29 days ago, the FDA issued an advisory against homemade formula.

In February, my office informed your team, Mr. Pichai, and as a followup I have sent a letter requesting information and action on this issue in the hopes of a response by April 1st. Mr. Pichai, this is just a yes-or-no question: Can I count on a response to my letter by the deadline of April 1st?

Mr. PICHAI. Congresswoman, definitely yes. Heartbreaking to hear the stories. We have clear policies. Thanks for your highlighting this. I think the videos have been taken down, and we are happy to follow up and update the team.

Ms. BLUNT ROCHESTER. We checked today. For years, these videos have clearly violated your own stated policy of banning the videos that endanger the, as you say, "physical well-being of minors." And so I am pleased to hear that we will be hearing back from you.

And while we are considering Section 230, what is clear from this hearing is that we should all be concerned by all of your abilities to adequately—and just as importantly, rapidly—moderate content. In some of these cases, we are talking life and death.

Second, as many of my colleagues have noted, your companies profit when users fall down the rabbit hole of disinformation. The spread of disinformation is an issue all of us grapple with from all across the political spectrum. Disinformation often finds its way to the people most susceptible to it because the profiles that you cre-

ate through massive data collection suggest what they will be receptive to.

I introduced the DETOUR Act to address common tactics that are used to get such personal data as possible. And these tactics are often called “dark patterns,” and they are intentionally deceptive user interfaces that trick people into handing over their data.

For the people at home, many of you may know this as when you go on an app, it doesn’t allow you to have a No option, or it will insinuate that you need to do something else, install another program like Facebook Messenger app to get on Facebook.

You all collect and use this information. Mr. Pichai, yes or no: Would you oppose legislation that banned the use of intentionally manipulative design techniques that trick users into giving up their personal information?

Mr. PICHAI. We definitely are happy to have oversight on these areas and explain what to do.

Ms. BLUNT ROCHESTER. Thank you. I have to go to Mr. Dorsey. Mr. Dorsey, yes or no?

Mr. DORSEY. Open to it.

Ms. BLUNT ROCHESTER. Mr. Zuckerberg?

Mr. ZUCKERBERG. Congresswoman, I think the—

Ms. BLUNT ROCHESTER. Yes or no, please.

Mr. ZUCKERBERG [continuing]. Principle makes sense, and the details matter.

Ms. BLUNT ROCHESTER. OK. Mr. Zuckerberg, your company recently conducted this massive ad campaign on how far the internet has come in the last 25 years. Great ad. You end it with a statement: “We support updated internet regulations to address today’s challenges.” Unfortunately, the proposal that you direct your viewers to fails to address dark patterns, user manipulation, or deceptive design choices.

Mr. Zuckerberg, will you commit now to include deceptive design choices as part of your platform for better internet regulations?

Mr. ZUCKERBERG. Congresswoman, I will think about it. My initial response is that I feel there are other areas that I think might be more urgently in need.

Ms. BLUNT ROCHESTER. That might be your—if you say this is a desire of yours to address the issues that we face today, dark patterns goes back to 2010, this whole issue of deceptive practices. And I hope that you will look into it.

I will say—Mrs. Trahan and others have mentioned—she mentioned our children. Others have mentioned seniors, veterans, people of color, even our very democracy, is at stake here. We must act and assure you—we will assure you we will act.

Thank you so much, and Mr. Chairman, I yield back 6 seconds.

Mr. DOYLE. I thank the gentlelady. The gentlelady yields back. And now the Chair recognizes Mr. Griffith for 5 minutes.

Mr. GRIFFITH. Thank you very much, Mr. Chair.

According to new data from the National Center for Missing and Exploited Children, Siler Pythian found the vast majority of child exploitation reports from Big Tech sites. Facebook had the most, 20.3 million. Google was second with 546,000-plus. Twitter had 65,000-plus. Put in perspective, MindGeek, the Canada-based parent company of major portion websites, had 13,229. Facebook

claims 90 percent of the flagged incidents were duplicates. All right. Let's accept that. That still leaves over 2 million incidents—2 million incidents.

Mr. Zuckerberg, yes or no, does Facebook have a problem with child exploitation on its platform?

Mr. ZUCKERBERG. Congressman, this is an area that we work on a lot. But the recent why those numbers are so high is because we are so proactive about trying to find this and send it to NCMEC and others who are doing good work in this area. We send content and flags over to them quite liberally, whenever we think that we might see that something is at issue.

And that is, I think, what the public should want us to do, not criticize us for sending over a large number of flags but should encourage the companies to do it.

Mr. GRIFFITH. So you are admitting that you all have a problem, and this is one way you are trying to work on it.

Mr. Pichai, yes or no: Do you agree with Mr. Zuckerberg that you all have a problem? Are you there?

Mr. PICHAI. Congressman, sorry, I was muted. This is an area which we invest very heavily. We have been praised by several authorities. We work proactively—

Mr. GRIFFITH. So the answer is yes.

Mr. Dorsey, yes or no: Do you agree?

Mr. DORSEY. If we see any problems, we try to resolve them as quickly as possible.

Mr. GRIFFITH. But you do have problems, and that is why you are trying to resolve them. I get that. The problem is, when you are talking about millions of incidents, and we take 90 percent of them as duplicates from the Facebook data, that is millions of incidents that are happening where our children are being exploited with child pornography on you all's sites. We have got to do better.

I think you all need, for everything that we have talked about today, an independent industrywide review team like the electronic industry did with the Underwriters Laboratory nearly 150 years ago. I told you all that when you were here before. Nobody has done anything. I don't think it needs to be within your company. I think it needs to be outside.

And on that vein, I would say to Google, special permission was given to Moonshot CVE to target ads against extremist keywords. Moonshot then directed thousands of individuals who searched for violent content to videos and posts of a convicted felon who espouses anti-law-enforcement, anti-Semitic, and anarchist viewpoints.

Mr. Pichai, are you aware of this problem?

Mr. PICHAI. Congressman, I am not aware of the specific issue. Last year we blocked over 3.1 billion bad ads, 6,000 ads per minute. And so we enforce vigorously. But I am happy to look into this specific issue and follow up back with you.

Mr. GRIFFITH. Well, here is what happened. You partnered with an outside group that didn't do their job. What are your standards when you partner with an outside group? What are your standards, and what are your philosophy? Because they sent people who were already looking for violence to a convicted felon with anarchist and anti-Semitic views.

Mr. PICHAI. There is no place for hate speech, and I am disappointed to hear of this. We will definitely look into it and follow up back with you.

Mr. GRIFFITH. Well, and I appreciate that. I recognize that. But I have the same concerns that Mr. McKinley had. And you weren't here last time, but we heard these same kinds of things about how "we are going to work on it" and how "we are going to get these problems resolved." And I forget when that hearing was, but a year or so ago.

And yet we continue to have the same problems, where political candidates' information is being taken down because for some reason it is flagged, where conservatives and people on the left are being hit and taken down. And I agree with many of the sentiments on both side of the aisle that, if you all aren't doing anything and it appears that you are not moving fast enough, we have no choice in Congress but to take action.

I don't want to. I would rather see you all do it, like the electric industry did with Underwriters Laboratory. But nobody is doing that. Nobody is coming up with a group that both sides of the aisle and the American families can feel comfortable with. And so we are going to have to take action, and it is probably going to be this year.

I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Ms. Schrier for 5 minutes.

Ms. SCHRIER. Thank you, Mr. Chair.

I am a pediatrician, and I have spent my life calming patients who are nervous about vaccines because of online misinformation. In fact, that is why I introduced a Vaccines Act when I was a new Member of Congress. Did you know that there are doctors who, after spending their entire day on the front line fighting this virus, come home at night and spend their scarce free time and family time fighting misinformation about vaccines online? And this misinformation, of course, comes primarily from Facebook and Twitter.

So the question is: Why do they do that? Well, they do it because of things like this that happened after I introduced the Vaccines Act. Here are some overt threats:

"Keep shoving this vaccine monitor down people's throats and expect riots."

"Be careful. You will answer for this tyranny one day."

"She needs to just disappear. Can we vote her out of office? I am enraged over these poison pushers."

"We have weapons and are trained to fight off possible forced vaccinations. I will die protecting my family."

And then there is just the misinformation.

"It says 'safe and effective' many times, yet no vaccine has been studied in a double-blind study." False.

"Who is going to take this vaccine? I heard rumors that it changes a person's DNA." False.

"You do not give"—excuse my language—"You do not give a shit about the health and welfare of our children. This horrid vaccine has already killed 600 people. You are deplorable." And of course that again is false.

So while the overt threats are unsettling, particularly after January 6, I think about this whole ecosystem, your ecosystem, that directs a hostile sliver of society, en masse, to my official Facebook page. And these are not my constituents. In fact, most came from two specific groups that directed their members to my page.

Mr. ZUCKERBERG, I have some questions for you. I know you understand these issues are important, and sometimes misinformation can be very hard to spot. Would you agree?

Mr. ZUCKERBERG. Congresswoman, I agree with both of those. This is important, and the enforcement processes can be difficult.

Ms. SCHRIER. Thank you. And I heard your answer earlier to Representative Upton's question, that there are 35,000 people doing content review of posts that have been flagged by users and AI. Can you tell me what "content review" means and how many of those 35,000 are dedicated to topics regarding health?

Mr. ZUCKERBERG. Congresswoman, yes. What the people are doing overall is, you know, content gets flagged, either by the AI systems or by another person in the community. And if the AI can't by itself determine that something either violates or doesn't, then it gets flagged for human review and human judgment. And the 35,000 people go through all those different queues, focused on all the different types of harms that we have discussed today.

I don't have the number off the top of my head about how many of them are focused on vaccine misinformation. But, as you know, we have a policy that doesn't allow vaccine misinformation, and we work with the WHO and CDC to take down false claims around COVID, and the vaccines around that, that could cause harm.

Ms. SCHRIER. That is where it really gets tricky, because you have to have experts and healthcare professionals who really understand. Are your people trained in healthcare to really even be able to discern what is real, what is fake, and what to take down?

Mr. ZUCKERBERG. Congresswoman, the people who set the policies either are experts in these areas or engage in a consultative process where they talk to a lot of these different folks. In this case, we largely defer to the CDC and WHO on which claims they think are going to be harmful. And then we try to break that down into kind of very simple protocols that the 35,000 people can follow and that we can build into AI systems to go find as much of that content proactively as possible without requiring all those people to be medical experts.

Ms. SCHRIER. So with my short time remaining I would love to jump to that part about the CDC because I want to turn my attention to the COVID resource center that you describe as a central part of your efforts to fight misinformation directed over 2 billion people to the COVID-19 Information Center.

But on the information page, almost all of the content links to additional Facebook pages. It looks to me like an extension of Facebook's walled garden that just keeps users on the site instead of leading directly to authoritative, trusted sources like the CDC.

So knowing that your platform is a large source of misinformation, did you consider just referring people directly to sites like the CDC rather than keeping them within your platform?

Mr. ZUCKERBERG. Congresswoman, I think we have considered both, and I think we have done both in different cases. The team

is very focused on building this in the way that is going to be most effective at getting people to actually see the content, and I believe that they have concluded that showing content from people within a person's community that they are going to trust on the service is one of the most effective things that we can do.

Mr. DOYLE. The gentlelady's time is expired.

Ms. SCHRIER. Thank you. I yield back.

Mr. DOYLE. The Chair now recognizes Mr. Crenshaw for 5 minutes.

Mr. CRENSHAW. Thank you, Mr. Chairman. Thank you all for being here. It has been a long one.

I have been on some social media longer than anyone in Congress, I think. I was one of the first schools to have Facebook back in 2004. And it seemed to me that the goal of social media was simply to connect people.

Now, the reason we are here today is because, over time, the role of social media has expanded in an extraordinary way. Your power to sway opinions and control narratives is far greater than the U.S. Government's power ever has been.

So I noticed a trend today. There is a growing desire from many of my colleagues to make you the arbiters of truth. See, they know you have this power and they want to direct that power for their own political gain. Mr. Zuckerberg, since Facebook was my first love, I am going to direct questions at you. And this isn't a trick question, I promise.

Do you believe in the spirit of the First Amendment—free speech, robust debate, basically liberal values?

Mr. ZUCKERBERG. Yes, absolutely.

Mr. CRENSHAW. See, my colleagues can't infringe on the First Amendment. The American people in their speech are protected from government, as they should be. My colleagues, this administration, they can't silence people they disagree with no matter how much they want to.

But I do think they want to. Just in this hearing, I have heard Democrats complain about misinformation, by which they clearly mean political speech they disagree with. They have complained today that Prager University content is still up. I have heard them accuse conservative veterans of being tinfoil-hat-wearing extremists, and that opinions on climate change that they disagree with should be taken down.

This is quite different from the Republican complaint that illegal content needs to be addressed. There is a growing number of people in this country that don't believe in the liberal values of free speech and free debate. I promise you, the death of the First Amendment will come when the culture no longer believes in it. But that happens and it becomes OK to jail or investigate citizens for speech, like has happened in Canada and throughout Europe. Their culture turned against free speech.

You all sitting here today as witnesses are part of the culture. You can stand up for the spirit of open debate and free speech, or you can be the enemy of it. Your stance is important because it is clear that many want to weaponize your platforms to get you to do their bidding for them.

Mr. Zuckerberg, do you think it is your place to be the judge of what is true when it comes to political opinions?

Mr. ZUCKERBERG. Congressman, no. I don't believe that we should be the arbiter of truth.

Mr. CRENSHAW. Thank you. And look. I promise you this: As long as you resist these increasing calls from politicians to do their political bidding for them, I will have your back. When you don't, you become an enemy of liberty and longstanding American tradition.

You might all agree in principle with what I just said. Mr. Zuckerberg, you clearly do, and I appreciate it. I have a feeling the others would answer it as well, I just don't have time to ask everybody. But the fact remains that community standards on social media platforms are perceived to be applied unequally and with blatant bias.

Mr. Dorsey, in just one example, I saw a video from Project Veritas that was taken down because they confronted a Facebook executive on his front lawn. But here is the thing: I can show you a video of CNN doing the exact same thing to an old woman who was a Trump supporter in her front yard. I have looked at both videos. It is an apples to apples comparison. CNN remains up, Project Veritas was taken down.

I will give you a chance to respond to that. I have a feeling you are going to tell me you have to look into it.

Mr. DORSEY. I don't have an understanding of the case, but I would imagine, if we were to take a video like that down, it would be due to a doxxing concern, private address.

Mr. CRENSHAW. The address was blurred out. Look, you don't have it and you don't have the case in front of you. I get that. The point is that there are countless examples like this. I just found that one today. But there are countless examples like this.

So even if we agree in principle on everything I just went over, you guys have lost trust. And you have lost trust because this bias is seeping through. And we need more transparency. We need a better appeals process, more equitable application of your community guidelines, because we have to root out political bias in these platforms.

I think—and I have talked with a lot of you offline or at least your staff, and I think there is some agreement there. And I haven't heard, in this hearing, anybody ask you what you're doing to achieve these goals. So I will allow you to do that now. Maybe, Mr. Zuckerberg, we will start with you.

Mr. ZUCKERBERG. Sorry. To achieve which goals?

Mr. DORSEY. More transparency, more feeling that—better appeals process for content taken down, more equitable application of community guidelines.

Mr. ZUCKERBERG. So for transparency, we issue quarterly community standards enforcement reports on what prevalence of harmful content of each category—from terrorism to incitement of violence to child exploitation, all the things that we have talked about—how much of it there is and how effective we are at finding that, and states around that.

For appeals, the biggest thing that we have done is set up this independent oversight board, which is staffed with people who all have a strong commitment to free expression, for whom people in

our community can ultimately appeal to them and that group will make a binding decision, including overturning several of the things that we have taken down and telling us that we have to put them back up, and then we respect that.

Mr. DOYLE. The gentleman's time is expired.

The Chair now recognizes—

Mr. CRENSHAW. I yield back seconds.

Mr. DOYLE [continuing]. Last but not least, my fellow Pennsylvanian, Mr. Joyce. You are recognized for 5 minutes.

Mr. JOYCE. Thank you for yielding. And thank you, Mr. Chairman and the ranking members, for convening this hearing. I thank you all. It has been a long day.

But this is an incredibly important day. We have heard consistently during this hearing about alarming accounts of content policing, censorship, and even permanent deplatforming of individuals. I have also been concerned about the lack of transparency and consistency in Facebook's application, of Facebook's own standards.

As you mentioned, I am a representative from Pennsylvania, and in my district Facebook shut down the personal pages of Walt Tuchalski and Charlotte Shaffer as well as the Adams County Republican Committee Facebook page that they administered in historic Gettysburg, Pennsylvania. And this all occurred without warning.

Since the pages were taken down in December, these Pennsylvanians haven't received an acceptable answer from Facebook about why they were banned, nor have they been given the opportunity to appeal this decision.

Mr. Zuckerberg, could you please explain how something like this could happen?

Mr. ZUCKERBERG. Congressman, I am not familiar with those specific details. But in general, I agree that building out a better appeals process and better and more transparent communication to people about why specific decisions were made is one of the most important things that we need to do next. And that is one of the big things on our roadmap for this year and next year, and I hope we can dramatically improve those experiences.

Mr. JOYCE. Mr. Zuckerberg, may I get from you a commitment that a more concise and transparent appeals process will be developed?

Mr. ZUCKERBERG. Congressman, yes. We are working on more transparent communication to people and more of an appeals process as part of our product now, like I just said.

Mr. JOYCE. And will you commit to getting my constituents answers as to why they were banned?

Mr. ZUCKERBERG. Congressman, I can certainly have my team follow up with them and make sure that we can do that.

Mr. JOYCE. Thank you for that.

I am also concerned by potential partisan bias in Facebook's enforcement of its content policies. Shutting down the Adams County Republican Committee Facebook page strikes me as an infringement on speech, and that is normally protected in the public domain.

Mr. Zuckerberg, does Facebook maintain data on how many Democrat and Republican county committee pages that you have banned from your platform?

Mr. ZUCKERBERG. No, Congressman, we don't. We don't generally keep any data on whether the people who use our platform are Democrats or Republicans. So it is hard for us—

Mr. JOYCE. Then let me—time is running short here, and it is a long day. But Mr. Zuckerberg, you say you have not maintained that data. Would you consider gathering such data to verify that there is no political bias in your enforcement algorithms?

Mr. ZUCKERBERG. Congressman, I am not sure that that is a great idea. I don't know that most people would want us to collect data on whether they are a Democrat or a Republican and have that be a part of our overall system.

Mr. JOYCE. I think there is a huge disparity, as I represent Pennsylvania. And I think that that data would be appreciated if shared with us in a fair manner.

My next question is to Mr. Dorsey. Does Twitter maintain data on the political affiliations of accounts that you block?

Mr. DORSEY. No.

Mr. JOYCE. Have you determined that any political bias is necessary for your enforcement?

Mr. DORSEY. I'm not sure what you mean, but no.

Mr. JOYCE. I think that these discussions today are so important. I think that you all recognize that the platforms that you represent have developed an incredible ability for Americans to connect and contact. But this free speech that we hold so dear to us must be maintained.

Again, I thank the chairman, I thank the ranking member for bringing us together and allowing us to present what I feel are sincere concerns to you. Thank you, Mr. Chairman, and I yield.

Mr. DOYLE. I thank the gentleman. The gentleman yields back.

Everyone who wanted to ask a question has asked one. And I want to thank all of you for your patience today. I request unanimous consent to enter the following records, testimony, and other information into the record:

A letter from Asian Americans Advancing Justice.

A letter from the Leadership Conference on Civil and Human Rights.

A letter from New America's Open Technology Institute.

A letter from New York Small Farma, Limited.

A statement from the Alphabet Workers Union.

Letters from National Black Justice Coalition.

A letter from Sikhs for Justice.

A letter from State AGs.

A letter from the Computer and Communications Industry Association.

A letter from AVAAZ.

Opening statement from Anna Eshoo.

A blog from Neil Fried of DigitalFrontiers Advocacy.

A letter from the music community.

A letter from the Disinfo Defense League.

A letter from Consumer Reports.

A report from the Center for Countering Digital Hate called “The Disinformation Dozen.”

A letter from the Coalition for a Secure and Transparent Internet.

A letter from the Sikh American Legal Defense and Education Fund.

A letter from gun violence survivors, Faces of Tech Harm Congress.

Letter to YouTube from Rep. Eshoo.

Letter to Facebook from Rep. Eshoo.

Letter to Twitter from Rep. Eshoo.

A longitudinal analysis of YouTube’s promotion of conspiracy videos.

A letter from the Alliance for Safe Online Pharmacies.

A CCIA statement.

A comment by Donovan, et al., from the Technology and Social Change team.

A Wall Street Journal article titled “Facebook Executives Shut Down Efforts to Make Site Less Divisive.”

A Voice of America article titled “FBI: Surge in Internet Crime Cost Americans \$4.2 Billion.”

A Global Research Project report.

An opinion article titled “Google Is Not Cracking down on the Most Dangerous Drug in America.”

An MIT Technology Review article titled “How Facebook Got Addicted to Spreading Misinformation.”

An article from the Independent.

An article from the New Yorker.

A letter from the Coalition for a Safer Web.

A New York Times article titled “Tech Companies Detect a Surge in Online Videos of Child Sex Abuse.”

An MIT Review article titled “Thank You for Posting: Smokers Lessons for Regulating Smug Social Media.”

An article from Imprimis.

An article from The Atlantic.

A New York Times article titled “Square, Jack Dorsey’s Pay Service, Is Withholding Money Merchants Say They Need.”

A response letter from Twitter to Rep. Rodgers.

A response letter from Google to Rep. Rodgers.

A response letter from Facebook to Rep. Rodgers.

An article from Engadget.

A letter regarding Spanish language misinformation.

Data from the Centers for Disease Control: “The National Survey on Drug Use and Health.”

And Mercado, Holland, Leemis, Stone, and Wang regarding teen mental health.

A report from the House Committee on Veterans’ Affairs.

Without objection, so ordered.

[The information appears at the conclusion of the hearing.^{1]}

¹ The Open Technology Institute, New York Small Farma, and AVAAZ letters with accompanying reports, the MIT Technology Review article, and the Center for Countering Digital Hate, Global Research Project, and House Committee on Veterans’ Affairs reports are saved in committee files and are available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=111407>.

Mr. DOYLE. I want to thank our witnesses today for appearing. We appreciate it. We appreciate your patience while you answered these questions from all Members. I hope you can take away from this hearing how serious we are on both side of the aisle to see many of these issues that trouble Americans addressed. But thank you for being here today.

I want to remind all Members that, pursuant to Committee Rules, they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared. And I would ask each witness to respond promptly to any questions that you may receive.

At this time, this hearing is adjourned.

Ms. SCHAKOWSKY. Mr. Chairman?

Mr. DOYLE. Yes?

Ms. SCHAKOWSKY. Jan Schakowsky here.

Mr. DOYLE. Yes. You are recognized.

Ms. SCHAKOWSKY. Thank you. As chair of the Consumer Protection and Commerce Subcommittee, I just want to say that I was glad to be really a cochair of this. I think you did a great job, Mike, in making this happen. It is 5 and a half hours. I want to thank the witnesses for doing your best to answer the questions, or at least being willing to be here to hear all the questions. You can see there is a lot of concern.

We want to work with you and we want to work with each other in order to move ahead. As I said at the very beginning, if you take one thing away from this hearing today, is that these democratically elected Members are ready to act, are ready to legislate, are ready to regulate in your arena. And we are hoping that we can work with you as well.

So thank you, Mike, and I yield back.

Mr. DOYLE. Thank you, Jan. This hearing is adjourned.

[Whereupon, at 5:33 p.m., the subcommittees were adjourned.]

PREPARED STATEMENT OF HON. ANNA G. ESHOO

Chairs Doyle and Schakowsky, thank you for holding this critically important hearing.

As I've said before, misinformation is killing Americans and damaging our democracy. Social media companies—Facebook, YouTube, and Twitter—are a major cause of misinformation proliferating across society.

We'll hear a lot today about content moderation issues. I have no knowledge of what my colleagues will ask today, but we've all seen this movie before. I've asked, as have my Democratic colleagues, why companies won't remove posts and accounts that spread misinformation. My colleagues on the other side of the aisle have asked the opposite question about why certain posts and accounts are being taken down. Though I haven't found evidence for any alleged anticonservative bias, I hear their point and doubt I or this hearing will change minds on this issue. These are indeed important questions and issues, but these issues are the symptoms. It's time we start addressing the disease.

To truly address misinformation, we have to address root problems.

First, we must use Section 230 strategically. I was a conferee for the Telecommunications Act of 1996 which included the now famous Section 230. I have a reverence for the core idea of the statute—online user speech must be protected. However, we could not have conceived of the role internet platforms would play in amplifying, recommending, and sorting content using complex and opaque, AI-driven algorithms. Too often, platforms are the ones amplifying illegal or harmful speech, including speech that leads to offline violence.

This is why Rep. Malinowski and I reintroduced our legislation, the Protecting Americans from Dangerous Algorithms Act, which narrowly amends Section 230 to

remove liability immunity for a platform if its algorithm is used to amplify or recommend content directly relevant to a case involving interference with civil rights (42 U.S.C. 1985); neglect to prevent interference with civil rights (42 U.S.C. 1986); and in cases involving acts of international terrorism (18 U.S.C. 2333). 42 U.S.C. 1985 and 1986 are Reconstruction-era statutes originally designed to reach Ku Klux Klan conspirators. Sadly, they are being invoked in lawsuits against insurrectionists and perpetrators of the January 6th attacks.

This bill is not a panacea for all online harms—no bill is—and I believe it can pair well with some other narrow Section 230 reforms that are being suggested. We should use a scalpel, not a sledgehammer, in reforming this critically important law.

Second, we must ban surveillance advertising. We've begun to work in silos where privacy is one problem, advertising is another, and misinformation is a third. I think this is the wrong way to see things. All of these problems, and others, are interconnected. We have to work on all of them and more.

Surveillance advertising is the root of the tree where the poisonous fruit of misinformation thrives. It incents platforms to maximize engagement by collecting unseemly amounts of data to target ads and amplify content that induces anger, anxiety, and fear. It's why algorithmic amplification thrives unchecked.

That's why, Rep. Schakowsky and I will introduce a bill in the coming weeks to ban surveillance advertising altogether. Misinformation is a deadly problem, and we must address it at its roots. When a business model is fundamentally harmful, it shouldn't continue.

Finally, traditional content moderation must be improved. Platform companies have made important efforts to combat COVID-19 misinformation but the outcomes show that more must be done. According to a Walgreens executive, about 60% of employees and 20% of residents at long-term care facilities declined vaccines. National polls similarly show high levels of hesitancy, and social media is often cited as the cause of vaccine hesitancy.

Some platforms have turned to removing COVID misinformation that can cause “imminent harm” and labeling the rest. Research shows that introducing additional information to someone that believes medical or science-related misinformation can backfire and cause them to further entrench in their preexisting views. The implication is clear: Labels just don't cut it. When it comes to COVID-19 misinformation, companies must rely on removals.



March 25, 2021

The Honorable Frank Pallone, Jr., Chairman
 The Honorable Cathy McMorris Rodgers, Ranking Member
 U.S House Energy and Commerce Committee

The Honorable Michael F. Doyle, Chairman
 The Honorable Robert E. Latta, Ranking Member
 U.S. House Communications and Technology Subcommittee

The Honorable Janice D. Schakowsky, Chairwoman
 The Honorable Gus M. Bilirakis
 U.S. House Consumer Protection and Commerce Subcommittee

RE: Energy and Commerce Committee Hearing with Facebook CEO Mark Zuckerberg, Alphabet CEO Sundar Pichai, and Twitter CEO Jack Dorsey

Dear Chairman Pallone, Ranking Member McMorris Rodgers, Chairman Doyle, Ranking Member Latta, Chairwoman Shakowsky, Ranking Member Bilirakis, and Members of the Subcommittees:

On behalf of Asian Americans Advancing Justice | AAJC (Advancing Justice | AAJC), we submit this comment in advance of your March 25th, 2021 hearing with the CEOs of Alphabet, Facebook, and Twitter to examine the proliferation and management of misinformation and disinformation content on their platforms.

Advancing Justice | AAJC is a national non-profit, non-partisan organization that works through policy, advocacy, education, and litigation to advance the civil and human rights of Asian Americans and to build and promote a fair and equitable society for all. Founded in 1991, Advancing Justice | AAJC is one of the nation's leading experts on civil rights issues of importance to the Asian American and Pacific Islander (AAPI) community including hate incidents, immigrant rights, and racial profiling.

The insurrection at the Capitol on Jan. 6 is only one instance of how mis- and disinformation, conspiracy theories, and racially-charged rhetoric have led to increases in violence. Disinformation and its negative offline effects profoundly impact minority and Black, Indigenous and people of color communities. Mis- and disinformation seeks to manipulate and indoctrinate Asian American communities with false information, while other campaigns scapegoat Asians and Asian Americans with baseless theories that ultimately stoke hate and violence against AAPIs.

As demonstrated by the recent surge in anti-Asian hate, Asian Americans are suffering from race-related discrimination, harassment, and violence. Platforms have failed to enforce their own internal guidelines and policies prohibiting hate speech and the incitement of violence, allowing racist and xenophobia to proliferate online. Derogatory online content has fueled, justified, and inspired acts of violence targeting AAPI individuals and perpetuated fear in AAPI communities across the country. While expressing legitimate criticism of or disagreement with the Chinese government for the handling of COVID-19 based on verified facts is certainly permissible and important, what cannot be tolerated is the use of “dog whistles” to spread verifiably false information or to falsely equate the actions and responsibilities of a government entity to an entire community of people based on race. Language that conflates Asians and Asian Americans with the Chinese government is weaponized to mischaracterize and harm an entire race. Failure to recognize and remove such “dog whistles” perpetuates and escalates harm to AAPI communities. In a 2017 report, Advancing Justice | AAJC noted an increase in hate crimes, harassment, and violence against Asian Americans within the first year of the Trump presidency when such conflation and disinformation started to become more normalized.¹ The number of anti-Asian incidents dramatically increased in 2020² – an outcome of continued anti-Asian rhetoric amplified and normalized by Trump and others on social media platforms.

Hate crimes against Muslims in the United States have also increased by 15% in recent years. According to the Council on American-Islamic Relations (CAIR), this rise can be attributed to xenophobic rhetoric used by Trump, including his statements on social media platforms.³ Under the Trump administration, a greater percentage of hate incidents against Muslims became physically violent against victims. Facebook, Twitter, YouTube, and other platforms have been consistently used as an organizing tool by white nationalists and militias to advance violent, anti-Muslim agendas; but Trump’s own anti-Muslim rhetoric gave such views legitimacy and authority. Allowing such content to persist on platforms without oversight or contest proliferated and uplifted the rhetoric of far-right extremist groups and encouraged violence and harassment against members of the Muslim community.

While some platforms have taken some steps to flag and/or label potential disinformation⁴, they continue to host, monetize, and enable the sharing of such content. Community organizers and advocates do not believe that labeling does enough to stop the harmful effects of such content. Platforms must do more to prevent the active spread of harmful content, including enforcing their own terms and conditions by banning and taking down flagged disinformation. Even though some entities like Facebook publicly committed to bolstering security and content moderation efforts during the election cycle,⁵ some researchers believe that enforcement was not as effective or vigilant on non-English content such as Asian language videos (even after they had been flagged by users as featuring problematic content).⁶ As some of the largest and most influential digital platforms, Alphabet, Twitter, and Facebook must go beyond monitoring only explicit calls

¹<https://www.advancingjustice-ajjc.org/news/advocates-see-disturbing-rise-hate-crimes-targeting-asian-americans>

²http://www.asianpacifcouncil.org/wp-content/uploads/A3PCON_Public_Weekly_Report_3.pdf

³<https://www.dw.com/en/anti-muslim-hate-crime-on-the-rise-in-donald-trumps-us-report/a-43500942>

⁴<https://www.vox.com/identities/21579752/asian-american-misinformation-after-2020>

⁵<https://www.nytimes.com/2020/11/05/technology/facebook-election-misinformation.html>

⁶<https://www.vox.com/recode/21551696/stolen-election-misinformation-youtube-trump-voter-fraud>

to violence in response to user flags, to actively identifying and removing “dog whistles,” discriminatory language, and other more implicit but equally threatening and dangerous content.

Examples of hate speech and violence inciting language on digital platforms

Google:

Content perpetuating the myth that COVID-19 is the result of a lab or other conspiracy theories surrounding China’s responsibility for the spread of the virus continues to proliferate on platforms like YouTube.⁷ Other content repeatedly insists that “China must pay” for “victimizing the world,”⁸ blaming China for the “wuhan flu’s” “devastation” on America.⁹ In some videos, Trump supporters also blamed his 2020 presidential election loss on the “kung flu.”¹⁰ Another video goes as far as to claim that the Chinese government intentionally deployed Chinese tourists with the virus to deliberately spread it.¹¹ This type of YouTube content scapegoats China and Chinese people, while normalizing and legitimizing hateful and dehumanizing speech. Google does label COVID-19 related content with a link to the CDC website, but many of these videos remain unflagged and unmarked with any warning about their false claims. Moreover, some content creators deny the prevalence of anti-Asian hate stemming from disinformation they spread about the pandemic, dismissing victims’ reports and undermining statements of law enforcement.¹² This rhetoric continues to be readily accessible on YouTube and shared through networks, accumulating views and receiving supportive comments from viewers.

While Google has removed some YouTube content in reaction to content-enforcement flags, its reasons for removing videos is not always consistent with addressing racism or hateful content. For example, one video that suggested Chinese restaurants were responsible for the spread of COVID-19 was not removed for its jarring racist images, but because Google found the video to be in violation of COVID misinformation policies that prohibit content that underplays the severity of the illness.¹³ Alphabet must set clear guidelines on racist and xenophobic content and strictly adhere to enforcement of such guidelines.

Facebook:

During the COVID-19 pandemic, thousands of Facebook posts baselessly accused Chinese individuals and Chinese Americans for the spread of COVID-19 in the United States. Trump and other prominent figures repeatedly posted content on Facebook that scapegoated China and Chinese individuals for the outbreak of the virus, using phrases like “China ban,”¹⁴ “China virus,”¹⁵ and other racialized rhetoric like “Remember, it was China’s fault!”¹⁶ Posts also encouraged xenophobia against Asians and Asian Americans, suggesting only U.S. citizens were

⁷ One example with 146 views: https://www.youtube.com/watch?v=rR2C7gkd_4E; another with 185k views: <https://www.youtube.com/watch?v=U023FSiOdf0>

⁸ <https://youtu.be/em77L2CsqYg>

⁹ <https://www.youtube.com/watch?v=JY1RhCSj0v0&t=478s>

¹⁰ <https://www.youtube.com/watch?v=LiUN6e7iXVc&t=2225s>

¹¹ <https://www.youtube.com/watch?v=QX97s5RNuY8&t=438s>

¹² <https://www.youtube.com/watch?v=oziCnBBDAw>

¹³ <https://www.mercurynews.com/2021/03/17/youtube-takes-down-racist-video-but-not-because-of-the-racism/>

¹⁴ Over 12 instances of “China ban,” “China travel ban,” or other language on Trump’s account alone, suggesting individuals of Chinese descent should not be allowed to enter the United States.

¹⁵ Over 40 instances of “China virus” or “ChinaVirus” appear in Donald Trump’s Facebook posts alone

¹⁶ <https://www.facebook.com/153080620724/posts/10166036380945725>

welcome into the country¹⁷ and even conflating U.S. Chinatowns with the virus.¹⁸ The scapegoating of Chinese people is a continuation of anti-Asian rhetoric Trump and other right-wing personalities have amplified on Facebook's platforms throughout recent years, including content that repeatedly singles out Chinese and North Koreans as threats.

Prominent Facebook accounts and groups have also frequently shared negatively charged language like “terrorist” and “jihadist” and attached negative connotations to the word “Muslim.” In one Facebook post, Trump characterized Middle Eastern immigrants as “terrorists, jihadists, and violent extremists.” The post garnered over 273,000 reactions, 45,000 comments, and 58,000 shares with a sizable number of reactions and comments in support of this hateful rhetoric.¹⁹ Groups such as Muslim Advocates have repeatedly called for Facebook to take anti-Muslim rhetoric on the platform seriously. They cite that White nationalists and militias have used Facebook to organize protests at mosques.²⁰ They also emphasize that the platform has been used internationally to incite violence and even genocide against Muslims.

Twitter:

Anti-Asian hate and scapegoating intensified on Twitter as prominent accounts with high numbers of followers like those of Trump, Senator Cruz, and others amplified hateful rhetoric, hashtags, and disinformation on the platform. The former President's tweets referring to COVID-19 as the “#chinesevirus” was associated with a rise in anti-Asian content on the platform. Posts that contained “#chinesevirus” had higher associations with anti-Asian language and the use of other hateful hashtags such as “#batmaneatingflu” and “#yellowmanflu,”²¹ shifting blame to Asians and Asian Americans. One popular hashtag that proliferated anti-Asian sentiment was “#ChinaLiedPeopleDied,” which more explicitly blamed China for the virus, baselessly accused Chinese people of intentionally spreading the virus, and even called for revenge. Another trending topic was “#MakeChinaPay,” which echoed the Trump administration’s desire to punish China for the pandemic.²²

Studies indicate that increases in hateful social media activity and content consumption is associated with increases in anti-minority sentiment and even hate crimes. For example, Trump’s tweets “about Islam-related topics are highly correlated with anti-Muslim hate crimes... [and] Trump’s tweets [even] predict[ed] more anti-Muslim Twitter activity of his followers.”²³ Social media platforms like Twitter normalize anti-minority sentiments, which can make such bigotry seem more socially acceptable, potentially leading to an increase in violence.

Conclusion

¹⁷ <https://www.facebook.com/153080620724/posts/10164590148900725>

¹⁸ <https://www.facebook.com/153080620724/posts/10165154893590725>

¹⁹ <https://www.facebook.com/153080620724/posts/10165726004780725>

²⁰ <https://www.commondreams.org/newswire/2021/01/11/muslim-advocates-calls-facebooks-new-civil-rights-vp-ban-trump-prioritize-anti>

²¹ Hsuen, Yulin, et al. “Association of ‘#covid19’ Versus ‘#chinesevirus’ With Anti-Asian Sentiments on Twitter: March 9–23, 2020.” American Journal of Public Health, Mar. 2021, pp. e1–9. DOI.org (Crossref), doi:10.2105/AJPH.2021.306154.

²² <https://www.cnbc.com/2020/07/15/the-world-will-make-china-pay-a-price-over-coronavirus-outbreak-mike-pompeo-says.html>

²³ Muller, Karsten, and Carlo Schwarz. From Hashtag to Hate Crime: Twitter and Anti-Minority Sentiment. p. 110.

When tech platforms like Alphabet, Facebook, and Twitter fail to adequately respond to the rise of hate speech, xenophobic content, and fabricated claims, they amplify and enable racist, white-supremacist, violent agendas that lead to the dehumanization of and attacks against Asian American communities. Continuing to give hateful rhetoric a platform without proper oversight and consequences will continue to encourage and normalize the scapegoating and otherization of Asian Americans. The recent surge in anti-Asian hate demonstrates how critical it is to address the sources of mis- and disinformation, xenophobia, and scapegoating of the Asian American community. Dismantling the spread of hateful rhetoric must be a priority to protect minority and BIPOC communities from harm, and Alphabet, Facebook, and Twitter have a crucial role to play here. They must do more, and they must be held accountable.

Asian Americans Advancing Justice | AAJC thanks you for your attention to and examination of this critical issue, and urges you to consider the effects of mis- and dis-information on minority and BIPOC communities.

Please contact Emily Chi, Assistant Director for Telecommunications, Technology and Media at Asian Americans Advancing Justice | AAJC at echi@advancingjustice-aajc.org for any inquiries.

Sincerely,
Asian Americans Advancing Justice | AAJC

**The Leadership Conference
on Civil and Human Rights**

1620 L Street, NW
Suite 1100
Washington, DC
20036

202.466.3311 voice
202.466.3435 fax
www.civilrights.org



March 25, 2021

The Honorable Michael F. Doyle
Chair
Subcommittee on Communications and Technology
Committee on Energy and Commerce
U. S. House of Representatives
Washington, DC 20515

The Honorable Janice D. Schakowsky
Chair
Subcommittee on Consumer Protection and Commerce
Committee on Energy and Commerce
U.S House of Representatives
Washington, DC 20515

The Honorable Robert E. Latta
Ranking Member
Subcommittee on Communications and Technology
Committee on Energy and Commerce
U. S. House of Representatives
Washington, DC 20515

The Honorable Gus M. Bilirakis
Ranking Member
Subcommittee on Consumer Protection and Commerce
Committee on Energy and Commerce
U.S House of Representatives
Washington, DC 20515

Dear Chair Doyle, Chair Schakowsky, Ranking Member Latta, and Ranking Member Bilirakis,

On behalf of The Leadership Conference on Civil and Human Rights, a coalition charged by its diverse membership of more than 220 national organizations to promote and protect the rights of all persons in the United States, we thank you for the opportunity to submit our views regarding the misinformation and disinformation plaguing online platforms. We ask that this letter be entered into the record of the hearing entitled “Disinformation Nation: Social Media’s Role in Promoting Extremism and Misinformation” on March 25, 2021.

The January 6, 2021 deadly attack on the U.S. Capitol by far-right extremists attempting to overturn the free, fair, and secure 2020 presidential election was a catastrophic reminder of the fragility of our democracy. This violent insurrection did not happen in a vacuum. It was

Officers
Chair
 Judith L. Lichtenman
 National Partnership for
 Women & Families
Vice Chairs
 Derrick Johnson
 NAACP
 Farhana Khera
 Muslim Advocates
 Thelma A. Saenz
 Mexican American Legal
 Defense and Educational Fund
Secretary
 Fatima Goss Graves
 National Women’s Law Center
Treasurer
 Lee A. Saunders
 American Federation of State,
 County & Municipal Employees

Board of Directors
 Kimberly Churches
 AAUW
 Alphonso David
 Human Rights Campaign
 Rory Gamble
 International Union, UAW
 Jonathan Greenblatt
 Anti-Defamation League
 Rep. Kyrsten Sinema
 Service Employees International Union
 Damon Hewitt
 Lawyers’ Committee for
 Civil Rights Under Law
 Sheryll Cashin
 NAACP Legal Defense and
 Educational Fund, Inc.
 David H. Istrate
 Japanese American Citizens League
 Rep. Frederica J. Johnson
 People’s Way to the American Way
 Derrick Johnson
 NAACP
 Virginia Kase
 League of Women Voters of the
 United States
 Samer E. Khader
 American-Arab
 Anti-Discrimination Committee
 Marc Morano
 National Urban League
 Jonel Murray
 UnidosUS
 Debra L. Ness
 National Partnership for
 Women & Families
 Christian F. Raible
 National Organization for Women
 Rabbi Jonah Pesner
 Religious Action Center
 Of Reform Judaism
 Roberta Pernell
 National Education Association
 Lisa Rice
 National Fair Housing Alliance
 Anthony Romero
 American Civil Liberties Union
 Fawn Sharp
 National Congress of American Indians
 Maria Town
 American Association of
 People with Disabilities
 Richard L. Trumka
 AFL-CIO
 Randi Weingarten
 American Federation of Teachers
 John C. Yang
 Asian Americans Advancing Justice |
 AAJC

Interim President & CEO
 Wade Henderson

paired with numerous hurdles that voters faced during the election cycle, including a pandemic and relentless efforts by former President Trump and his allies to threaten civil rights, spread hate speech, undermine election integrity, impose barriers to the ballot box, and discount the votes of communities of color.

As stated in the final report of the July 8, 2020 Facebook civil rights audit, when Facebook and the other companies that dominate and control social media do not address content that leads to voter suppression and threatens civil rights, the result is a corrosive effect on our democracy that can lead directly to violence:

If politicians are free to mislead people about official voting methods (by labeling ballots illegal or making other misleading statements that go unchecked, for example) and are allowed to use not-so-subtle dog whistles with impunity to incite violence against groups advocating for racial justice, this does not bode well for the hostile voting environment that can be facilitated by Facebook in the United States.¹

The internet has created immense positive value by connecting people, facilitating civil rights advocacy, and adding new voices to our culture and public debate. However, it can also enable discriminatory conduct, exacerbate existing disparities, and give new tools to those who want to threaten, harass, intimidate, defame, or violently attack people different from themselves. Social media platforms have continually allowed discriminatory conduct and false information to spread wildly even though the content violates their own civic integrity policies and community standards. Voter Fraud 2020, a project from the Jacobs Technion-Cornell Institute at Cornell Tech, found “7.6M tweets and 25.6M retweets from 2.6M users that includes key phrases and hashtags related to voter fraud claims between October 23rd and December 16th.”² The lack of enforcement by the platforms of their own policies resulted in the spread of false information before and after the 2020 election and fueled the flames for the insurrection at the U.S. Capitol on January 6. Congress now needs to fully use its oversight and legislative powers to address disinformation and protect our democracy going forward.

Technological progress should promote equity and justice as it enhances safety, economic opportunity, and convenience for everyone. On October 21, 2020, The Leadership Conference joined dozens of leading civil rights and technology advocacy organizations in releasing updated Civil Rights Principles for the Era of Big Data,³ in response to the current risks to civil rights — including COVID-19, a surge in hate-based violence, private sector and government surveillance, and disinformation on social media platforms designed to manipulate or suppress voter participation — and with an eye toward how technology can meet its promise and affirmatively promote justice and equity. These principles provide important guidelines to aid this committee in ensuring that new technologies — including algorithmic

¹ <https://about.fb.com/wp-content/uploads/2020/07/Civil-Rights-Audit-Final-Report.pdf>

² <https://voterfraud2020.io/>

³ <https://www.civilrightstable.org/principles/>

decision making, artificial intelligence, and machine learning — protect civil rights, prevent unlawful discrimination, and advance equal opportunity.

Congress must press platforms to reduce online activities and disinformation that harm communities of color, religious minorities, and other marginalized communities. For years, we have urged major tech platforms to take responsibility for ensuring that their products and business processes protect civil and human rights and do not result in harm or bias against historically marginalized groups, but they have failed to take sufficient action. And despite years of advocacy urging the companies to rectify the problems, misinformation and content intended to suppress or deter people from voting and spread hate speech continue to proliferate. The failure of tech platforms to address these activities harms people of color and members of other marginalized communities.

The violent insurrection at the Capitol, fueled by white supremacy and anti-Semitism, horrified us all. Sadly, for the members of our coalition and the people we represent, this violence is not new. Nor is the disinformation propagated across multiple social media platforms that inspired the insurrectionists to take action to advance their racist agenda.

Just as they have been doing throughout the pandemic, white supremacists online are continuing to weaponize the collective pain and fear of this pandemic by encouraging violence against the AAPI community. Moreover, despite new policies that ostensibly forbid white supremacy, white supremacists continue to use multiple platforms to incite racist violence against Asian Americans, African Americans, Jews, Muslims, people with disabilities, and members of the LGBTQ community.

Platforms have the tools and the ability to respond effectively to these concerns if they only had the will. Congress should press tech companies on the actions they are taking to improve and enforce their own policies and stop the weaponization of their platforms to spread hate and undermine our democracy.

Congress should not be distracted by baseless claims of “anti-conservative” bias and should instead focus on platforms’ efforts to respond to online voter suppression and other threats to our democracy. A commitment to civil and human rights is not a ‘right’ or ‘left’ issue — it is about right versus wrong. Baseless allegations of so-called anti-conservative bias should not distract tech companies. Research shows that anti-conservative bias is a phantom problem; a number of studies, articles, and reports show that the voices of marginalized communities are more likely to be regarded as “toxic” by content moderators and content moderation artificial intelligence. In addition, misinformation about voting and elections is more pervasive from far right-wing voices. The Election Integrity Partnership’s report on misinformation in the 2020 election found that there are far more influential Twitter accounts aligned with the right wing. The report stated that these accounts, led by repeat spreaders such as Trump and his allies, were responsible for the most widely spread incidents of false and misleading information about the election.⁴ A recent report from New York University found that misinformation sources significantly outperform non-misinformation sources on the far-right.⁵

⁴ <https://stacks.stanford.edu/file/druid:tr171zs0069/EIP-Final-Report-v2.pdf>, p. 180-201.

⁵ <https://medium.com/cybersecurity-for-democracy/far-right-news-sources-on-facebook-more-engaging-e04a01efae90>

Trump and his allies repeatedly posted false information about voting by mail and the voting process before the election, and continually posted false information about the counting of ballots and lies about “fraud” that took place after the election, clearly violating the platforms’ voter interference and civil integrity policies. This disinformation laid the groundwork for the statements and videos that Trump and his allies posted on the day of the insurrection that led to the violence and loss of life that was predicted in the civil rights audit. Had the platforms enforced their own policies consistently before and after the election, the disinformation could have been curbed and addressed in a proper manner before it escalated. We are pleased that the platforms permanently or temporarily suspended Trump’s account and made some policy changes before and after the election. In a recent study, Zignal Labs found after Trump’s suspension from Twitter and other platforms the week of January 6, misinformation and disinformation on multiple platforms about the election dropped 73 percent, from “from 2.5 million mentions to 688,000 mentions across several social media sites in the week after Trump was suspended.”⁶ But most of the changes were reactive after the damage had already occurred.

Congress should focus on some of the more significant challenges facing social media platforms, such as safeguarding our election from manipulation and disinformation, as well as fighting hate and harassment online. Going forward, Congress must press platforms to take stronger steps to stem the tide on false, misleading, and harmful content on the companies’ platforms that could lead to voter suppression and the spread of hate speech.

Specifically, Congress should push platforms to set clear, unambiguous, and consistently enforceable voter inference and civic integrity policies. Platforms should combine all their policies and interpretations in one place and consistently enforce those policies to remove or limit the ability to share disinformation and voter suppression content. Congress should also press platforms to preserve and provide transparency data on content moderation, voter suppression content, and advertising targeting. Vetted users and researchers should have access to this data so they can understand forces that enable misinformation and disinformation on voting and civil rights to proliferate, identify where these content and advertising moderation policies and practices fell short, and make recommendations on how they can be improved.

Congress must push platforms to stop the spread of disinformation on COVID-19 targeted at communities of color, particularly from the same actors responsible for the spread of other false information. The Leadership Conference is pleased to see leading social media entities implement policies and take new steps aimed at reducing the spread of misinformation about the COVID-19 pandemic on their channels.⁷ However, despite these efforts, we continue to be concerned about the spread of false claims and inaccurate information concerning the COVID-19 vaccines on social media platforms and the potential impact of this misinformation, especially on communities of color that have been hit hardest by the pandemic.⁸

⁶ <https://www.washingtonpost.com/technology/2021/01/16/misinformation-trump-twitter/>

⁷ <https://www.forbes.com/sites/siladityaray/2021/03/15/facebook-will-add-labels-to-all-posts-about-covid-19-vaccines-that-will-promote-authoritative-information/?sh=562a57f27cb8>

⁸ <https://www.usatoday.com/story/tech/2021/03/10/covid-vaccine-facebook-youtube-instagram-black-misinformation-fight/6943180002/>

Most troubling from the perspective of the civil rights community is that many of the same actors who spread white supremacist, anti-Semitic, and anti-immigrant disinformation are spreading COVID-19 disinformation and misinformation. For example, roughly a quarter of former President Trump's posts from 2020 were connected to COVID-19 misinformation, election lies, or what could be considered extremist rhetoric.⁹ Facebook's own research shows that there is overlap between vaccine skeptics and groups associated with QAnon and that just 111 people are behind the worst comments.¹⁰ Recent reports of a foreign-backed online disinformation campaign conducted through social media platforms in the United States to erode confidence in certain COVID-19 vaccines is also deeply troubling, especially at this critical time when our nation is continuing to battle the COVID-19 pandemic while simultaneously embarking on a widespread vaccine distribution effort.¹¹

Congress must press the platforms to address these issues immediately and provide additional data on the content and the actors behind COVID-19 disinformation. These false claims take advantage of and play upon distrust that certain communities may have in the health care system, given a history of medical racism and exploitation to create fear and steer people away from scientifically informed recommendations, especially as vaccine distribution is ramping up. Moreover, as platforms continue to work toward addressing COVID-19 disinformation, Congress must urge them to share lessons learned from addressing false information on COVID-19 and apply similar solutions to reduce the spread of online mis- and disinformation on voting, hate speech, and other issues that are directed at targeted communities.

Congress should press tech companies to conduct independent civil rights audits as well as improve their civil rights infrastructure. Structural changes within the platforms will also help better protect civil rights by ensuring platforms can hold themselves accountable to their commitment to civil rights, diversity, and inclusion. Among the companies appearing at the committee hearing, only Facebook has undertaken a civil rights audit with outside auditors, though civil rights groups have urged all the major platforms to do so. But Facebook's example demonstrates that without institutional commitment and outside pressure, the impact of an audit will be limited and short-lived.

That is why, in addition to pushing for civil rights audits, Congress must also urge tech companies to adopt structural reforms that comply with federal civil rights law and demonstrate that the companies understand that civil rights are not a partisan issue, but instead are fundamental to protecting the constitutional rights of all people and thus should be part of the organic structure and operations of these companies. This means that tech companies must hire staff with civil rights expertise in senior leadership. The civil rights infrastructure within the companies must be well-resourced, empowered, and consulted on the companies' major decisions. New and clarified policies should be subject to vetting and review by

⁹ <https://www.mediamatters.org/facebook/roughly-quarter-trumps-posts-facebook-2020-contained-covid-19-misinformation-election-lies>

¹⁰ <https://www.washingtonpost.com/technology/2021/03/14/facebook-vaccine-hesitancy-qanon/>

¹¹ https://www.wsj.com/articles/russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200?reflink=desktopwebshare_twitter

internal teams with real civil rights expertise and experience, prior to their implementation. Finally, tech companies should provide a process and format through which civil rights advocates and the public can engage with the companies and monitor their progress.

Congress must also press tech companies to do more to address meaningful diversity and inclusion at their workplaces and the lack of people of color in senior executive, engineering, and technical positions. People of color who are working at the companies often face discrimination and unequal pay, as well as a culture where they are devalued. Tech companies must ensure that this does not happen in their workplaces and must address the inequities that may have already occurred. They also must build on strategies to attract and retain talent in diverse communities to expand access to jobs and opportunities.

Prevention of harm, not damage and after-the-fact repair, must be the goal. This goal cannot be fully accomplished if those with civil rights expertise are not part of decision-making processes. Congress must continue to review and scrutinize tech companies to make sure that they are taking the necessary steps to accomplish this goal.

Congress should consider other meaningful ways to protect civil and human rights. Congress should also focus on other means to protect civil and human rights. For example, invasive data collection and use practices can lead to civil rights violations. Congress should pass comprehensive federal consumer privacy legislation that protects consumers by requiring companies to minimize the data they collect; define permissible and impermissible purposes for collecting, sharing, and using personal data; prohibit discriminatory uses of personal data; and provide for algorithmic transparency and fairness in automated decisions. In addition, Congress should ensure federal agencies are focusing on identifying and ending data processing and algorithmic practices that discriminate on the basis of protected characteristics with respect to access to credit, housing, education, public accommodations, and elsewhere.

Conclusion

The spread of discriminatory conduct and false information, especially when content is concentrated in a limited number of platforms, is a threat to civil rights and the integrity of our democracy. The threat to safe and fair elections, civil rights, and health care can have a corrosive effect on the fabric of our country and the safety and voting rights of people of color and other targeted communities. After largely ignoring these issues, social media platforms and tech companies have taken steps in recent months to address the problems. But far more needs to be done and the companies need to be more engaged on solutions to address the proliferation of false, misleading, and harmful content.

The Leadership Conference urges Congress to press the companies to institute the reforms outlined in this letter. We also stand ready to work with Congress and elected officials to find solutions that will keep our democracy safe, limit the concentration of content, and stop the suppressive effect that disinformation is having on civil rights and racial justice. Should you require further information or have any questions regarding this issue, please contact David Toomey, Voting Rights and Technology Fellow, at toomey@civilrights.org.

March 25, 2021
Page 7 of 7



Sincerely,



Wade Henderson
Interim President and CEO



LaShawn Warren
Executive Vice President for Government Affairs

Statement of the Alphabet Workers Union On “the Misinformation and Disinformation Plaguing Online Platforms” Before the House Energy and Commerce Committee March 25, 2021



March 25, 2021

Workers across Alphabet have previously organized against the company's continued refusal to take meaningful action to stop the proliferation of hate, harassment, incitement of violence, or harmful misinformation from YouTube and other Alphabet-operated platforms, without good faith engagement from leadership.

Alphabet is responsible for directly contributing to harmful misinformation campaigns that fuel fascist, white nationalist and hateful movements that perpetrate violence in the United States and around the world. While much attention has been paid to YouTube and other online platforms' role in radicalizing white supremacists, this hearing is also an opportunity to illuminate how these technologies contribute to dangerous disinformation movements including QAnon, "Patriot" militias, and anti-vaccine advocacy. [\(1\)](#), [\(2\)](#).

Alphabet has demonstrated a continued policy of reactive, selective and insufficient enforcement of its guidelines against disinformation and hate. As a union that fights for, and welcomes the contributions of, every worker in Alphabet, we find it abhorrent that systems to which we have dedicated our work continue to profit from the hate and disinformation that harms so many of these same workers. [\(3\)](#), [\(4\)](#), [\(5\)](#), [\(6\)](#), [\(7\)](#), [\(8\)](#).

Online misinformation can have real and dire consequences offline, ranging from targeted violence to vaccine hesitancy. Misinformation on Alphabet products facilitates the

proliferation of hate-filled conspiracy theories, like QAnon, which has repeatedly lead to incidents of targeted violence and been deemed a domestic terror threat by the FBI. Beyond physical violence, the spread of conspiracy theories and misinformation online contributes to diffuse harms that affect those across the US and abroad, such as public health violations, lower vaccination rates, and decreased democratic participation. (11), (12), (13).

Misinformation on Alphabet products can also facilitate the undermining of democracy, as was the case with virulent election-related misinformation in the United States and elsewhere in 2020. While some key disinformation peddlers were retroactively deplatformed—after other companies decided to act first—there remains an entire ecosystem of disinformation influencers and publishers who have profited from attacking the foundations of democracy on YouTube and Google Ads infrastructure. The processes behind these decisions and those processes' influence on community guidelines and authoritative source lists is not transparent which makes it more difficult for researchers at Alphabet and elsewhere to solve these problems. (10).

From election misinformation to anti-Semitic conspiracies, Alphabet's incremental and reactive policies have proven to be a lose-lose approach, angering free speech advocates and allowing harmful movements to fuel atrocities and insurrections before they are penalized. Failing to crack down on misinformation and disinformation proactively has led to harassment, threats, injuries, and death—real trauma and real pain for so many people (9).

YouTube has said it welcomes peer-reviewed research on disinformation, but it needs to engage directly with academics and outside experts, including sharing data on removed videos, in order to credibly foster more understanding of the problem (14).

Alphabet workers built these systems and we know how to make them better—the company has a variety of tools to mitigate misinformation at its disposal that we believe ought to be deployed beyond retroactive removals and ranking. We invite Alphabet's leadership to tackle these issues and others collaboratively with our union. We are ready and eager to share our perspectives and proposals constructively with Alphabet leadership, on this and other issues of the public good.

One thing we will not be, however, is silent.

Contextual Sources

1. [YouTube, the Great Radicalizer](#) from Zeynep Tufekci in the New York Times
2. [Alternative Influence](#) from Rebecca Lewis in Data & Society
3. [Black creators sue YouTube, alleging racial discrimination](#) from The Washington Post
4. [LGBTQ Creators Are Suing YouTube For Discrimination](#) from Buzzfeed News
5. [A group of YouTubers is trying to prove the site systematically demonetizes queer content](#) from Vox
6. [YouTube will let Steven Crowder run ads after year-long suspension for harassment](#) from The Verge
7. [YouTube's arbitrary standards: Stars keep making money even after breaking the rules](#) from The Washington Post
8. [YouTube's purge of white supremacist videos also hits anti-racism channels](#) from the LA Times
9. [The Christchurch Shooter and YouTube's Radicalization Trap](#) from WIRED
10. [YouTube faces complaints of lax approach on overseas election misinformation](#) from Reuters
11. [Auditing radicalization pathways on YouTube](#)
12. [How QAnon and other dark forces are radicalizing Americans as the COVID-19 pandemic rages and election looms](#) From USA Today
13. [FBI memo warns QAnon poses potential terror threat: report](#) from The Hill
14. [Tracking Viral Misinformation](#) from The New York Times



National Black Justice Coalition
 Post Office Box 71395
 Washington, DC 20024
 Office: 202.319.1552
www.NBJC.org

Honourable Michael F. Doyle
 Chairman
 House Committee on Energy and Commerce
 Subcommittee on Communications and Technology
 United States House of Representatives
 2125 Rayburn House Office Building
 Washington, DC 20515

Honourable Robert E. Latta
 Ranking Member
 House Committee on Energy and Commerce
 House Subcommittee on Communications and Technology
 United States House of Representatives
 2125 Rayburn House Office Building
 Washington, DC 20515

Re: Congressional Hearing on Mitigating the Spread of Disinformation and Misinformation Across Digital Platforms

Dear Chairman Doyle, Ranking Member Latta, and Members,

On behalf of the National Black Justice Coalition (NBJC), the nation's premier civil rights organization dedicated to the empowerment of Black lesbian, Gay, Bisexual, Transgender, Queer+ and Same Gender Loving (LGBTQ+/ SGL) people, including those living with HIV and AIDS, we write to contribute to the record on important conversations about the spread of misinformation and disinformation across digital platforms.

Codified in 1996, Section 230 of the Communications Decency Act was designed to protect "internet speech". Technology innovation and the power of social media has grown tremendously since 1996. Leading up to the 2020 election, we have witnessed technology giants, like those invited to testify before congress, leverage Section 230's protections to respond to false information and disinformation--including efforts designed to prevent poor, stigmatized and minoritized individuals and communities from voting; suppress the efforts of civil rights and social justice organizers; and affirm anti-democratic and white supremacist propaganda.

Conversations about and efforts to ensure that the internet is both accessible and safe for everyone to use remain incredibly important; however, we remain concerned that current debates around misinformation and content moderation are focused on bad actors with large followers and multiple platforms from which to disseminate (mis/dis) information publicly. The current conversation, for example, focuses overwhelmingly on Trump and Parler. What is being missed, as a result, is how even conversations about potential changes to Section 230 are negatively impacting social justice organizations like NBJC, non-profit organizations that engage in life affirming and life-saving advocacy and direct-action

work—organizations that would be crippled if stripped of the ability to share messages and to engage in actions across digital platforms--actions that have been threatened by conversations about content moderation generally, and Section 230 specifically.

NBJC's HIV/AIDS advocacy efforts, for example, have been impacted, in recent months, by conversations about potential changes to Section 230. Many of our ads for awareness days like National Black HIV/AIDS Awareness day and more recently National Women and Girls HIV/AIDS Awareness day were flagged for review by at least two of the platforms testifying before congress. Beyond that review timelines caused significant delays to our work and at times prevented us from engaging in our work altogether.

Here are but a few of the questions we hope will be considered in conversations about content moderation as a result of the important efforts to stop the spread of misinformation and disinformation:

- Under the last presidential administration, we saw evidence of civil rights and social justice activists become targets of federal and local law enforcement agencies. We also saw that when elected “leaders” sent dog whistles to white supremacist groups the personal and physical safety of civil rights and social justice activists were threatened, sometimes by groups that organized online. What is being done, at present, to ensure the safety of civil rights and social justice activists?
- How are you currently protecting against bias that results from the existence of and collusion of anti-Blackness, white supremacy, and homophobia across the digital platforms that you provide?
- Tell us more about what recent and current action is being taken to ensure that social justice, civil rights, and non-profit organizations are not being negatively impacted by efforts to moderate content in ways that ensure everyone has safe access to the digital platforms you provide?
- What steps have been taken to ensure that there is diversity among the teams responsible for developing and operating systems that develop content moderation algorithms and systems as well as to ensure ethical development and use of technology more generally?
- What steps are the platforms taking to proactively promote and support content developed by and for stigmatized minoritized communities generally and BIPOC LGBTQ+ communities specifically?

Thank you for your consideration and taking the time to read our letter. We thank you in advance for considering the inclusion of the overlooked implications of this conversation as well as the questions we've submitted. Should you have any additional questions or need additional information please do not hesitate to contact Victoria Kirby York, Deputy Executive Director, at (202) 460-4420 or vkirbywork@nbcj.org.

Yours in the work,



David J. Johns
Executive Director
National Black Justice Coalition



National Black Justice Coalition
 Post Office Box 71395
 Washington, DC 20024
 Office: 202.319.1552
www.NBJC.org

Honourable Janice D. Schakowsky
 Chairwoman
 House Committee on Energy and Commerce
 Subcommittee on Consumer Protection and Commerce
 United States House of Representatives
 2125 Rayburn House Office Building
 Washington, DC 20515

Honourable Gus M. Bilirakis
 Ranking Member
 House Committee on Energy and Commerce
 House Subcommittee on Consumer Protection and Commerce
 United States House of Representatives
 2125 Rayburn House Office Building
 Washington, DC 20515

Re: Congressional Hearing on Mitigating the Spread of Disinformation and Misinformation Across Digital Platforms

Dear Chairwoman Schakowsky, Ranking Member Bilirakis, and Members,

On behalf of the National Black Justice Coalition (NBJC), the nation's premier civil rights organization dedicated to the empowerment of Black lesbian, Gay, Bisexual, Transgender, Queer+ and Same Gender Loving (LGBTQ+/ SGL) people, including those living with HIV and AIDS, we write to contribute to the record on important conversations about the spread of misinformation and disinformation across digital platforms.

Codified in 1996, Section 230 of the Communications Decency Act was designed to protect "internet speech". Technology innovation and the power of social media has grown tremendously since 1996. Leading up to the 2020 election, we have witnessed technology giants, like those invited to testify before congress, leverage Section 230's protections to respond to false information and disinformation--including efforts designed to prevent poor, stigmatized and minoritized individuals and communities from voting; suppress the efforts of civil rights and social justice organizers; and affirm anti-democratic and white supremacist propaganda.

Conversations about and efforts to ensure that the internet is both accessible and safe for everyone to use remain incredibly important; however, we remain concerned that current debates around misinformation and content moderation are focused on bad actors with large followers and multiple platforms from which to disseminate (mis/dis) information publicly. The current conversation, for example, focuses overwhelmingly on Trump and Parler. What is being missed, as a result, is how even conversations about potential changes to Section 230 are negatively impacting social justice organizations like NBJC, non-profit organizations that engage in life affirming and life-saving advocacy and direct-action

work—organizations that would be crippled if stripped of the ability to share messages and to engage in actions across digital platforms--actions that have been threatened by conversations about content moderation generally, and Section 230 specifically.

NBJC's HIV/AIDS advocacy efforts, for example, have been impacted, in recent months, by conversations about potential changes to Section 230. Many of our ads for awareness days like National Black HIV/AIDS Awareness day and more recently National Women and Girls HIV/AIDS Awareness day were flagged for review by at least two of the platforms testifying before congress. Beyond that review timelines caused significant delays to our work and at times prevented us from engaging in our work altogether.

Here are but a few of the questions we hope will be considered in conversations about content moderation as a result of the important efforts to stop the spread of misinformation and disinformation:

- Under the last presidential administration, we saw evidence of civil rights and social justice activists become targets of federal and local law enforcement agencies. We also saw that when elected “leaders” sent dog whistles to white supremacist groups the personal and physical safety of civil rights and social justice activists were threatened, sometimes by groups that organized online. What is being done, at present, to ensure the safety of civil rights and social justice activists?
- How are you currently protecting against bias that results from the existence of and collusion of anti-Blackness, white supremacy, and homophobia across the digital platforms that you provide?
- Tell us more about what recent and current action is being taken to ensure that social justice, civil rights, and non-profit organizations are not being negatively impacted by efforts to moderate content in ways that ensure everyone has safe access to the digital platforms you provide?
- What steps have been taken to ensure that there is diversity among the teams responsible for developing and operating systems that develop content moderation algorithms and systems as well as to ensure ethical development and use of technology more generally?
- What steps are the platforms taking to proactively promote and support content developed by and for stigmatized minoritized communities generally and BIPOC LGBTQ+ communities specifically?

Thank you for your consideration and taking the time to read our letter. We thank you in advance for considering the inclusion of the overlooked implications of this conversation as well as the questions we've submitted. Should you have any additional questions or need additional information please do not hesitate to contact Victoria Kirby York, Deputy Executive Director, at (202) 460-4420 or vkirbywork@nbcj.org.

Yours in the work,



David J. Johns
Executive Director
National Black Justice Coalition



NEW YORK
 Bulova Corporate Center
 75-20 Astoria Blvd. Suite 170
 East Elmhurst, New York 11370
 T: +1 (833) 735 - 2020 | F: +1 (718) 672 - 4728
 E: support@sikhsforjustice.org

WASHINGTON D.C.
 National Press Building
 529 14th St NW, Suite 1111
 Washington, DC 20045
 T: +1 (202) 662 - 8820 | F: +1 (202) 662 - 8817
 E: support@sikhsforjustice.org

www.sikhsforjustice.org www.referendum2020.org www.facebook.com/sikhsforjusticepage

VIA E-MAIL

March 22, 2021

House Committee On Energy and Commerce
 United States Congress, Washington, DC 20515
Joe.orlando@mail.house.gov; Ed.kaczmarski@mail.house.gov;

Re: March 25th Hearing On "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation".

Sub: Twitter, Google and Facebook Are Collaborating With The Indian Government In Suppressing The First Amendment Rights of The Americans.

Honorable Chairman Frank Pallone, Jr.
 Ranking Member Cathy McMorris Rodgers
 And Members of the Committee

My name is Gurpatwant Singh Pannun. I am an attorney admitted to practice by the State of New York. My main area of practice is human rights and civil rights. I am also General Counsel to US based international advocacy group "Sikhs For Justice" (SFJ). SFJ's aim and objective is to raise awareness about the human rights issues being faced by the Sikh people in India, including seeking right to self-determination through the democratic means of Referendum.

On behalf of the Sikh Americans who follow and support SFJ, I am writing to convey to the Committee, the pressing concerns and related questions which we urge to be raised during the March 25th Sub-Committee Hearing titled "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation."

It is indeed reassuring that this Committee is taking up the issue which impacts the lives of billions of people across the globe and role of social media giants, Google, Facebook and Twitter, which has been of indifference towards the problem, giving free pass to the violent narratives at home and abroad while at the same time willingly collaborating with fascist regimes like Modi Government of India in suppressing the freedom of expression of Americans.

The most recent and pressing issue is that in the wake of ongoing farmers protest in India, Twitter, Facebook and Google have been collaborating with the Indian authorities in suppressing the freedom of speech of not only of farmers in India but also of fellow Americans. We, therefore, urge that during March 25th hearing, Zuckerberg, Pichai and Dorsey be asked:

Q.1: Why Facebook, Google and Twitter are actively suppressing the First Amendment Rights of American Citizens by blocking their content and removing their accounts at the request of the Modi Govt. in the wake of ongoing farmers protest?

Q.2: As CEO of American Corporations, how do you justify the blocking/deleting within America the First Amendment protected content and accounts on the request of the Indian Government?

Q.3: Why Google, Twitter and Facebook are actively complying with Indian laws in American territory regarding blocking and deleting First Amendment protected accounts and content of fellow Americans?

Q.4: Is it true that Twitter, Google and Facebook, unbeknownst to the American users, has shared their personal information with Indian authorities, as reported by New York Times on February 10, 2021?

Note: We are not questioning the blocking of access in India to the content posted by Americans. Our Question is only about blocking within America of the US Citizen's first amendment protected content.



NEW YORK	WASHINGTON D.C.
Bulova Corporate Center 75-20 Astoria Blvd. Suite 170 East Elmhurst, New York 11370 T: +1 (833) 735 - 2020 F: +1 (718) 672 - 4728 E: support@sikhsforjustice.org	National Press Building 529 14th St NW, Suite 1111 Washington, DC 20045 T: +1 (202) 662 - 8820 F: +1 (202) 662 - 8817 E: support@sikhsforjustice.org

www.sikhsforjustice.org
 www.referendum2020.org
 www.facebook.com/sikhsforjusticepage

Honorable Chairman and Members, besides myself, whose several First Amendment protected content – advocacy for Sikhs Right to Self Determination through Khalistan Referendum - and associated accounts have been deleted by Twitter, Google and Facebook. I present to this esteemed Committee, the following specific, recent and egregious examples of these America corporations' collaboration with India in suppressing the freedom of speech of the Sikhs and other fellow Americans.

TWITTER:

On February 10, 2021, New York Times reported that Twitter received about 5,500 demands from Indian government to block content or remove the accounts altogether and around 5,900 requests for access to the personal information of users. See "Twitter Blocks Accounts in India as Modi Pressures Social Media". <https://www.nytimes.com/2021/02/10/technology/india-twitter.html>

Google:

On the request of the Indian Government, Google removed the app "2020 Sikh Referendum" from its Play-Store. The app was prepared and launched by American NGO "Sikhs For Justice" (SFJ) and was facilitating Sikh people in USA, India and everywhere to register in NGO's proposed non-governmental referendum. The app was not violating any US Law and thus removing this at the behest of Indian Government clearly violated First Amendment rights of the US Citizens. <https://www.thestatesman.com/technology/google-takes-pro-khalistan-2020-sikh-referendum-app-play-store-1502824147.html>

Google owned platform Youtube removed channels run by American Sikhs solely on the request of Indian government. India sought removal of the channels for relaying the content critical of Modi Government's policies. In one of the many such cases, Youtube blocked and removed the channel "Khabardar Punjab" which was being run and operated by the American Citizens sitting in the United States, solely on the request of Government of India. https://theprint.in/india/governance/these-are-the-apps-and-websites-modi-govt-blocked-in-2020/623337/?utm_source=izoot&utm_medium=push_notification&utm_campaign=ThePrint&

Facebook:

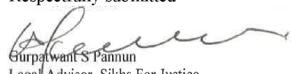
On the behest of Indian Government, Facebook has blocked and removed several Accounts and Pages of American citizens supporting ongoing farmers' protest and non-governmental referendum for Khalistan. In one of the many such cases, Facebook has blocked access to the page of American NGO Sikhs For Justice (SFJ) www.facebook.com/sikhsforjusticepage in India on the request of the Indian Government. *Sikhs for Justice "SFJ", Inc. v. Facebook, Inc.*, 697 F. App'x 526 (9th Cir. 2017)

In addition to the above, recently, Twitter removed American lawyer-cum activist Meena Harris' tweet supporting farmers' right to protest while allowed the brazen calls for violence against Ms. Harris by the supporters of PM Modi. American singer Rihanna was threatened with violence on twitter by the people of Indian descent in response to her tweet supporting farmers' right to protest. While Twitter did remove the violent Tweets against Rihanna, it also complied with Indian government's request to block the content critical of Modi Government.

The above cited cases show that how Facebook, Google and Twitter, on one hand are colluding and collaborating with Indian Government in suppressing the freedom of expression of Americans and on the other hand are freely allowing violence instigating content against critics of Modi Government to be posted and spread through their platforms.

Honorable Congress Members, we are certain that significance of "freedom of speech" and First Amendment being the bedrock of American democracy and in fact of any true democracy, is of prime importance for you and hence our request for probe into the role of Google, Twitter and Facebook in the ongoing violations of First Amendment rights of Americans at the behest of Indian Government.

Respectfully submitted


 Gurpatwant S Pannun
 Legal Advisor, Sikhs For Justice
 E: gurpatwant.pannun@gmail.com; gurpatwant.pannun@sikhsforjustice.org
 Mobile: +1-917-789-2914



OFFICE OF THE ATTORNEY GENERAL
CONNECTICUT

WILLIAM TONG
ATTORNEY GENERAL

March 24, 2021

Via First Email

Honorable Frank Pallone, Chair
Honorable Cathy McMorris Rodgers, Ranking Member
House Energy and Commerce Committee

Honorable Michael F. Doyle, Chair
Honorable Robert E. Latta, Ranking Member
Communications and Technology Subcommittee

Honorable Janice Schakowsky, Chair
Honorable Gus Bilirakis, Ranking Member
Consumer Protection and Commerce Subcommittee

Re: *Vaccine Disinformation*

Dear Representatives Pallone, McMorris Rodgers, Doyle, Latta, Schakowsky and Bilirakis,

As attorneys general responsible for safeguarding the well-being of residents and consumers in our states, we are concerned about the role of social media platforms in enabling the spread of vaccine misinformation that threatens the health and safety of our communities. In advance of your March 25 hearing on online mis- and disinformation, we are sharing a letter that we have sent to Twitter CEO Jack Dorsey and Facebook CEO Mark Zuckerberg, calling on them to remove coronavirus vaccine misinformation from their platforms.

During the hearing, we encourage you to hold Mr. Dorsey and Mr. Zuckerberg accountable for enforcing the policies against coronavirus vaccine misinformation that each of their companies has established, by posing two simple questions: “Will you enforce your policies?” and, “Will you do so within 48 hours?” Currently, as our enclosed letter shows, they have done a poor job of implementing these policies and are allowing prominent purveyors of vaccine disinformation to continue to operate on their platforms. Mr. Dorsey’s and Mr. Zuckerberg’s cooperation in removing this content will protect vulnerable Americans and hasten our recovery from the pandemic.

We commend your oversight work on this important issue.

165 Capitol Avenue
Hartford, Connecticut 06106

An Affirmative Action/Equal Opportunity Employer

Representatives Pallone, McMorris Rodgers, Doyle, Latta, Schakowsky and Bilirakis
March 24, 2021
Page | 2

Sincerely,



WILLIAM TONG
Attorney General of Connecticut



KATHLEEN JENNINGS
Attorney General of Delaware



TOM MILLER
Attorney General of Iowa



MAURA HEALY
Attorney General of Massachusetts



DANA NESSEL
Attorney General of Michigan

Representatives Pallone, McMorris Rodgers, Doyle, Latta, Schakowsky and Bilirakis
March 24, 2021
Page | 3



KEITH ELLISON
Attorney General of Minnesota



LETITIA JAMES
Attorney General of New York



JOSHUA STEIN
Attorney General of North Carolina



ELLEN F. ROSENBLUM
Attorney General of Oregon



JOSH SHAPIRO
Attorney General of Pennsylvania



PETER NERONHA
Attorney General of Rhode Island

Representatives Pallone, McMorris Rodgers, Doyle, Latta, Schakowsky and Bilirakis
March 24, 2021
Page | 4

Mark R. Herring

MARK HERRING
Attorney General of Virginia



OFFICE OF THE ATTORNEY GENERAL
CONNECTICUT

WILLIAM TONG
ATTORNEY GENERAL

March 24, 2021

Via First Class and Electronic Mail

Jack Dorsey
Chief Executive Officer
Twitter, Inc.
1355 Market St.
San Francisco, CA 94103

Mark Zuckerberg
Chairman & Chief Executive Officer
Facebook, Inc.
1 Hacker Way
Menlo Park, CA 94025

Re: Vaccine Disinformation

Dear Messrs. Dorsey and Zuckerberg:

As Attorneys General committed to protecting the safety and well-being of the residents of our states, we write to express our concern about the use of your platforms to spread fraudulent information about coronavirus vaccines and to seek your cooperation in curtailing the dissemination of such information. The people and groups spreading falsehoods and misleading Americans about the safety of coronavirus vaccines are threatening the health of our communities, slowing progress in getting our residents protected from the virus, and undermining economic recovery in our states.

As safe and effective vaccines become available, the end of this pandemic is in sight. This end, however, depends on the widespread acceptance of these vaccines as safe and effective. Unfortunately, misinformation disseminated via your platforms has increased vaccine hesitancy, which will slow economic recovery and, more importantly, ultimately cause even more unnecessary deaths. A small group of individuals use your platforms to downplay the dangers of COVID-19 and spread misinformation about the safety of vaccines. These individuals lack medical expertise and are often motivated by financial interests. According to a recent report by the Center for Countering Digital Hate¹, so-called “anti-vaxxer” accounts on Facebook, YouTube, Instagram, and Twitter reach more than 59 million followers. “Anti-vaxxers” are using social media platforms to target people of color and Black Americans specifically, members of communities who have suffered the worst health impacts of the virus and whose vaccination rates are lagging.

¹ [Center for Countering Digital Hate \(counterhate.com\)](http://counterhate.com)

165 Capitol Avenue
Hartford, Connecticut 06106

An Affirmative Action/Equal Opportunity Employer

Jack Dorsey, CEO, Twitter
Mark Zuckerberg, Chairman & CEO, Facebook
March 24, 2021
Page | 2

Given “anti-vaxxers” reliance on your platforms, you are uniquely positioned to prevent the spread of misinformation about coronavirus vaccines that poses a direct threat to the health and safety of millions of Americans in our states and that will prolong our road to recovery.

The updated community guidelines you have established to prevent the spread of vaccine misinformation appear to be a step in the right direction. However, it is apparent that Facebook has not taken sufficient action to identify violations and enforce these guidelines by removing and labelling misinformation and banning repeat offenders. As a result, anti-vaccine misinformation continues to spread on your platforms, in violation of your community standards.

- Twitter and Facebook have yet to remove from all their platforms the accounts of prominent “anti-vaxxers” who have repeatedly violated the companies’ terms of service. Digital media research groups estimate that as of March 10, 12 “anti-vaxxers” personal accounts and their associated organizations, groups and websites are responsible for 65% of public anti-vaccine content on Facebook, Instagram, and Twitter.
- Facebook has failed to consistently apply misinformation labels and popups on Facebook pages and groups that discuss vaccines or COVID-19. For example, the company neglected to apply warning labels on dozens of Facebook groups that “anti-vaxxer” Larry Cook created for his followers. At the same time, the company has mistakenly flagged pro-vaccine pages and content in ways that have undermined pro-vaccine public education efforts.
- Facebook has allowed anti-vaxxers to skirt its policy of removing misinformation that health experts have debunked, by failing to prevent them from using video and streaming tools like Facebook Live and sites like Bitchute, Rumble, and Brighteon to evade detection.

We call on you to take immediate steps to fully enforce your companies’ guidelines against vaccine misinformation. By effectively rooting out fraudulent information about coronavirus vaccines, you can prevent needless illness and death and hasten our road to recovery.

Sincerely,



WILLIAM TONG
Attorney General of Connecticut

Jack Dorsey, CEO, Twitter
Mark Zuckerberg, Chairman & CEO, Facebook
March 24, 2021
Page | 3



KATHLEEN JENNINGS
Attorney General of Delaware



TOM MILLER
Attorney General of Iowa



MAURA HEALY
Attorney General of Massachusetts



DANA NESSEL
Attorney General of Michigan



KEITH ELLISON
Attorney General of Minnesota

Jack Dorsey, CEO, Twitter
Mark Zuckerberg, Chairman & CEO, Facebook
March 24, 2021
Page | 4



LETITIA JAMES
Attorney General of New York



JOSHUA STEIN
Attorney General of North Carolina



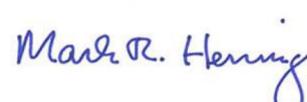
ELLEN F. ROSENBLUM
Attorney General of Oregon



JOSH SHAPIRO
Attorney General of Pennsylvania



PETER NERONHA
Attorney General of Rhode Island



MARK HERRING
Attorney General of Virginia



March 24, 2021

The Honorable Michael F. Doyle
 Chair
 House Committee on Energy & Commerce
 Subcommittee on Communications &
 Technology
 Washington, DC 20515

The Honorable Janice D. Schakowsky
 Chair
 House Committee on Energy & Commerce
 Subcommittee on Consumer Protection &
 Commerce
 Washington, DC 20515

The Honorable Robert E. Latta
 Ranking Member
 House Committee on Energy & Commerce
 Subcommittee on Communications &
 Technology
 Washington, DC 20515

The Honorable Gus M. Bilirakis
 Ranking Member
 House Committee on Energy & Commerce
 Subcommittee on Consumer Protection &
 Commerce
 Washington, DC 20515

Re: March 25 Subcommittee Hearing: Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation

Dear Chairs Doyle and Schakowsky and Ranking Members Latta and Bilirakis:

On behalf of the Computer & Communications Industry Association (CCIA),¹ I write to offer some information for consideration in advance of the March 25, 2021 hearing on "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation."

We understand that during the hearing, Section 230 of the Telecommunications Act may be discussed. This is a critical provision for any website that allows third-party user-generated content. Codified at 47 U.S.C. § 230, Section 230 facilitates legal certainty regarding online commerce and communication, making it possible for millions of entrepreneurs and businesses to flourish. Section 230 also enables the companies we represent to invest substantial time and resources in developing and maintaining content moderation policies that protect consumers and promote free expression.

Digital services are committed to ensuring consumer trust and safety online. As you may be aware, a number of companies recently announced that they have been voluntarily participating in the Digital Trust & Safety Partnership to develop best practices to ensure a safer and more trustworthy Internet.² Responsible services take aggressive steps to moderate harmful content, including extremism and misinformation, with content moderation requiring a mix of automated

¹ CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For nearly fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more, visit www.cianet.org.

² Digital Trust & Safety Partnership, <https://dtspartnership.org/>.

tools and human review. Nothing in the current law prohibits the application of state or federal civil rights law to content that is posted online. A reduction in moderation would lead to an increase in the spread of reprehensible content online, including racism and hate speech, religious and ethnic intolerance, public health-related misinformation, and election-related disinformation by foreign agents.

Services can respond aggressively to this material because they have the legal certainty to do so. What makes this moderation possible is Section 230, including the phrase "otherwise objectionable," which enables digital services to act regarding speech that is problematic, but still lawful. Congress's decision to use this term acknowledged that it could not anticipate and legislate every form of problematic online content or behavior. Under a narrower definition, digital services would be discouraged from acting against a considerable amount of potentially harmful but legal content online, lest moderating it lead to litigation.³

By protecting intermediary decisions whether content is removed or not, Section 230 encourages services to fight misconduct and protect users from online harms by removing disincentives to moderate. This helps combat online content and misbehavior that is abusive, inappropriate, or otherwise objectionable, though lawful. Narrowing this protection would have the perverse result of impeding online services' and websites' efforts to police bad actors and misconduct, including key consumer protections that users have come to expect, such as spam filtering.

Weakening Section 230 protections is likely to produce different responses from different online services. Smaller operators may avoid moderating content at all because online services have less legal liability if they engage in no monitoring. As demonstrated in the 1995 *Stratton Oakmont* decision that Section 230 overturned, removing 99% of inappropriate content could create the appearance of endorsing the 1% that an online service overlooked. Small firms may adopt even more aggressive editorial policies, or decide to exit the market – or never enter it – which would discourage innovation and free expression by all stakeholders. Cautious sites and services, wary of anything that could lead to risk, may only give a platform to establishment viewpoints. Marginalized communities would suffer the most, being subject to increased scrutiny by litigation-wary lawyers hoping to avoid controversy.⁴

The U.S. legal framework for online services is critical to American leadership in the digital economy, promoting growth and innovation across sectors. The certainty provided by this framework reduces the threat of costly, likely ruinous litigation, enabling small U.S. businesses and startups to scale up.⁵ Undermining foundational intermediary liability protections could cost an estimated 4.25 million American jobs and \$400 billion over the next decade, according to 2017 research.⁶ Intermediary liability protections also play a key role in enabling American small

³ See Matt Schruers, *What Is Section 230's "Otherwise Objectionable" Provision?*, Disruptive Competition Project (July 29, 2020), <https://www.project-disco.org/innovation/072920-what-is-section-230s-otherwise-objectionable-provision/> (explaining the contours of "otherwise objectionable").

⁴ Adi Robertson, *Social justice groups warn Biden against throwing out Section 230*, The Verge (Jan. 27, 2021), <https://theverge.com/2021/1/27/22251093/section-230-civil-rights-groups-letter-biden-harris-congress-defense>.

⁵ Engine, *Section 230: Cost Report* (2019), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5c8168cae5e5f04b9a30e84e/1551984843007/Engine_Primer_230cost2019.pdf.

⁶ Christian Dippon, *Economic Value of Internet Intermediaries and the Role of Liability Protections* (NERA 2017), <http://internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protectios.pdf>.

businesses to build trust and customer relationships in new markets. Today, millions of U.S. small businesses are taking advantage of online commerce to reach far beyond their localities, including through marketing tools and interactive customer services. However, for these tools to function, companies need legal certainty that they will not be held liable for all communications that arise between businesses and consumers using these tools, or sued for efforts to improve the consumer's experience.

Thank you very much for your thoughtful consideration of these important issues. We look forward to continuing to work with you as Congress considers Section 230.

Sincerely,

Arthur D. Sidney
Vice President of Public Policy
Computer & Communications Industry Association

Why Section 230 Isn't Really a Good Samaritan Provision



siam.pukkato/shutterstock.com

Neil Fried

As the House Commerce Committee revisits [internet platform responsibility](#) this week, it bears recognizing that [section 230](#) of the Communications Act[*] does not make platforms more likely to protect their users. In fact, despite its description as a “good samaritan” provision, it does the opposite.

The Good Samaritan Misnomer

Good samaritan statutes typically limit liability for individuals who have no relationship to the person in jeopardy, and thus who have no obligation to lend assistance. A stranger, for example, has no duty to help someone who is drowning. If the stranger tries anyway, however, he or she has a duty at common law not to do so

in a way that unreasonably causes harm.

That means that if the stranger injures the person, such as by administering CPR recklessly and breaking a rib, he or she could potentially face liability. This risk can discourage the stranger from providing assistance. A properly functioning good samaritan statute removes the liability risk for someone with no duty of care, thereby eliminating the disincentive to act and creating a net increase in the likelihood of aid.

In section 230 scenarios, by contrast, the platform is not a stranger. It has a business relationship with its users. Indeed, the platform created the environment in which its users are interacting.

Ordinarily, businesses have a duty of care at common law to avoid unreasonably causing harm to their customers, as well as to take reasonable steps to prevent harm to them from other customers. But as applied today, section 230 removes this duty of reasonable care for platforms. That makes it less likely platforms will protect their users, not more, contrary to the goals of a good samaritan statute.

How did we get here?

Stratton Oakmont v. Prodigy

In 1996, Congress wanted online platforms to grow as venues for commerce and communication while at the same time to proactively curb harmful behavior online. Congress saw the recent New York trial court ruling in *Stratton Oakmont v. Prodigy* as an obstacle to that objective, however.

The court had concluded that Prodigy's decision to moderate user content made it a "publisher" and therefore subject to potential liability for defamatory posts, even for user content it did not moderate. Congress worried that ruling would discourage platforms from moderating in the first place.

To overturn *Prodigy*, Congress passed section 230 of the Communications Act. In

particular, section 230(c)(2) states that “[n]o provider or user of an interactive computer service shall be held liable on account of … any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.”

Analogizing to protections for people who help others in jeopardy, Congress labelled section 230(c) the “good samaritan” provision. Congress’s theory was that limiting the liability of platforms when they seek to prevent harmful behavior on their services would encourage them to take such measures.

The Misapplication of Section 230

Unfortunately, courts have misapplied another part of section 230—subsection (c)(1)—to shield platforms not just when they do moderate content, but even when they don’t.

Section 230(c)(1) states that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” Courts have concluded this “creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.”

Consequently, judges have ruled that platforms cannot be held culpable for negligently, recklessly, or knowingly facilitating terrorism, harassment, sexual disparagement, non-consensual dissemination of intimate photos, housing discrimination, distribution of child sexual abuse materials, and other unlawful conduct. Absent that potential liability, platforms are less likely to moderate content, not more.

This creates a net decrease in the likelihood platforms will prevent harm and arguably even increases the likelihood they will put their users in peril, defeating

Congress's goal. For example, platform promotion of [divisive content](#) in the quest for engagement might be less likely, or at least more quickly addressed, if platforms could be held liable. Section 230 today is therefore acting as a bad samaritan provision—shielding platforms even when they negligently, recklessly, or even knowingly facilitate harm, and thus making such lack of responsibility more likely.

Restoring the Duty of Reasonable Care

The best way of addressing this problem is to amend section 230 so platforms must take reasonable steps to curb unlawful activity as a condition of receiving the liability limitations, as [I](#) and [others](#) have previously suggested.

That would restore the duty of care in a way that [avoids the criticisms](#) lodged by opponents of section 230 reform. Platforms would not need to stop every harm from the potentially large volume of content they carry so long as they take reasonable steps. The common law reasonableness standard would also take into account the resources of platforms, ensuring small services are not treated the same as large ones.

And it would do so [without inappropriately expanding litigation](#), while reducing the need for Congress to pass piecemeal, issue-specific legislation. The section 230(c)(2) liability limitation would remain, continuing to solve the *Prodigy* problem and ensuring platforms can still moderate content while serving as avenues for free expression.

Most importantly, this approach would increase the likelihood platforms will protect their users and the public from harmful behavior on their services, as Congress intended.

[*]Section 230 was added to the Communications Act by [section 509 of the 1996 Telecommunications Act](#). Section 509 and all the other provisions in 1996 Telecommunications Act title V—which sought to address indecent, obscene, and

violent transmissions by phone, on television, and over the internet—are collectively referred to as the Communications Decency Act.

DigitalFrontiersAdvocacy.com

© 2021 DigitalFrontiers Advocacy® PLLC



March 25, 2021

Hon. Frank Pallone, Chair

Hon. Cathy McMorris Rodgers, Ranking Member

Hon. Michael Doyle, Chair, Subcommittee on Communications & Technology

Hon. Robert Latta, Ranking Member, Subcommittee on Communications & Technology

Hon. Jan Schakowsky, Chair, Subcommittee on Consumer Protection & Commerce

Hon. Gus Bilirakis, Ranking Member, Subcommittee on Consumer Protection & Commerce

Committee on Energy and Commerce

U.S. House of Representatives

Dear Chairs Pallone, Doyle and Schakowsky and Ranking Members McMorris Rodgers, Latta, and Bilirakis:

We write as artist, songwriter, and creative community organizations committed to a healthy internet and a robust exchange of information, ideas, and digital creative works. Thank you for convening this important hearing on the responsibility of large technology platforms regarding misinformation and disinformation online.

Given the appearance of Twitter and Square CEO Jack Dorsey, we want to call your attention to Twitter's related failure to meet the most basic standards of responsible moderation with respect to other illegal activity – specifically, the rampant theft of creative works on its platform. We ask you to engage Twitter on this issue as part of this hearing and include it in the Committee's ongoing platform accountability oversight.

While Twitter publicly claims to support artists and creativity, in the real world, it erects almost insurmountable obstacles to artists and creators trying to protect their work online. As the Committee explores broader questions regarding the platforms' response to online mis- and dis-information, we believe there is much to be learned from the gaping disconnect between Twitter's lofty promises to artists and its heavy-handed and inadequate actions.

Twitter has become a major player in the distribution and consumption of commercial music, much of it without authorization or any kind of license. As a result, the music industry sent over 2 million infringement notices to Twitter last year. Critically, over 200,000 of those deal with pre-release leaks – an especially damaging form of online piracy that steals an artist or labels' irreplaceable first chance to tell their story and meet fans on their own terms.

This attack on the legitimate music marketplace hurts music creators and fans and undermines all legitimate licensed services – from full-service music platforms like Apple Music or Spotify to emerging services like TikTok. It also undermines music's powerful contribution to America's

economic strength and security – including \$170 billion in GDP, \$9 billion in export sales, and 2.47 million jobs each year in both core music businesses and supporting industries nationwide. Today, there are over 236,000 music-related businesses across the country – many of which operate exclusively online.¹

Yet even with this success, online piracy remains a major threat to artists, songwriters, and digital creators. Indeed, during the pandemic when working artists and musicians lost so many income streams, [music piracy exploded on the internet](#), and working to protect digital creative works online became all the more important.

Over the past few years, artists, songwriters, and their label and publishers partners have routinely sought Twitter's cooperation to address this hugely damaging activity, with only nominal success. While the company claims it "takes copyright issues seriously,"² and that its users aren't focused on "find[ing] and watch[ing] protected content online,"³ in reality, Twitter knows people want to engage with music on its platform and markets music information and connections to its users.

Twitter's music-focused marketing is pervasive. Its "[how to](#)" section directly targets artists and record labels, titled "How to promote an album release." And the company recently touted how popular #kpop is on its platform and noted the ten most popular K-pop artists on Twitter.⁴ What they don't tell fans is that, in the last two years, music creators and their partners have been forced to send over 18,000 infringement notices to Twitter for *just three* of those top 10 K-pop artists.

Twitter's head in the sand approach is perhaps most jarring in the case of dedicated pre-release leak accounts, which are often recommended by the auto-complete feature of the service's search function. When a user types the name of a popular artist, it is common for the auto-complete to suggest adding "leak" to the search.

In the last two years, music creators have identified over 100 obvious pre-release leak accounts with names like LeakQueen, ArianaLeaks, KanyeLeaks, LeakCarti, DrakeLeak, MilleyLeaks, HipHopLeaks, etc. It's often not easy to discover infringing behavior, but sometimes it is. Yet even in these simplest cases, Twitter does nothing to proactively find and address these accounts, leaving it to artists, songwriters and their label and publishers partners to do all the work. And while commercially established artists and their representatives can sometimes fill in the gaps, smaller acts, new bands, and non-commercial creators are left with no meaningful recourse at all.

¹ <https://www.riaa.com/wp-content/uploads/2021/02/The-U.S.-Music-Industries-Jobs-Benefits-2020-Report.pdf>

² See February 15, 2021 letter from Twitter to Senators Coons, Hirono, and Tillis ("Twitter letter").

³ Twitter letter, p. 1.

⁴ https://blog.twitter.com/en_us/topics/insights/2021/kpoptwitter-achieves-new-record-of-6-billion-tweets-globally-in-2020.html.

Twitter recently tried to defend this shoddy record to your colleagues in the Senate, arguing that “[C]opyright takedowns worldwide are a tiny fraction of overall Tweets uploaded to the service.”⁵

But obviously, with [hundreds of billions of tweets posted each year](#), a “tiny fraction” of online piracy can do a great deal of damage to artists, creators, and fans. The fact that Twitter failed to take any action regarding 4.5 million instances of infringement on its platform until it received a formal notice makes clear just how big the problem is – and how little the company appears to care about it.

In light of this high volume of piracy on the service, creators’ representatives have repeatedly asked Twitter for high-volume “API” access to the underlying data stream in order to search for and notice infringement of their work at scale. But instead of acting like a responsible partner and providing ready access to this vital tool, Twitter demands creators pay handsomely just for the ability to do necessary monitoring the company itself refuses to undertake. This is a particularly harmful double-edged sword for small creators and independent labels that don’t have the resources either to pay for API access or to endure lengthy litigation after their intellectual property is infringed.

Twitter does offer a free API option, but it is not nearly robust enough for these purposes, with unreasonable limits on the number and quality of searches that can be run, the number of results the system will report, and the time frame that is covered. Twitter already offers free API access at scale to other users, like academic researchers, showing it is feasible to do, but the company refuses to offer the same to artists, songwriters, labels, and publishers, cynically hoping to cash in on our need to stop the theft of our work Twitter itself enables or to simply continue to status quo: making money off the theft of our work.

Twitter’s attack on creators takes other forms as well. It uses an obsolete web form that allows reporting of only 20 infringing tweets at one time, offering only the fallback of email-based reporting to larger users while slow-walking any requests submitted in that way, with erratic response times that often take days and can linger a week or more. And once notice and supposedly removed, the same works routinely reappear, sometimes instantaneously, in a never-ending whack-a-mole challenge. This past year, one infringing track was taken down and reappeared nearly 9,000 times.

Twitter claims the “overwhelming” number of cases of infringement are resolved in minutes, but that’s not our experience. Even when un-released material has been leaked onto the service and the economic and creative damage is piling up by the second, Twitter insists creators follow its slow and cumbersome multistep process.

Twitter must do better.

⁵ Twitter letter, p. 1.

That means providing free access to an API at scale.

It means developing its own content protection technologies or licensing technologies such as PEX, Audible Magic, YouTube's Content ID, or Facebook's Rights Manager that identify and protect copyrighted works to automatically prevent the reappearance of infringing content on sites.

And above all, it means licensing and paying for the music that it uses. Twitter claims it has licensed music "in certain circumstances that warrant it"⁶ But it has yet to explain why the current circumstance in which it intentionally markets music, uses it to build an audience, and hosts millions of infringing performances every year doesn't "warrant" getting fully licensed and paying creators for the value of their work.

Thank you again for your work to make the internet stronger, safer, more secure, and more accountable.

Hopefully, this hearing and your ongoing oversight of technology platforms like Twitter will provide an opportunity for Jack Dorsey to explain why anyone should believe the company's claims about online mis- and dis-information in light of its long track record of broken promises, indifference, and outright extortion when it comes to artists and music creators.

Sincerely,

American Association of Independent Music (A2IM)
Artist Rights Alliance
Music Artists Coalition (MAC)
Nashville Songwriters Association International (NSAI)
National Music Publishers' Association (NMPA)
Recording Academy
Recording Industry Association of America (RIAA)
Songwriters of North America (SONA)

⁶ Twitter letter, p. 3.



March 25, 2021

The Honorable Frank Pallone, Jr., Chairman
 The Honorable Cathy McMorris Rodgers, Ranking Member
 U.S. House Energy and Commerce Committee

The Honorable Michael F. Doyle, Chairman
 The Honorable Robert E. Latta, Ranking Member
 U.S. House Communications and Technology Subcommittee

The Honorable Janice D. Schakowsky, Chairwoman
 The Honorable Gus M. Bilirakis
 U.S. House Consumer Protection and Commerce Subcommittee

Re: Misinformation and Disinformation Plaguing Online Platforms

Dear Chairman Pallone, Ranking Member McMorris Rodgers, Chairman Doyle, Ranking Member Latta, Chairwoman Shakowsky, Ranking Member Bilirakis, and Members of the Subcommittees:

We the undersigned parties, together the Disinfo Defense League, respectfully request that you accept this letter for the record of your March 25, 2021, hearing with the CEOs of Alphabet, Facebook and Twitter to examine misinformation and disinformation on their platforms.

The Disinfo Defense League, or DDL, is a distributed national network of grassroots, community-based organizations that are building a collective defense against disinformation campaigns deliberately targeting Black, Latinx, AAPI, and other communities of color. For the past year, the DDL has taken on the storm of conspiracy theories, half-truths, and lies surgically designed to depress the Black, Brown, Asian American, and Pacific Islander vote. Following the

January 6th insurrection at the Capitol, DDL researchers and members are working together to understand this ongoing threat and to find innovative solutions to combat these attacks on our democracy.

As Mark Zuckerberg, Jack Dorsey, and Sundar Pichai appear before your committee, it is vitally important that you and the CEOs themselves hear directly from grassroots, community leaders about the true cost of disinformation, and the real-world harms impacting our communities, which are perpetuated and amplified by Facebook, Twitter, and YouTube.

Mitigating disinformation is critical to a flourishing and inclusive democracy, and advancing public health and safety. As researchers at Harvard's Shorenstein Center have explained, disinformation disrupts our access to timely, relevant, and accurate information; it takes advantage of algorithmic amplification; and silences its victims through harassment and by inciting fear.¹ Repeated false claims about election fraud, which were proliferated on social and traditional media ahead of January 6th, drove the violent insurrectionist mob to storm the U.S. Capitol. Moreover, a flood of COVID-19 disinformation has led to weak public policy responses undermining our collective ability to mitigate the spread of the virus, and has spurred the politicization of various community safety regulations, which has resulted in massive infection and death rates, disproportionately affecting Black, Latinx, Native American, Indigenous, and Asian American people.

In fact, disinformation routinely and disproportionately harms communities of color, women, immigrants, religious minorities, people living on low incomes, LGBTQIA people and others.

Big Tech not only allows this disinformation, it drives it. Big Tech's hate-and-lie-for-profit business model has built algorithmic systems that direct traffic to content that keeps people engaged and enraged; and they funnel their users to certain kinds of content based, in part, on behavioral and demographic data that the companies collect on them. Facebook's own research revealed that 64 percent of people who find extremist content on the site are led there by Facebook's own recommendations system.² Facebook buried that research for several years, until

¹ See Letter from Joan Donavan et al., Technology and Social Change Team, Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy, to Irene Khan, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations (Feb. 15, 2021) (comment submitted to UN Special Rapporteur's Annual Thematic Report to be presented to the Human Rights Council at its 47th Session in June 2021), <https://mediamanipulation.org/sites/default/files/2021-02/Donovan%20et%20al%20TaSC%20Comment%20-%20FINAL.pdf>.

² See Jeff Horwitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive*, Wall St. J. (May 26, 2020), <https://www.wsj.com/articles/facebook-knws-it-encourages-division-top-executives-nixed-solutions-11590507499>.

the *Wall Street Journal* exposed it. How many such studies have these companies conducted? What else does it know about how its products are harming people and our democracy? These and other important questions must be answered by the CEOs before you today.

As we confront these threats, however, we must remember that hate-and-lie-for-profit punditry is hardly a new phenomenon — and broadcasters and cable companies are exploiting it too, as they have been for many years. Following the historic immigration reform marches in 2006, Lou Dobbs routinely spewed anti-immigrant lies from his CNN perch, falsely claiming for instance that Latinx immigrants were bringing 7,000 cases of leprosy to the United States per year. iHeartRadio (at the time, Clear Channel Radio), the largest radio broadcaster in the country with more than a thousand stations nationwide, is rife with talk shows spewing hate, divisiveness and downright racist conspiracy theories.³

Mega-media conglomerates like Fox News⁴ and Sinclair Broadcast Group,⁵ as well as channels like One America News Network⁶ and Newsmax TV,⁷ are also regular purveyors of hate and disinformation for profit to this day. In the past year alone, they have all spread, and amplified with their huge megaphones, dangerous conspiracies about the pandemic and vaccines, promoted outright lies about voting and the irrefutable outcome of the presidential election, and smeared activists, journalists and members of Congress.

³ See, e.g., Chon A. Noriega & Francisco Javier Iribarren, *Quantifying Hate Speech on Commercial Talk Radio* (Nov. 2011), https://www.chicano.ucla.edu/files/WP01_Quantifying-Hate-Speech.pdf; *Conservative talk radio contributes to more hate of minorities, study says*, Fox News Latino (Aug. 1, 2012), <https://www.chicano.ucla.edu/files/news/TalkRadio-ConservativeTalkRadio-FoxNewsLatino-08-01-12.pdf>; *Clear Channel Radio - A Risky Investment for Bain Capital and Thomas H. Lee Partners: NHMC Calls Investors to Help Stop Trafficking Hate*, LatinHeat (Jun. 14, 2012), <https://www.latinheat.com/the-biz/clear-channel-radio-a-risky-investment-for-bain-capital-and-thomas-h-lee-partners/>; National Hispanic Media Coalition, *American Hate Radio: How a Powerful Outlet for Democratic Discourse Has Deteriorated Into Hate, Racism and Extremism* (2012), https://www.nhmc.org/wp-content/uploads/2021/03/american_hate_radio_nhmc.pdf; National Hispanic Media Coalition, *Clear Channel's Company Culture of Hate Profiteering: How a Corporate Conglomerate Has Grown Immune to Market Forces*, <https://www.nhmc.org/wp-content/uploads/2021/03/Clear-Channels-Company-Culture-of-Hate-Profiteering-Final.pdf> (last visited Mar. 24, 2021).

⁴ See Media Matters for America, *Fox News*, <https://www.mediamatters.org/search?search=Fox+News> (last visited Mar. 24, 2021).

⁵ See Media Matters for America, *Sinclair Broadcast Group*, <https://www.mediamatters.org/search?search=Sinclair+Broadcast+Group> (last visited Mar. 24, 2021).

⁶ See Media Matters for America, *One America News Network*, <https://www.mediamatters.org/search?search=OAN> (last visited Mar. 24, 2021).

⁷ See Media Matters for America, *Newsmax TV*, <https://www.mediamatters.org/search?search=Newsmax> (last visited Mar. 24, 2021).

For these reasons, the undersigned thank you for examining the proliferation of disinformation over Big Tech platforms and urge you to examine the same over Big Media platforms. We look forward to working together to ensure the voices of your constituents impacted by disinformation help inform legislative interventions in Washington.

Respectfully submitted,

Access Now
APIAVote
Arab American Institute (AAI)
Asian Americans Advancing Justice | AAJC
Asian Pacific American Labor Alliance, AFL-CIO
Black Leaders Organizing for Communities (BLOC)
Common Cause
Equality Labs
Free Press Action
Generation Justice
Global Exchange
Higher Height Leadership Fund
Indivisible Northern Nevada
Indivisible Plus Washington
Kairos
MediaJustice
Media Matters for America
NARAL Pro-Choice America
National Council of Asian Pacific Americans (NCAPA)
New Georgia Project
People's Action
ReFrame
Rural Organizing Project
Stop Online Violence Against Women Inc.
UltraViolet
United We Dream
Voto Latino
Women's March



March 25, 2021

The Honorable Michael Doyle
 Chairman, Subcommittee on Communications
 and Technology
 House Energy and Commerce Committee
 2125 Rayburn House Office Building
 Washington, D.C. 20515

The Honorable Jan Schakowsky
 Chair, Subcommittee on Consumer Protection
 and Commerce
 House Energy and Commerce Committee
 2125 Rayburn House Office Building
 Washington, D.C. 20515

The Honorable Robert Latta
 Ranking Member, Subcommittee on
 Communications and Technology
 House Energy and Commerce Committee
 2322 Rayburn House Office Building
 Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
 Ranking Member, Subcommittee on
 Consumer Protection and Commerce
 House Energy and Commerce Committee
 2322 Rayburn House Office Building
 Washington, D.C. 20515

RE: Hearing on “Disinformation Nation: Social Media’s Role In Promoting Extremism And Misinformation”

Dear Chair Doyle, Chair Schakowsky, Ranking Member Latta, and Ranking Member McMorris Rodgers:

Consumer Reports (CR) welcomes today’s joint hearing to examine the role that social media plays in promoting extremism and misinformation online. Current law which governs online platforms fails to provide sufficient incentives for platforms to reduce misinformation and prevent other abuses, such as artificial amplification; indeed, it even shields platforms when their own algorithms *promote* harmful, misleading, or inflammatory extremist content.¹ The largest social media platforms are built to incentivize and reward highly engaging content—despite the harms such content can cause—because their business models rely on, and optimize for, engagement. Engagement ultimately drives up both the amount of time spent on platforms where

¹ John Bergmayer, “What Section 230 Is and Does — Yet Another Explanation of One of the Internet’s Most Important Laws,” Public Knowledge (May 14 2019), <https://www.publicknowledge.org/blog/what-section-230-is-and-does-yet-another-explanation-of-one-of-the-internet-s-most-important-laws/>.

users can be shown advertisements and the amount of data that platforms can collect to more specifically target those ads.² Yet high online engagement metrics have come at the cost of accelerating the spread of harmful, misleading, radicalizing content in the information ecosystem — where, lacking sufficient circuit-breaking context and curation, this content may self-reinforce in ways that keep engagement up — regardless of veracity.³ Platform-facilitated misinformation has contributed to the rapid proliferation of dangerous conspiracy theories that have led not only to anti-vaccination and anti-mask sentiment, but also those which led to the violence at the Capitol on January 6.⁴ It poses a significant risk to consumer health and to the public sphere.⁵ Social media platforms must be sufficiently incentivized to mitigate the harms that their businesses currently enable, amplify, and profit from. But they must also be held accountable for the product design and business decisions that have enabled and incentivized the scale of harm done to the information ecosystem.

Consumer Reports' Work on Platform Responsibility

The Consumer Protection and Commerce Subcommittee's hearing ("Buyer Beware: Fake and Unsafe Products on Online Marketplaces") held last spring, at which CR testified, touched upon some of the difficult challenges caused by online disinformation,⁶ as did last summer's joint hearing on divisive disinformation online ("A Country In Crisis: How Disinformation

²Robert H. Frank, "The Economic Case for Regulating Social Media" The New York Times (February 11, 2021), <https://www.nytimes.com/2021/02/11/business/social-media-facebook-regulation.html>.

³Katherine J. Wu, "Radical ideas spread through social media. Are the algorithms to blame?" PBS (March 28, 2019), <https://www.pbs.org/wgbh/nova/article/radical-ideas-social-media-algorithms/>; *see also* Filippo Menczer and Thomas Hills, "Information Overload Helps Fake News Spread, and Social Media Knows It" Scientific American (December 1, 2020), <https://www.scientificamerican.com/article/information-overload-helps-fake-news-spread-and-social-media-knows-it/>.

⁴Olivia Rubin, Lucien Bruggeman, and Will Steakin, "QAnon emerges as recurring theme of criminal cases tied to US Capitol siege," ABC News, (January 19, 2021) <https://abcnews.go.com/US/qanon-emerges-recurring-theme-criminal-cases-tied-us/story?id=75347445>. *see also* EJ Dickson, "Instagram Is Pushing Anti-Vaccine Misinformation and QAnon Content, Study Finds," Rolling Stone, (March 9, 2021), <https://www.rollingstone.com/culture/culture-news/instagram-anti-vaccine-misinformation-qanon-study-1139002/>.

⁵ Committee on Energy and Commerce Staff to Subcommittee on Consumer Protection and Commerce Members and Staff, September 21, 2020, "Hearing on 'Mainstreaming Extremism: Social Media's Role in Radicalizing America,'" <https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/09.24.20%20CPC%20Hearing%20Memo.pdf>; *see also* Ben Collins, "How QAnon rode the pandemic to new heights — and fueled the viral anti-mask phenomenon" NBC News (August 14 2020):

<https://www.nbcnews.com/tech/tech-news/how-qanon-rode-pandemic-new-heights-fueled-viral-anti-mask-n1236695>; *see also* Tanya Lewis, "Nine COVID-19 Myths That Just Won't Go Away," Scientific American (August 18, 2020), <https://www.scientificamerican.com/article/nine-covid-19-myths-that-just-wont-go-away/>.

⁶ CR's March 4, 2020 testimony is available online here: <https://advocacy.consumerreports.org/research/testimony-of-david-friedman-vice-president-advocacy-consumer-reports-for-u-s-house-hearing-on-fake-and-unsafe-products-on-online-marketplaces/>.

Online Is Dividing The Nation”), to which we also expressed our concerns via letter.⁷ We urged stronger incentives for platforms to protect consumers from fraudulent and illegal consumers in our comments to the Federal Trade Commission on their Endorsement Guidelines updates in June.⁸ In the fall, we submitted public comments to the Federal Communications Commission in part further highlighting the demonstrable need to strengthen incentives for effective content moderation.⁹ Since those hearings, the issues being discussed today have come into even sharper relief: the spread of harmful, extreme conspiracy theories and misinformation has only become more urgent, despite various platforms’ too-little, too-late attempts to patrol and remove the offending content.¹⁰

Last spring, a CR journalist created seven paid ads that intentionally violated Facebook’s pledge to prohibit COVID-19 ads on its platform that encouraged people to drink bleach or ignore social distancing guidelines. Sadly, all seven ads—which included claims that “coronavirus is a HOAX” or to “stay healthy with SMALL daily doses” of bleach—were approved. While CR pulled the ads before they were published by Facebook and viewed by the public, this demonstrates just one of many instances in which Facebook was unable to stop not just the spread of misinformation, but would have been paid for the proliferation of that dangerous misinformation, despite an ad approvals process. This type of paid misinformation could cause obvious harm to consumers and public health—and is just one of many such issues that extremist offshoots and misinformation campaigns have helped foment.¹¹

Finally, just last month, we published our assessment of the related Section 230 legislation proposed last year, and we look forward to continuing to work with Congress on these questions insofar as updates to Section 230 may be concerned.¹²

Platforms Do Not Have Sufficient Incentives to Address Misinformation and Illegal Activity

⁷ CR’s June 24, 2020 letter can be found here: <https://advocacy.consumerreports.org/research/cr-letter-on-joint-hearing-a-country-in-crisis-how-disinformation-online-is-dividing-the-nation/>.

⁸ CR’s June 22, 2020 comments can be found here: <https://advocacy.consumerreports.org/wp-content/uploads/2020/06/CR-Comments-on-FTC-Endorsement-Guides-.pdf>.

⁹ CR’s September 2, 2020 comments to the FCC can be found here: <https://advocacy.consumerreports.org/research/cr-comments-to-the-fcc-on-section-230/>.

¹⁰ Sheera Frenkel and Tiffany Hsu, “Facebook Tried to Limit QAnon. It failed.” New York Times (September 18, 2020), <https://www.nytimes.com/2020/09/18/technology/facebook-tried-to-limit-qanon-it-failed.html>.

¹¹ Kaveh Waddell, “Facebook Approved Ads With Coronavirus Misinformation” Consumer Reports (April 7, 2020), <https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation/>; see also Marianna Spring and Mike Wendling, “How Covid-19 myths are merging with the QAnon conspiracy theory” BBC (September 3, 2020), <https://www.bbc.com/news/blogs-trending-53997203>.

¹² CR’s Section 230 2020 Legislative Round-Up can be found here: <https://medium.com/cr-digital-lab/crs-section-230-2020-legislative-round-up-4683c309fcb3>.

As the Consumer Protection and Commerce Subcommittee noted prior to its September hearing on social media and extremism, while extremists use a wide range of social media platforms, between 2005 and 2016, the majority of extremists (near two-thirds) used Facebook to promote extremism.¹³ Similarly, the extremist QAnon later found a distinct home on the platform, growing unchecked, as Facebook failed to act decisively and explicitly on QAnon until August of last year. This came a month after Twitter, and nearly two years after Reddit explicitly banned key communities centered on the matter—after which, a number of the conspiracy theorists made their new home on Facebook (and more recently, on Facebook-owned Instagram.).¹⁴ New York Times cybersecurity reporter Sheera Frenkel reflected in the fall on a parallel rise in extremist content online back in 2015:

I wonder how different our world would look if Facebook, YouTube and Twitter joined Reddit in taking coordinated, effective action against QAnon. That's what the companies did in 2015 when the Islamic State was using social media to recruit new followers. You could see almost in real time that ISIS lost much of its ability to recruit online.

In my mind, that was the clearest example of the internet companies — when they were motivated to do so — taking action to remove a dangerous group that was pervasive on their sites. This action was supported by the White House, and the internet companies felt empowered to make an overwhelming show of force.¹⁵

Most striking in Frenkel's observation is the caveat: "when they were motivated to do so." While Section 230 of the Communications Decency Act (Section 230) makes it possible for platforms to moderate content, it does nothing to actively *encourage* that moderation, or to encourage responsible platform design in the first place. Internet platforms clearly have the capacity to do more to combat misinformation; while they bear some goodwill costs for providing a bad experience to users, they do not bear all the societal costs from extremism and misinformation, and lack of competition leaves consumers few alternatives in the marketplace. Users who wish to promote extremist content can amplify their message by creating fake accounts and engagement to game sorting algorithms to artificially boost visibility. While platforms prohibit such "coordinated inauthentic activity," the rules are often unclear, and

¹³ The National Consortium for the Study of Terrorism and Responses to Terrorism, "The Use of Social Media by United States Extremists," (2018), www.start.umd.edu/publication/use-socialmedia-united-states-extremists.

¹⁴ Casey Newton, "Facebook's big QAnon crackdown may have come too late" The Verge (August 20, 2020), <https://www.theverge.com/interface/2020/8/20/21375381/facebook-qanon-purge-content-policy-tide-pods>; Kaitlyn Tiffany, "The Women Making Conspiracy Theories Beautiful: How the domestic aesthetics of Instagram repackage QAnon for the masses" The Atlantic, (August 18, 2020).

¹⁵ Shira Ovide, "How Facebook Can Slow QAnon For Real" New York Times, (September 21, 2020), <https://www.nytimes.com/2020/09/21/technology/facebook-qanon.html>.

enforcement is sporadic.¹⁶ Indeed, platforms today have material *disincentives* to moderate deceptive and harmful activity: investing in comprehensive platform moderation would be expensive,¹⁷ while algorithmically recommended and amplified misinformation, fake reviews, views, accounts, harmful influence operations, and other social engagement all artificially amplify the metrics by which platforms are judged by users and investors—and extremist content, in particular, often begets even more engagement—which in turn continue to spread extremism and the harmful misinformation that can accompany it.¹⁸

Recommendation engines and algorithms that serve a bottom line rooted in engagement will seek it out *first*—cost to the public interest and consumer well-being notwithstanding. And so while moderating the inevitable harms of that ecosystem are crucial, just as crucial is responsible ecosystem design that does not incentivize and amplify these harms in the first place. And indeed, it has repeatedly been reported that platforms, once explicitly made aware of these trends, have still actively stifled internal efforts to address them.¹⁹ Without strong counter-incentives, platforms cannot be trusted to build responsible systems that prioritize people and the public interest over profits, nor govern those systems to standards adequate to protect their own users—let alone consumers broadly—from harm.

Potential Reforms

There are a number of ways that Congress can provide strong incentives and sufficient motivations for platforms to more effectively prevent, address, and mitigate the harms that they presently facilitate and worsen. As CR has previously discussed, any conversation around

¹⁶ Evelyn Douek, “What Does “Coordinated Inauthentic Behavior” Actually Mean?” *Slate*, (July 2, 2020), <https://slate.com/technology/2020/07/coordinated-inauthentic-behavior-facebook-twitter.html>; *see also* Judd Legum, “Facebook admits Ben Shapiro is breaking its rules” *popular.info* (July 2, 2020), <https://popular.info/p/facebook-admits-ben-shapiro-is-breaking>; *see also* Craig Silverman, Ryan Mac, and Pranav Dixit, “‘I Have Blood on My Hands’: A Whistleblower Says Facebook Ignored Global Political Manipulation” *Buzzfeed*, (September 14, 2020), <https://www.buzzfeednews.com/article/craigssilverman/facebook-ignore-political-manipulation-whistleblower-memo>.

¹⁷ Paul M. Barrett, “Who Moderates the Social Media Giants? A Call To End Outsourcing” *NYU Stern Center for Business and Human Rights* (June 2020), <https://bhr.stern.nyu.edu/tech-content-moderation-june-2020>; Deepa Seetharaman, “Facebook Throws More Money at Wiping Out Hate Speech and Bad Actors” *The Wall Street Journal* (May 15, 2018), <https://www.wsj.com/articles/facebook-throws-more-cash-at-a-tough-problem-stamping-out-bad-content-1526393256>.

¹⁸ Nicholas Confessore et al., “The Follower Factory” *New York Times* (Jan. 27, 2018), <https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html>; *see also* Max Fisher and Amanda Taub, “How Everyday Social Media Users Become Real-World Extremists” *New York Times* (April 25, 2018), <https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html>.

¹⁹ Jeff Horwitz and Deepa Seetharaman, “Facebook Executives Shut Down Efforts to Make the Site Less Divisive” *The Wall Street Journal* (May 26, 2020), <https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499>; *see also* Karen Hao, “How Facebook got addicted to spreading misinformation” *MIT Technology Review* (March 11, 2021), <https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/>.

content moderation will—and should—inevitably include discussion of Section 230. And there are, of course, further methods for both incentivizing platforms to take responsibility and for holding them accountable for harm that they enable. Ultimately, action in these spaces will ideally be driven by a return to an innovative, transparent, competitive, and open internet: one where platforms are better held accountable for activity they facilitate, and also perhaps one where, structurally, any one platform’s decisions simply cannot ultimately cause the same level of harm as is possible today.

Section 230 originally aimed to encourage the open internet, by broadly insulating online platforms from being treated as publishers, insofar as an offline publication is subject to liability for the content it distributes. Yet any serious discussion on the internet and on content moderation in 2020 must discuss the sheer scope of immunity it presently grants to platforms. Combating misinformation online alone is shaping up to be among the great challenges of the digital age—let alone extremism-fueled misinformation. CR does not support the wholesale repeal of Section 230 by any stretch. Indeed, as discussed in our public comments to the Federal Communications Commission, and in our review of proposed Section 230 legislation that we especially oppose any limiting of Section 230 immunities in response to platforms fact-checking or providing context on misinformation.²⁰

However, we are encouraged by the ongoing Congressional re-evaluation of what Section 230 updated for the modern era might look like, and a number of creative proposals deserve further engagement and consideration. Possibilities range from propositions adding a reasonableness standard,²¹ to those limiting the immunities for civil rights violations,²² to those restricting immunities for paid,²³ targeted,²⁴ or algorithmically recommended²⁵ content—amongst a number of other proposals that could incentivize not only improved platform moderation, but more responsible platform design from the outset.

²⁰ CR’s September 2, 2020 comments to the FCC can be found here: <https://advocacy.consumerreports.org/research/cr-comments-to-the-fcc-on-section-230/>.

²¹ Danielle Keats Citron and Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 419-423 (2017).

²² Pauline Kim, “Manipulating Opportunity” (October 9, 2019), Washington University in St. Louis Legal Studies Research Paper No. 19-10-12, 106 Va. L. Rev. 867 (2020). Available at SSRN: <https://ssrn.com/abstract=3466933>; see also Olivier Sylvain, “Discriminatory Designs on User Data” (April 6, 2018). Knight First Amendment Institute at Columbia University, Forthcoming. Available at SSRN: <https://ssrn.com/abstract=3157975>

²³ John Bergmayer, “How to Go Beyond Section 230 Without Crashing the Internet” Public Knowledge (May 21, 2019), <https://www.publicknowledge.org/blog/how-to-go-beyond-section-230-without-crashing-the-internet/>.

²⁴ U.S. Senate, S. 4337, “Behavioral Advertising Decisions Are Downgrading Services Act” 116th Congress (July 28, 2020), <https://www.congress.gov/bill/116th-congress/senate-bill/4337/text>.

²⁵ Roger McNamee, “Big Tech Needs to Be Regulated: Here Are 4 Ways to Curb Disinformation and Protect Our Privacy,” Time (July 29, 2020), <https://time.com/5872868/big-tech-regulated-here-is-4-ways/>; Bergmayer, *supra* note 19.

Congress could also consider legislation and structural remedies designed to ensure a fairer, more transparent, less concentrated online marketplace. Increasing competitive pressure on online platforms, specifically, could help in a few key ways. Competition could help push platforms toward delivering a product that is more effectively and transparently moderated, and therefore of higher quality for consumers. Increased competitive pressure could also come in the form of interoperability: other companies developing different sorting algorithms for media feeds could introduce diversity to the ecosystem, decreasing the reach of any one platform's moderation inclinations or abilities.²⁶ At the same time, efforts to facilitate and increase competition could reduce the market share of any given platform, and could decrease the reach, and therefore the efficacy of extremist content on its network.

Congress could further consider increasing and improving resourcing for the FTC and other relevant agencies, as Section 5 of the FTC Act may even *require* some level of moderation of harmful content to protect platform users. For at least fifteen years, the FTC has interpreted its Section 5 unfairness authority to require companies to use reasonable data security to prevent third-party abuse of their networks—and it has otherwise previously interpreted Section 5 to require policing of others' actions—such as in Neovi and LeadClick.²⁷ This could reasonably extend, too, to protecting platform users from harmful extremism and related misinformation—and the larger the platform, the greater responsibility to bear and potential harm to remediate.²⁸ Ensuring that the FTC has adequate resources to investigate and ensure adequate consumer protections on platforms may also serve to incentivize platforms to improve their moderation capabilities.

* * *

²⁶ U.S. Senate, S. 2658, “Augmenting Compatibility and Competition by Enabling Service Switching Act of 2019” 116th Congress (October 22, 2019); <https://www.congress.gov/bill/116th-congress/senate-bill/2658/text>; CR’s August 24, 2020 comments to the FTC on data portability and interoperability can be found here: <https://advocacy.consumerreports.org/research/cr-comments-to-the-ftc-on-data-portability/>.

²⁷ See Footnote 6. See also Press Release, “FTC Action Results in Contempt Order Against Online Check Writing Marketers”, Fed. Trade Comm'n (Jul. 27, 2012), <https://www.ftc.gov/news-events/press-releases/2012/07/ftc-action-results-contempt-order-against-online-check-writing>; Press Release, “U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for Lean-Spa Weight-Loss Supplement” Fed. Trade Comm'n (Oct. 4, 2016), <https://www.ftc.gov/news-events/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network>.

²⁸ Alexandra Berzon, Shane Shifflett, and Justin Scheck, “Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products” Wall Street Journal (August 23, 2019), <https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990>; see also Olivia Solon, “Facebook Management Ignored Internal Research Showing Racial Bias, Employees Say” NBC News (July 23, 2020), <https://www.nbcnews.com/tech/tech-news/facebook-management-ignored-internal-research-showing-racial-bias-current-former-n1234746> <https://www.nytimes.com/2019/11/28/business/online-reviews-fake.html>.

The rapid spread of extremism online, and the resultant proliferation of false remedies, conspiracy theories, misinformation, open up huge potential for real-world consumer harm — from anti-vaccine sentiment to the fomenting of real-world violence. American consumers deserve relief from the algorithmically-amplified harms that the largest online platforms incentivize and facilitate. Online platforms must be better held to account for the spread of extremism and misinformation, and significantly more incentivized to responsibly design, prevent, and appropriately handle the ever-rising tide of misinformation and its accompanying harms to consumers. We look forward to working with the Committee, colleague organizations, and industry to develop and implement novel solutions to meet this challenge of our time and ensure a safe online marketplace for American consumers.

Thank you for considering CR's views and allowing us to contribute to the ongoing discussion as we all seek to secure a safe, fair online marketplace for American consumers.

Sincerely,

Laurel Lehman
Policy Analyst

Jonathan Schwantes
Senior Policy Counsel

Justin Brookman
Director, Technology Policy

cc. Members of the House Energy and Commerce Committee



March 25, 2021

The Honorable Michael Doyle, Chairman
House Energy & Commerce Committee
Subcommittee on Communications & Technology
Washington, D.C. 20515

The Honorable Janice Schakowsky, Chairman
House Energy & Commerce Committee
Subcommittee on Consumer Protection & Commerce
Washington, D.C. 20515

The Honorable Robert Latta, Ranking Member
House Energy & Commerce Committee
Subcommittee on Communications & Technology
Washington, D.C. 20515

The Honorable Gus Bilirakis, Ranking Member
House Energy & Commerce Committee
Subcommittee on Consumer Protection & Commerce
Washington, D.C. 20515

Chairs Doyle and Schakowsky and Ranking Members Latta and Bilirakis:

On behalf of the Coalition for a Secure & Transparent Internet (CSTI) we write in support of the Committee's ongoing efforts to address disinformation campaigns, both on social media platforms and across the Internet.

CSTI was founded in 2018 by a diverse set of stakeholders who shared similar concerns over the potential impact the implementation of the European Union's General Data Protection Regulation (GDPR) would have on the ability to ensure timely access to WHOIS information.

WHOIS information has historically been used by law enforcement, consumer advocacy groups, third-party investigators, intellectual property holders and others to identify *who is* behind a domain name or website. If the registrant of a website or domain is conducting illegal or otherwise malicious activity, investigators can access information about the registrant to pursue legal avenues as well as identify other, potentially dangerous domains that are also attributed to that registrant. In this way, WHOIS is critical to our ability to identify, end as well as proactively prevent cybercrimes, exploitation, fraud (including disinformation), intellectual property theft and other harmful activity.

As the Committee continues to examine these issues, CSTI encourages it to consider how WHOIS can help *identify* bad actors involved in these disinformation campaigns; the need for WHOIS information to *connect* participants engaged in these campaigns; and the role WHOIS plays in *shutting down* such campaigns.

Several Executive branch agencies shared their views on this subject in response to Congressman Latta's inquiries last year and their comments are worth noting. In its July 2020 response to Congressman Latta, the U.S. Federal Trade Commission said:

"Before the GDPR took effect in May of 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud."



In its response to Congressman Latta (also in July of 2020), the U.S. Immigration & Customs Enforcement Homeland Security Investigations and the National Intellectual Property Rights Coordination Center said this regarding WHOIS:

"HSI uses domain name registration information, previously available via online WHOIS query, to aid in the identification of persons or entities responsible for registering domains that are used to conduct a wide variety of crimes, which include intellectual property crimes, cyber-crimes (such as the theft of personally identifiable information [PII] and credit card information), crimes related to illegal importation and exportation of goods, and the promotion and distribution of child sex abuse material."

Copies of these letters are enclosed.

Facebook, which is not a member of CSTI but is testifying today, has also expressed its concerns over the loss of WHOIS and the impact it has on protecting its own users. In a September 2020 letter to the National Telecommunications & Information Administration the company noted:

"WHOIS information and access is critical to protect the Facebook family of products from cybersecurity threats and fraud. Ensuring that WHOIS data is accurate, uniform, and easily accessible is key to our efforts to identify bad actors that target our platform and users with things like fake news, phishing attacks, brand infringement, and other malicious activity."

A copy of the letter is enclosed.

The restoration of open, accessible WHOIS information will greatly enhance the ability of law enforcement, consumer advocates and others to identify and put an end to disinformation campaigns on social media platforms and across the Internet.

We thank you for your consideration of this important issue and stand ready to work with you and your staff moving forward.

Sincerely,

The Coalition for a Secure & Transparent Internet

Enclosures



1 Hacker Way
Menlo Park, California 94025
United States of America

September 2, 2020

The Honorable Adam Candeb
Acting Assistant Secretary of Commerce for Communications and
Information Herbert C. Hoover Building
U.S. Department of Commerce
National Telecommunications and Information Administration
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Re: Additional Information Regarding WHOIS

Dear Adam,

Thank you for taking the time last month to listen to industry stakeholders regarding the importance of WHOIS and the problems we've identified with the ICANN policy proposals for a new system of WHOIS access.

I'm following up on your request for additional information regarding this topic, and its continued importance to Facebook.

- WHOIS information and access is critical to protect the Facebook family of products from cybersecurity threats and fraud. Ensuring that WHOIS data is accurate, uniform, and easily accessible is key to our efforts to identify bad actors that target our platform and users with things like fake news, phishing attacks, brand infringement, and other malicious activity.
- WHOIS is also important to ensure transparency and accountability on the Internet across the globe. WHOIS helps build an ecosystem of trust and security that not only impacts Facebook users, but supports the billions of users worldwide that rely on the Internet to engage in commerce, use social media to stay connected, and build communities.
- The usefulness of the WHOIS system has been significantly impaired since 2018. We no longer have meaningful, timely access to WHOIS as an investigative tool to identify bad actors and domain names involved in cybersecurity threats. Facebook now encounters significant delays and denials of access when requesting WHOIS, even in clear-cut cases of phishing, fraud and trademark infringement. This overall unavailability of WHOIS (with an over 70% denial rate) has made our efforts to fight these types of abuses much more difficult.¹
- The problem continues unabated in the face of increased abuse related to COVID. In the first few months of the COVID crisis, Facebook responded with a targeted, global enforcement

effort (for abuse outside of Facebook's platforms) to stop bad actors from harming our users and platforms during the pandemic. We identified over 3500+ phishing campaigns involving our brands and COVID-related matters, responded to over 600 potentially infringing/fraudulent off-platform COVID social media entries, over 250 fraudulent/infringing COVID domain names, and defensively registered over 1000 domain names containing our major brands and COVID-related terms across the key top-level domains to help pro-actively block virus-related abuse. Yet despite our efforts to address this abuse quickly, we were routinely denied WHOIS access for COVID related DNS abuse.

- It's been over two years since ICANN convened the expedited policy process known as the EPDP to resolve this issue. Unfortunately, this is not an issue that is capable of being fixed by ICANN through its multi-stakeholder model and policy processes. If adopted, ICANN's proposed access system would repeat today's broken WHOIS system where very few legitimate requests actually result in disclosure. Moreover, the lack of automated responses, even in obvious cases of phishing, fraud and trademark abuse, will result in significant delays to mitigation efforts, when quick action is critical to prevent massive consumer harm.

I hope this gives you a better understanding of Facebook's perspective on this important topic. Please feel free to reach out to me if you have any questions or would like additional information.

All the best,

Margie Milam
Intellectual Property & DNS Policy Lead
Facebook, Inc.

¹ Our experience is not unique among technology companies. For examples, please see the [statement](#) by the Cybersecurity Tech Accord on November 30, 2018 describing several compelling examples of the challenges faced by member companies in mitigating cybersecurity threats in the absence of WHOIS.

FACEBOOK



Office of the Chairman

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
 WASHINGTON, D.C. 20580

July 30, 2020

The Honorable Robert E. Latta
 United States House of Representatives
 Washington, D.C. 20515

Dear Representative Latta:

Thank you for your June 24, 2020 letter requesting information about how the Federal Trade Commission (“FTC” or “Commission”) uses domain name registration information, also known as WHOIS, to carry out its law enforcement mission, including its efforts to stop frauds related to COVID-19. You also highlighted your concerns that the implementation of the European Union’s General Data Protection Regulation (“GDPR”) has negatively affected the ability of law enforcement to identify bad actors online. I share your concerns about the impact of COVID-19 related fraud on consumers, as well as the availability of accurate domain name registration information.

Since the beginning of the pandemic, the FTC has been monitoring the marketplace for unsubstantiated health claims, robocalls, privacy and data security concerns, sham charities, online shopping fraud, phishing scams, work at home scams, credit scams, and fake mortgage and student loan relief schemes, and other deceptions related to the economic fallout from the COVID-19 pandemic.¹ In response, we have taken actions, including filing four cases in federal courts and sending hundreds of warning letters to businesses in the United States and abroad.² In addition, we have conducted significant public outreach and education efforts.³

Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud.⁴ The FTC uses this information to help identify wrongdoers and their locations, halt their conduct, and preserve money to return to defrauded victims. Our agencies may no longer rely on this information because, in response to the GDPR, ICANN developed new policies that significantly limit the publicly available contact information relating to domain name registrants. For

¹ See generally Prepared Statement by the Federal Trade Commission before the S. Comm. on Commerce, Science, and Transp., Subcommittee on Manufacturing, Trade, and Consumer Protection: Consumer Protection Issues Arising from the Coronavirus Pandemic (July 21, 2020), <https://www.ftc.gov/public-statements/2020/07/prepared-statement-federal-trade-commission-consumer-protection-issues>.

² See generally <https://www.ftc.gov/coronavirus>. This page is updated regularly.

³ *Id.*

⁴ See, e.g., Comment of the Staff of the FTC Bureau of Consumer Protection before the ICANN Public Comment Forum, In the Matter of Tentative Agreements among ICANN, U.S. Dep’t of Commerce, and Network Solutions, Inc. (Oct. 29, 1999), <https://www.ftc.gov/policy/policy-actions/advocacy-filings/1999/10/ftc-staff-comment-internet-corporation-assigned-names>; Prepared Statement of the Federal Trade Commission, Hearing on Internet Governance: The Future of ICANN, Before the Subcommittee on Trade, Tourism, and Econ. Dev. of the S. Committee on Commerce, Science, and Transp., 109th Cong. (Sept 20, 2006), <http://www.ftc.gov/os/testimony/P035302igovernancefutureicanncommissiontestsenate09202006.pdf>.

The Honorable Robert E. Latta – Page 2

example, before the GDPR went into effect, the FTC could quickly and easily obtain detailed information about the name, address, telephone number and email of the domain name registrant by typing a simple query. Since May 2018, however, we generally must request this information directly from the particular registrar involved. This can be a time-consuming and cumbersome process.⁵

This lack of access also limits consumers' ability to identify bad actors using WHOIS information. Prior to the GDPR, thousands of the complaints filed in our Consumer Sentinel complaint database referred to the filer's use of WHOIS data to identify businesses involved in spyware, malware, imposter scams, tech support scams, counterfeit checks, and other malicious conduct.⁶

The FTC would benefit from greater and swifter access to domain name registration data. Achieving this goal is difficult, however, given the complexity of the GDPR's effect, the required international coordination, and the many stakeholders involved. We have been working with other U.S. agencies to develop solutions through our interaction with ICANN and our international law enforcement colleagues.

One approach that could help overcome the current obstacles would be to mandate disclosure of domain name registration data associated with legal entities, as opposed to natural persons. Legal entities register a significant percentage of domain names, and the GDPR protects the information of natural persons but does not apply to information related to legal entities. ICANN's current mechanisms result in over-application of the GDPR by permitting registrars to choose whether to make the registration data of legal entities public or not. We have raised this issue within ICANN's policy development process.

I appreciate your interest in these issues. If you or your staff has additional questions or comments, please contact Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195.

Sincerely,



Joseph J. Simons
Chairman

⁵ There are more than 2,500 ICANN accredited registrars, many located outside the U.S., with different procedures to obtain registrant data. It can be challenging to determine where to direct a request and what to include in such request for access to this now non-public information as many registrars fail to place such guidance in a location that is easy to find on their websites. After submitting a request, the FTC must wait for the registrar to approve or reject our requests. Moreover, when data is located in a foreign jurisdiction, the process may be more time consuming and require cooperation from our law enforcement partners.

⁶ In 2017, we identified over 4,000 complaints filed over a five-year-period.

Office of Congressional Relations

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536



**U.S. Immigration
and Customs
Enforcement**

July 16, 2020

The Honorable Robert E. Latta
U.S. House of Representatives
Washington, DC 20515

Dear Representative Latta:

Thank you for your June 24, 2020 letter to U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI) and the National Intellectual Property Rights Coordination Center (IPR Center) regarding the European Union's General Data Protection Regulation (GDPR) and its impact on HSI's ability to obtain WHOIS information in support of its criminal investigations.

HSI uses domain name registration information, previously available via online WHOIS query, to aid in the identification of persons or entities responsible for registering domains that are used to conduct a wide variety of crimes, which include intellectual property crimes, cyber-crimes (such as theft of personally identifiable information [PII] and credit card information), crimes related to illegal importation and exportation of goods, and the promotion and distribution of child sex abuse material.

HSI used WHOIS data regularly prior to the implementation of GDPR in May 2018. Subsequent to GDPR, the inability to conduct instant electronic queries has added an extra step and slowed down the investigative process. HSI continues to request and use domain name registrant information via legal process from registrars who maintain that information. The registries and registrars review requests for information and determine if the requestor has the authority, if the order was issued by a court of competent jurisdiction, and whether the request violates any portion of the GDPR. Unfortunately, there is no centralized point of contact from whom to request the information, and with over 2,000 registrars, some outside of the United States, it is sometimes difficult to determine who to contact and how to procure a legal order they will recognize and respond to. In addition to slowing the process to get registrant information, the likelihood of getting a judicial order for the release of information can be difficult since a number of requests are made in the initial stage of an investigation or response and agents may not have enough information on the criminal activity to satisfy necessary requirements. Lastly, due to the penalties that can be imposed by GDPR for improper release of a registrant's PII, many registries and registrars are redacting registrant information regardless of whether or not the subject is a citizen within the European Union.

As a recent example of GDPR inhibiting HSI investigations, the HSI Cyber Crime Center (C3) Cyber Crimes Unit identified several websites posing as legitimate coronavirus disease 2019 (COVID-19) fundraising organizations, but are actually fraudulent. These websites claim to be sites for entities such as the World Health Organization, United Nations' foundations, and other non-governmental organizations, and appear to be legitimate. When HSI conducted WHOIS queries for these domains, most of the subscriber information was redacted as a result of GDPR. Having

www.ice.gov

The Honorable Robert E. Latta
Page 2

increased and expedient access to domain name registration information would have allowed HSI to identify the registered owners of the domains expeditiously in order to prevent further victimization by these illegitimate fundraising websites. When HSI is required to use legal process (e.g. administrative subpoenas, non-disclosure orders, or grand jury subpoenas) to obtain registrant information, this can cause delays and potentially negatively impact an investigation.

HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain.

In an effort to address the challenge of limited WHOIS information as a result of GDPR, the HSI C3 has assigned full-time representatives to the Public Safety Working Group (PSWG) within the Internet Corporation for Assigned Names and Numbers (ICANN) organization. The PSGW is comprised of law enforcement and consumer protection agencies that work closely with various constituencies that are represented within the ICANN ecosystem. In the absence of a more viable solution, HSI C3 members on the PSGW continue to work with registries, domain registrars, and civil society groups to develop a consensus solution for access to domain name registration information within the ICANN framework and compliant with GDPR.

Thank you again for your letter and interest in this matter. Should you wish to discuss this matter further, please do not hesitate to contact me at (202) 732-4200.

Sincerely,

Sean Hackbart
for

Raymond Kovacic
Assistant Director
Office of Congressional Relations



**Written Statement of
Sikh American Legal Defense and Education Fund**

**Before the United States House of Representatives
Committee of Energy & Commerce
Subcommittee on Communications and Technology
Subcommittee on Consumer Protection and Commerce**

**Hearing on “Disinformation Nation:
Social Media’s Role in Promoting Extremist and Misinformation”
March 25, 2021**

Dear Chairman Doyle, Chairwoman Schakowsky, Ranking Member Bilirakis, Ranking Member Latta, and Members of the Committee:

On behalf of the Sikh American Legal Defense and Education Fund (SALDEF) and the Sikh American community, thank you for the opportunity to submit this written statement to the Communications and Technology and Consumer Protection and Commerce Subcommittees.

Despite representing a significant portion of the Indian diaspora in the United States, Sikhs are an underrepresented religious minority both here and in India. After 9/11, hate crimes, bullying, and bigotry against the Sikh American community increased significantly, largely due to their visible articles of faith. Now, in the age of social media, these incidents have become systematic in nature, censoring information relevant to Sikhs and promoting disinformation that incites violence against their communities.

The Sikh American Legal Defense and Education Fund (SALDEF) was founded in 1996 as an organization to promote awareness about Sikhism. Now, nearly 25 years later, it is the oldest Sikh civil rights organization in the United States working with its partners in Congress and across the nation to increase representation of Sikh Americans in government and policy. On behalf of the Sikh American community, we strongly urge Members of Congress to shed light on the plight of religious minorities on social media platforms, including those of Sikh Americans.

We are deeply concerned about ongoing Sikh censorship and the spread of anti-Sikh disinformation on social media platforms, including Facebook, Twitter, and Youtube. Of particular note for the Sikh community is the recent uptick in censorship and disinformation as a tactic of suppression by the Indian government, supporters of the current Administration, and other nationalist groups. While these tactics have been in place for years, they have expanded dramatically due to the resistance against the Indian Agricultural Acts of 2020, commonly known

Statement of SALDEF
March 25, 2021

as the Farmers' Protests. These incidents are having a direct impact on communities across the globe, including in the United States.

Oftentimes armed with information obtained from online platforms¹, the Indian government has targeted², arrested³, and tortured⁴ journalists and activists for their advocacy against the actions of the Indian government. Recently, India's status as a free nation dropped⁵, and what is especially concerning to commentators, political observers, and members of the Sikh American community is how closely these actions mirror those of other governments who place restrictions on the press, social media, and discussion of sociopolitical issues. Recent examples include the Chinese government in spreading disinformation during the Hong Kong protests⁶ and concealing its genocide against the Uyghurs⁷, the Myanmar military in inciting a genocide against the Rohingya people⁸, and Turkish regime in censoring information on social media to favor its autocracy⁹.

Of particular note to the Sikh American community are the actions being taken on social media to limit the spread of information about the Farmers' Protests, Sikh advocacy, and Sikh holidays with the cooperation of US-based technology companies. Further, the Sikh American community is concerned about the potential for targeting individuals who express support for the protests or speak out against the actions of the Indian government, given its demonstrated history of already doing so. Lastly, Sikh Americans are troubled by the impact of domestic Indian policies on the rights of individuals outside of India. For example, see the reaction to celebrities such as Rhianna¹⁰, Meena Harris¹¹, and Greta Thunberg¹², who expressed support for the Farmers' Protests.

¹ Klein, Naomi. "India Targets Climate Activists With the Help of Big Tech." *The Intercept*, 27 Feb. 2021, theintercept.com/2021/02/27/india-climate-activists-twitter-google-facebook/.

² TNN / Feb 3, 2019. "Youth Detained for 'Mistakenly' Liking Facebook Post Supporting Khalistan: Dehradun News - Times of India." *The Times of India*, TOI, timesofindia.indiatimes.com/city/dehradun/youth-detained-for-mistakenly-liking-facebook-post-supporting-khalistan/articleshow/67821860.cms.

³ Singh, Vijaita. "Evidence Gathered from Social Media Secures Conviction in Khalistani Case." *The Hindu*, The Hindu, 12 July 2019, www.thehindu.com/news/national/evidence-gathered-from-social-media-secures-conviction-in-khalistani-case/article28414529.ece.

⁴ Gopal, Navjeevan. "House Committee to Probe 'Torture' of Sikh Youths in Tihar, Labour Right Activists in Haryana Jail." *The Indian Express*, 6 Mar. 2021, indianexpress.com/article/cities/chandigarh/committee-to-probe-torture-of-sikh-youths-in-tihar-labour-right-activists-in-haryana-jail-no-deep-7216419/.

⁵ "India: Freedom in the World 2021 Country Report." *Freedom House*, freedomhouse.org/country/india/freedom-world/2021.

⁶ Stewart, Emily. "How China Used Facebook, Twitter, and YouTube to Spread Disinformation about the Hong Kong Protests." *Vox*, Vox, 29 Aug. 2019, www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media.

⁷ Samuel, Sigal. "China Paid Facebook and Twitter to Help Spread Anti-Muslim Propaganda." *Vox*, Vox, 22 Aug. 2019, www.vox.com/future-perfect/2019/8/22/20826971/facebook-twitter-china-misinformation-ughur-muslim-interment-camps.

⁸ Mozur, Paul. "A Genocide Incited on Facebook, With Posts From Myanmar's Military." *The New York Times*, The New York Times, 15 Oct. 2018, www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

⁹ "Turkey: Social Media Law Will Increase Censorship." *Human Rights Watch*, 28 Oct. 2020, www.hrw.org/news/2020/07/27/turkey-social-media-law-will-increase-censorship.

¹⁰ "Farmers' Protest: Rihanna Tweet Angers Indian Government." *BBC News*, BBC, 3 Feb. 2021, www.bbc.com/news/world-asia-india-55914858.

¹¹ "Meena Harris Doubles Down on Support to Farmers, Slams 'Militant Nationalism'." *The Wire*, thewire.in/world/meena-harris-support-farmers-protest-militant-nationalism.

¹² "Greta Thunberg Effigies Burned in Delhi after Tweets on Farmers' Protests." *The Guardian*, Guardian News and Media, 4 Feb. 2021, www.theguardian.com/world/2021/feb/04/greta-thunberg-effigies-burned-in-delhi-after-tweets-on-farmers-protests.

Statement of SALDEF
March 25, 2021

The actions of the Indian government, in conjunction with the full cooperation of big-tech corporations like Facebook, Twitter, and Google, play into a broader movement¹³ of unapologetic nationalism at the cost of religious minorities on the South Asian subcontinent. This active repression of the freedom of expression, protest, and speech only contributes to a growing instability in the region. As the paragon of democracy, the United States owes it to its citizens—many of whom are Sikhs and descendants of the Indian diaspora—to hold these social media platforms accountable to the freedom of speech. Without this, we will only see an even greater rise in the targeting of Sikh Americans and religious minorities—both at home and abroad.

Sikh Censorship on Social Media Prior to the Indian Farmers' Protests

We have chosen to analyze the systematic censorship of the Sikh community in two categories: censorship prior to the start of the Indian Farmers' Protests and censorship during the Indian Farmers' Protests. This lens of analysis is merely a superficial method of breaking down the problem—the same issues of cultural insensitivity, deprioritization of minorities, and easily manipulatable digital infrastructure exist at the root of both.

Since the development of social media as the predominant method for political discourse, political actors have hoped to seize control of the medium out of fear of its power for collective engagement. The Indian government has been no stranger to this means of political control in cases dealing with the Sikh community. A July 2020 report from the World Sikh Organization of Canada¹⁴ details hundreds of instances in which Sikhs have been unlawfully arrested without trial because of 'social media activity.' Human rights activists, political dissenters, and members of minority communities, especially Sikhs, have faced the brunt of these charges and arrests because of social media discourse. The lack of pre-existing internationally-enforced norms focused on social media conduct has led to the systematic suppression of peaceful communities.

Even if the use of social media platforms for political suppression was conducted without cooperation with these platforms, it would still be incumbent on social media firms to prevent the use of their product for anti-democratic activity. However, social media companies, particularly Facebook through their Facebook and WhatsApp platforms, have on many occasions provided data from their servers for critical evidence in arrests and detainment. For example, in 2019, an 18-year-old boy in India was arrested after liking a poem on Facebook promoting a controversial Sikh-related political doctrine; and was released only after agreeing to deactivate his account.¹⁵ Similarly, the Indian government received assistance from WhatsApp and Facebook servers in

¹³ <https://www.v-dem.net/en/news/democratic-backsliding-india-worlds-largest-democracy/>

¹⁴ World Sikh Organization of Canada. *Enforcing Silence: India's War on Sikh Social Media*. July 2020, d3n8a8pro7vhmx.cloudfront.net/worldsikh/pages/824/attachments/original/1595202264/WSO_Social_Media_Crackdown_Report.pdf?1595202264.

¹⁵ TNN / Feb 3, 2019. *Youth Detained For 'Mistakenly' Liking Facebook Post Supporting Khalistan*. Dehradun News - Times of India. timesofindia.indiatimes.com/city/dehradun/youth-detained-for-mistakenly-liking-facebook-post-supporting-khalistan/articleshow/57821860.cms.

Statement of SALDEF
March 25, 2021

the United States to convict Jarman Singh on political charges.¹⁶ Such instances of anti-democratic cooperation represent a profound failure on the part of social media firms to protect their users of vulnerable minority communities.

Social media firms have also been responsible for repeated and flagrant acts of undue content moderation against the Sikh community for much of 2020. With the global pandemic raging, online forums have become increasingly important as centers for political discourse. Additionally, as a diasporic community, online means of communication are essential for Sikh community organizing and information flow. The lack of accountability of these social media firms has disrupted our community's ability to congregate and respond to the growing crisis facing its members.

On many occasions, especially around the anniversary of Operation Blue Star (June)¹⁷ and the 1984 anti-Sikh pogroms (November)¹⁸, #Sikh has been blocked by Instagram without any explanation as to why or what decision-making process went into informing those actions. The wholesale removal and suppression of a benign religious channel of discourse is unprecedented in the history of media and should have warranted a more urgent response.¹⁹ Yet, little continues to be said by these social media platforms about how they are ensuring that they protect the right to freedom of speech in and beyond India, especially as it relates to American citizens.

While instances of overt and visible censorship are more eye-catching and easily solvable by social media firms, a worrying undercurrent²⁰ of less visible content moderation remains the largest challenge to the Sikh community. On Instagram, for much of 2019 and 2020, all Sikh-related hashtags (including #Sikh, #Sikhism, #Turban, #Khalsa, and #Gurdwara) were constantly inundated with Turkish-language graphic pornographic bot spam that made these channels unuseable for community members. Additionally—especially around Sikh religious and cultural holidays, days of remembrance, and tragic anniversaries—benign individual posts will be flagged as 'hate speech' and removed by Instagram's algorithm. These same patterns of undue content moderation have similarly been visible on Twitter, alongside the simultaneous allowance of violent hate speech targeted at community members.

This level of censorship falls under a broader pattern of systematic oppression against minorities in and beyond India.²¹ Unfortunately, these issues have only heightened with the rise of the peaceful Indian Farmers' Protest.

¹⁶ World Sikh Organization of Canada. *Enforcing Silence: India's War on Sikh Social Media*. July 2020, d3n8a8pro7vhmx.cloudfront.net/worldsikh/pages/824/attachments/original/1595202264/WSO_Social_Media_Crackdown_Report.pdf ?1595202264.

¹⁷ "Instagram Blocks #Sikh Hashtag for the Second Time." *AsAmNews*, 1 Dec. 2020, asamnews.com/2020/12/01/instagram-blocked-the-sikh-hashtag-amidst-the-punjab-farmers-protest/.

¹⁸ Admin, and Admin. "Facebook Censoring Sikhs during #SikhGenocide Week." *SikhPA*, 3 Nov. 2020, www.sikhpaa.com/facebook-censoring-sikhs-during-sikhgenocide-week/.

¹⁹ Philipose, Rahel. "#Sikh Hashtag Ban Lifted, but Community Still Looking for Answers." *The Indian Express*, 15 June 2020, indianexpress.com/article/technology/social/sikh-hashtag-ban-lifted-but-community-still-looking-for-answers-6460117/.

²⁰ Singh, Jagmeet. "Instagram Blocks #Sikh Hashtag Yet Again for Some Users." *NDTV Gadgets 360*, Gadgets 360, 28 Nov. 2020, gadgets.ndtv.com/apps/news/instagram-sikh-hashtag-block-facebook-2331467.

²¹ Person, "The Farmers' Protests Are a Turning Point for India." *Time*, Time, 12 Feb. 2021, time.com/5938041/india-farmer-protests-democracy/.

Statement of SALDEF
March 25, 2021

Sikh Censorship on Social Media During the Indian Farmers' Protests

In response to the Indian Agricultural Acts of 2020, farmers across India have been protesting since November 2020. Commonly referred to as the Indian Farmers' Protests, this movement is the largest protest in modern Indian history. What's more, Sikh and Punjabi Americans across the world, including in dozens of American cities, have also been rallying in support of the farmers and their movement.

The response of the Indian government, however, has been particularly alarming.²² While the protests have been overwhelmingly peaceful, and have even served as sites for schooling, makeshift malls, and health clinics, they have been met by force from Indian law enforcement—the nature of which has been both excessive and, in certain cases, unlawful. Specifically, as more than 248 farmers died during the protests,²³ the Indian government and its respective law enforcement arms have taken a systematic approach to suppressing the movement. Human rights activists, including Disha Ravi,²⁴ Nodeep Kaur,²⁵ and Shiv Kumar,²⁶ have been kidnapped, imprisoned, sexually abused, and physically tortured. Journalists, including Mandeep Punia from *The Caravan*,²⁷ have been targeted,²⁸ illegally detained,²⁹ and charged.³⁰ Even an American physician from New Jersey who had traveled to Delhi in order to provide free medical aid to other injured protestors was brutally beaten by the Indian police.³¹ Most recently, a group of 25 women who refused to remove the *Nishaan Sahib* flag (i.e. a flag representing the Sikh faith) and the *morcha* flag (i.e. the flag representing the Farmers' Protests) were arrested; among those detained was a two-year-old toddler.³²

As a result, several Senators and Members of Congress have spoken out about the human rights violations that have been taking place in India. These members include Senator Robert

²² "US Lawyers Write to President Biden on Farmers' Protests, Modi Govt's Repressive Tactics." *The Wire*, thewire.in/rights/farmers-protests-uapa-caa-minority-muslim-sikh-joe-biden.

²³ Chaba, Anju Agnihotri. "248 Farmers Have Died during Protest against Three Agri Laws'." *The Indian Express*, 21 Feb. 2021, indianexpress.com/article/india/248-farmers-have-died-during-protest-against-three-agri-laws-7198797/.

²⁴ "What Exactly Is the Crime Disha Ravi Is Accused Of?" *The Wire*, thewire.in/rights/disha-ravi-toolkit-sedition-bail-farmers-protest-khalistan.

²⁵ Pandey, Geeta. "Nodeep Kaur: The Jailed Activist Meena Harris Tweeted About." *BBC News*, BBC, 17 Feb. 2021, www.bbc.com/news/world-asia-india-56071706.

²⁶ Ajay Sura / TNN / Feb 19, 2021. "Farmers Protests: Punjab and Haryana HC Orders Medical Examination of Labour Activist Shiv Kumar: Chandigarh News - Times of India." *The Times of India*, TOI, timesofindia.indiatimes.com/city/chandigarh/farmers-protests-punjab-and-haryana-hc-orders-medical-examination-of-labour-activist-shiv-kumar/articleshow/81112915.cms.

²⁷ Bal, Hartosh Singh. "If India Can Charge Journalists with 'Sedition' for Doing Their Jobs, It Has No Free Press ." *The Guardian*, *Guardian News and Media*, 6 Feb. 2021, www.theguardian.com/commentisfree/2021/feb/06/india-journalists-sedition-no-free-press-police-farmers-modi.

²⁸ Al Jazeera. "Indian Journalists Accused of Sedition for Farmer Protest Reports." *Freedom of the Press News | Al Jazeera*, Al Jazeera, 1 Feb. 2021, www.aljazeera.com/news/2021/2/1/indian-journalists-accused-of-sedition-over-farmers-stir-reports.

²⁹ Kajal, Kapil, et al. "Muzzled, Detained, Jailed: What Journalists Face at Farmers' Protest Site." *The Federal*, 1 Feb. 2021, thefederal.com/news/muzzled-detained-jailed-what-journalists-face-at-farmers-protest-site/.

³⁰ "India: Journalists Covering Farmer Protests Charged." *Human Rights Watch*, 2 Feb. 2021, www.hrw.org/news/2021/02/02/india-journalists-covering-farmer-protests-charged#.

³¹ Patel, Bhavisha. "US Doctor and His Team Are 'Brutally Beaten' by Police." *Daily Mail Online*, Associated Newspapers, 30 Jan. 2021, www.dailymail.co.uk/news/article-9205129/US-doctor-team-brutally-beaten-police.html.

³² "Women Protesters on Their Way to Gurdwara Rakabganj Refuse to Remove 'Flags', Detained." *Tribuneindia News Service*, 3 Mar. 2021, www.tribuneindia.com/news/punjab/women-protesters-refuse-to-remove-flags-detained-220217.

Statement of SALDEF
March 25, 2021

Menedez (NJ),³³ Senator Cory Booker (NJ), Representative Brendan Boyle (PA-2), Representative Debbie Dingell (MI-120), Representative Jim Costa (CA-16),³⁴ Representative Josh Gottheimer (NJ-5), Representative Josh Harder (CA-10),³⁵ Representative Brian Fitzpatrick (PA-1), Representative John Garamendi (CA-3),³⁶ Representative Pramila Jayapal (WA-7), Rep. Ro Khanna (CA-17),³⁷ Representative Doug LaMalfa (CA-1),³⁸ Representative Sheila Jackson Lee (TX-18), Representative Andy Levin (MI-9),³⁹ Representative Donald Norcross (NJ-1), Representative Ilhan Omar (MN-5),⁴⁰ Representative Mary Gay Scanlon (PA-5), Representative Brad Sherman (CA-30),⁴¹ Representative Eric Swalwell (CA-15),⁴² and Representative David Trone (MD-6).⁴³ However, little has been said about the systematic increase in abuse, censorship, and disinformation the Sikh community is facing online as a result of these protests.

Of particular note for this Committee is how the response of the Indian government, oftentimes in collaboration with social media companies and their respective platforms, has served to censor the movement. While freezing the assets of non-governmental organizations like Amnesty International in order to prevent them from operating in the nation after publicly denouncing the human rights violations in India,⁴⁴ the Indian government has also enforced internet blockages at and around the sites of protests.⁴⁵

³³ "United States Senate Writes Letter in Support of Indian Farmer Protests." *Daily Sikh Updates*, 12 Dec. 2020, dailysikhupdates.com/united-states-senate-writes-letter-in-support-of-indian-farmer-protests/.

³⁴ Costa, Rep. Jim. "The Unfolding Events in India Are Troubling. As a Member of the Foreign Affairs Committee, I Am Closely Monitoring the Situation. The Right to Peaceful Protest Must Always Be Respected. #FarmersProtest." *Twitter*, Twitter, 2 Feb. 2021, twitter.com/RepJimCosta/status/1356737481857785858.

³⁵ Harder, Rep. Josh. "Indian Farmers Should Be Able to Express Their Frustrations about the New Laws Rolled out by Prime Minister Modi. I Stand with Indians and Indian Americans in the Valley in Support of Peaceful Protest and the Right to Petition Their Government." *Twitter*, Twitter, 25 Jan. 2021, twitter.com/repjoshharder/status/1353848427239628802.

³⁶ "Rep. Garamendi, American Sikh Caucus Co-Chair, Stands up for Indian Farmers Met with Violent Backlash During Peaceful Protests." *Congressman John Garamendi*, 11 Dec. 2020, garamendi.house.gov/media/press-releases/rep-garamendi-american-sikh-caucus-co-chair-stands-indian-farmers-met-violent.

³⁷ Khanna, Rep. Ro. "India & the US Share a Rich Tradition of Democracy & Peaceful Protests. Farmworkers Are the Backbone of Both Our Nations & Must Have Their Voices Heard. I Hope There's a Peaceful and Fair Solution so They Can Provide for Their Families. I Am Encouraged by the Ongoing Dialogue." *Twitter*, Twitter, 13 Dec. 2020, twitter.com/RepRoKhanna/status/1337918194036535297.

³⁸ LaMalfa, Rep. Doug. "I Stand in Solidarity with the Punjabi Farmers in India Protesting for Their Livelihoods and Protection from Misguided, Manipulative Government Regulations. Punjabi Farmers Must Be Allowed to Protest Peacefully against Their Government without Fear of Violence #IStandWithFarmers." *Twitter*, Twitter, 7 Dec. 2020, twitter.com/replalamalfa/status/1336083214335684612.

³⁹ Levin, Rep. Andy. "Last Week, I Called on the Indian Government to Respect the Vital Right to Peaceful Protest and to Engage in Good-Faith Talks to Ensure Farmers' Livelihoods Are Preserved. Read My Full Statement in the Congressional Record: [Https://T.co/1IxazwvCT3](https://T.co/1IxazwvCT3)." *Twitter*, Twitter, 30 Dec. 2020, twitter.com/repandy Levin/status/1344314306385620993.

⁴⁰ Omar, Rep. Ilhan. "Solidarity with All the Farmers across India Protesting for Their Livelihood. India Must Protect Their Basic Democratic Rights, Allow for the Free Flow of Information, Reinstate Internet Access, and Release All the Journalists Detained for Covering the Protests. [Https://T.co/uOvvNklu5n](https://T.co/uOvvNklu5n)." *Twitter*, Twitter, 3 Feb. 2021, twitter.com/IlhanMN/status/1357088420443602944.

⁴¹ Sherman, Rep. Brad. "I Urge the Indian Government to Make Sure That the Norms of Democracy Are Maintained. That Protesters Are Allowed to Protest Peaceably and to Have Access to the Internet, and to Journalists. All Friends of India Hope That the Parties Can Reach an Agreement. (2/2)." *Twitter*, Twitter, 5 Feb. 2021, twitter.com/BradSherman/status/1357827849655357445.

⁴² Swalwell, Rep. Eric. "The USA and India Were Built by Small Farmers, Diversity, and Democracy. We Cannot Stray from Our Shared Values. India Must Commit to Peace, Negotiate with Small Farmers, Restore Internet Access, and Reject Discrimination." *Twitter*, Twitter, 5 Feb. 2021, twitter.com/RepSwalwell/status/13577913818608463.

⁴³ "Trone Statement on Indian Farmer Protests." *Representative David Trone*, 22 Dec. 2020, trone.house.gov/media/press-releases/trone-statement-indian-farmer-protests.

⁴⁴ Zargar, Arshad R. "India Freezes Amnesty International Bank Accounts after Reports Critical of Government." *CBS News*, CBS Interactive, 30 Sept. 2020, www.cbsnews.com/news/india-amnesty-international-bank-accounts-after-reports-critical-of-government-new-ngo-funding-law/.

⁴⁵ Hollingsworth, Julia, and Esha Mitra. "India Cuts Internet around New Delhi as Protesting Farmers Clash with Police." *CNN*, Cable News Network, 3 Feb. 2021, www.cnn.com/2021/02/01/asia/india-internet-cut-farmers-intl-hnk/index.html.

Statement of SALDEF
March 25, 2021

More aggressively, the Indian government pressured Twitter to remove over 500 accounts⁴⁶—many of which were based in the United States—and more than 150 tweets⁴⁷ related to Sikhism and the Farmers' Protests—a significant portion of which were also blocked in the United States. Of the accounts successfully removed was @WorldSikhOrg, an account based outside of India. After being temporarily suspended from Twitter, they posted the letter they received from Twitter Legal, which outlined that the request to remove their account had come directly from Indian law enforcement.⁴⁸ Other accounts suspended include the Caravan, an unbiased news journal with a significant following in the United States; Kisan Ekta Morcha, one of the biggest accounts used to organize peaceful protests for farmers across the world; and activist, Hansraj Meena.⁴⁹ SALDEF also conducted its own qualitative study after the first round of Sikh censorship during the Farmers' Protests and found that the accounts temporarily or permanently blocked were largely accounts outside of India based in the US, UK, and Canada. They include (but are not limited to) @SherePunjabUK (Twitter), @DalKhalsaUK (Twitter), @22Sxng (Twitter), @FreeJaggiNow (Instagram), @everythings_13 (Twitter), @savingpunjab (Instagram), and @Dawinderpal (Facebook).

Facebook and Twitter are not alone in their coordination with the Indian government. In February, YouTube removed several songs by mainstream Punjabi artists at the request of the Indian government.⁵⁰ These songs, whose lyrics demonstrated support for the Farmers' Protests, have since been unable to be viewed within India. Now, the Indian government is threatening to jail Facebook, WhatsApp, Twitter, and other platform employees who do not comply with their demands to censor content about the Farmers' Protests.⁵¹

Most appalling, however, is how the Indian government receives direct assistance from big-tech companies to target activists. Companies like Facebook and Google have directly cooperated with the Indian government to provide whatever private information is requested to detain activists who are not explicitly violating the law. For example, Disha Ravi, a climate change activist and supporter of the Farmers' Protests, was tracked down based on her accessing and editing a Google doc.⁵² Ravi spent 10 days in jail on claims enhanced by data collected by social media companies that were later ruled to have no legitimate basis whatsoever by an Indian Judge.⁵³ These actions by Google and Facebook come in stark contrast to other tech

⁴⁶ Singh, Karan Deep. "Twitter Blocks Accounts in India as Modi Pressures Social Media." *The New York Times*, The New York Times, 10 Feb. 2021, www.nytimes.com/2021/02/10/technology/india-twitter.html.

⁴⁷ "Most Accounts Withheld by Twitter on IT Ministry Directions Now Restored." *The Indian Express*, 1 Feb. 2021, indianexpress.com/article/india/twitter-withholds-multiple-accounts-following-direction-from-it-ministry-7170134/.

⁴⁸ Garcha, Neetu. "Online Censorship Claims Shadow Indian Farmer Solidarity Protests." *Global News*, Global News, 19 Dec. 2020, globalnews.ca/news/7532961/online-censorship-claims-shadow-indian-farmer-solidarity-protests/.

⁴⁹ "Farmers Protest: Twitter Restores Blocked Indian Accounts." *BBC News*, BBC, 2 Feb. 2021, www.bbc.com/news/world-asia-india-55898708.

⁵⁰ Correspondent. "YouTube Takes down Song on Farmers' Protest Following Government Order." *The Hindu*, The Hindu, 9 Feb. 2021, www.thehindu.com/news/national/youtube-takes-down-song-on-farmers-protest-following-govt-order/article33794366.ece.

⁵¹ Horwitz, Jeff, and Newley Purnell. "WSJ News Exclusive | India Threatens Jail for Facebook, WhatsApp and Twitter Employees." *The Wall Street Journal*, Dow Jones & Company, 5 Mar. 2021, www.wsj.com/articles/india-threatens-jail-for-facebook-whatsapp-and-twitter-employees-11614964542.

⁵² Klein, Naomi. "India Targets Climate Activists With the Help of Big Tech." *The Intercept*, 27 Feb. 2021, theintercept.com/2021/02/27/india-climate-activists-twitter-google-facebook/.

⁵³ Dutt, Barkha. "Opinion | I'm an Indian Journalist. A Video Called for Me to Be Hanged for My Reporting." *The Washington Post*, WP Company, 24 Feb. 2021, www.washingtonpost.com/opinions/2021/02/24/barkha-dutt-disha-ravi-video-complaint-journalism/?fbclid=IwAR2UfkNVVDYakiPBiQDyPDvMMu5n7tvuBPkTCM-cktFJZKP-kwapT0Yjn-Q.

Statement of SALDEF
March 25, 2021

companies like Apple, for example, that have on multiple occasions refused to hand over private information to law enforcement.⁵⁴

Beyond the social media censorship of the Farmers' Movement directed by the Indian government, the algorithmic inconsistencies incorporated into these platforms seem to be biased against content by or about minority communities. For example, supporters of the Farmers' movement have been organizing around several hashtags including #KisanMajdoorEktaZindabad, #KisanEktaZindabad, #FarmersProtest, #Sikh, and #Sikhism, since Sikhs overwhelmingly occupy the agricultural sector in India. However, many of these hashtags were blocked in the United States and abroad, including #Sikh for the second and third times in 2020 alone.⁵⁵ Additionally, many popular US- and Canadian-based accounts that frequently posted using these hashtags were prevented from LiveStreaming.⁵⁶ Unfortunately, despite several attempts to gather more information from both Twitter and Facebook, little is known about what procedures were used to justify the removal, blockage, or banning of the hashtags. Similarly, no information is yet available about when these policies were implemented or who was involved in creating these policies. Additionally, since few media outlets report on these hashtag blocks, little is known about the exact number of times or for how long #Sikh and #Sikhism were taken down in 2020 and whether automated systems or humans were responsible for making these decisions.

Anti-Sikh Disinformation on Social Media

Disinformation has been at the center of this Committee and the nation's political discourse since the events of the 2020 election. However, the challenges that disinformation poses to minority communities have not received enough coverage.

Social media has been used as a vehicle for anti-Sikh disinformation and for promoting acts of hate, bias, and intimidation against minority communities. Unsurprisingly, while the hashtags that have been used to mobilize the international community around the Indian Farmers' Protests and Sikh awareness have been blocked, banned, and censored, social media platforms have remained a steadfast lightning rod for the promotion of fake news, religiously charged hate speech, doctored graphics, and general disinformation-fueled political vitriol.

Pro-government groups in India have leveraged the lack of accountability on social media platforms to coordinate attacks against religious minority groups across India. These activities are rooted in Hindu nationalism, and disturbingly mirror the sentiments of white supremacy in the United States that fueled the Capitol Riot on January 6th, 2021.

⁵⁴ Feiner, Lauren. "Apple Refuses Government's Request to Unlock Pensacola Shooting Suspect's iPhones." CNBC, CNBC, 14 Jan. 2020, www.cnbc.com/2020/01/14/apple-refuses-barr-request-to-unlock-pensacola-shooters-iphones.html.

⁵⁵ Kim, Yunkyo. "Instagram Blocks #Sikh Hashtag for the Second Time." AsAmNews, 1 Dec. 2020, asamnews.com/2020/12/01/instagram-blocked-the-sikh-hashtag-amidst-the-punjab-farmers-protest/.

⁵⁶ Tera Fufad. "Image: Blocked from Sharing Live Video." Instagram, Tera Fufad, 26 Jan. 2021, www.instagram.com/p/CKf6hb2LKIA/?igshid=16i7r9r5138yj.

Statement of SALDEF
March 25, 2021

A World Sikh Organization report⁵⁷ points out how organizations like Asian News International (ANI) have been explicitly deployed to propagate anti-Sikh narratives, spread disinformation about the faith, and position them as anti-nationals and terrorists. These organizations use social media as their platform of operation—in ANI's case, by running several fake Facebook, Twitter, and Instagram accounts to 'organically' spread their disinformation.

In focusing on the Indian Farmers Protests specifically, disinformation in the forms of fake news and manipulated content continues to circulate social media.⁵⁸ Common examples have included falsified content on Facebook and Twitter that misidentifies protestors as known extremists⁵⁹; doctored videos from past protests⁶⁰ that associate current protestors with separatist or terrorist movements⁶¹; and manipulated graphics or photos used to foment anti-Sikh sentiment⁶². All of this information propagated by vigilante groups on Facebook and WhatsApp platforms to incite violence against minorities⁶³ is then legitimized by government Twitter accounts⁶⁴.

This ecosystem of disinformation is entirely housed on social media platforms and has been allowed to fester without regulation. As we learned in January, the consequences of these 'Big Lies' are far more than hurt feelings and unproductive discourse. Last month, Twitter did not remove the #Shoot, which called for the murder of protesting farmers, when it began trending⁶⁵. These tools of stirring up violence inevitably result in violence. Specifically, this inaction led to the death of a protestor on-the-ground in New Delhi. No information has yet been released on why the same procedures to block benign Sikh hashtags were not utilized to block #Shoot when it was explicitly attempting to incite violence against vulnerable protestors.

The Increasing Threat to the Sikh Community Online

On February 25, 2021, the Indian government implemented secondary legislation that dramatically increased its oversight of social media platforms. What is especially dangerous to individuals outside of India is the burden of high liability and quick turnaround time placed on social media platforms to present requested information on its users, particularly those who post content deemed inappropriate by the Indian government. This requirement perpetuates a

⁵⁷ World Sikh Organization of Canada. *India's Disinformation Campaign Against Canada's Sikhs*. d3n8a8pro7hmx.cloudfront.net/worldsikh/pages/1608/attachments/original/1612320038/wso_india_disinfo_report2.pdf?1612320038.

⁵⁸ Dahiya, Himanshi. "We Know Why We Are Protesting": Farmers Respond to Fake News." *TheQuint*, 8 Dec. 2020, www.thequint.com/news/webqoof/farmers-at-singhu-border-respond-to-social-media-disinformation.

⁵⁹ Capron, Alexandre. "Why Are Protesting Farmers in India Being Labelled 'Violent Muslim Infiltrators'?" *The Observers - France 24*, The Observers - France 24, 28 Jan. 2021, observers.france24.com/en/asia-pacific/20210128-farmers-india-protests-fake-news-social-media.

⁶⁰ Alphonso, Anmol. "Farmers' Protests: How Old Visuals Were Used To Peddle A Pro-Khalistan Narrative." *BOOM, BOOM*, 14 Dec. 2020, www.boomlive.in/fake-news/farmers-protests-how-old-visuals-were-used-to-peddle-a-pro-khalistan-narrative-11090.

⁶¹ Pathan, Aqib. "Old Video from UK Viral as Farmers Raising pro-Pak and Khalistan Slogans during Protests." *Alt News*, 30 Nov. 2020, www.altnews.in/old-video-from-uk-viral-as-farmers-raising-pro-pak-and-khalistan-slogans-during-protests/.

⁶² Webqoof, Team. "Fake News From Anti-CAA Stir Now Being Linked to Farmers' Protest." *TheQuint*, 2 Feb. 2021, www.thequint.com/news/webqoof/fake-news-from-anti-caa-stir-is-now-targeting-farmers-agitation.

⁶³ Ali, Mohammad. "The Rise of a Hindu Vigilante in the Age of WhatsApp and Modi." *Wired*, Conde Nast, www.wired.com/story/indiass-frightening-descent-social-media-terror/.

⁶⁴ Kajal, Kapil, et al. "Protesting Farmers Counter Propaganda: Fake News with IT Cell, Newsletter." *The Federal*, 23 Dec. 2020, thefederal.com/news/protesting-farmers-counter-propaganda-fake-news-with-it-cell-newsletter/.

⁶⁵ Dixit, Pranav. "Violent Protests Erupted In India. Then Calls For Police To Shoot The Protesters Went Viral On Twitter." *BuzzFeed News*, BuzzFeed News, 27 Jan. 2021, www.buzzfeednews.com/article/pranavdixit/india-protests-viral-tweets-police-brutality.

Statement of SALDEF
March 25, 2021

culture of sharing personally identifiable information under the specter of legal threat that critics argue will have significant consequences on free expression for those outside of India.⁶⁶

This threat, however, is doubled for those in the United States who identify with the broader Indian diasporic community: not only will the sharing of information potentially impact their own ability to travel to and from India or place them under the threat of being doxxed, but the lives and safety of their family members in India will also be at great risk by a government that has had a history of targeting activists, political dissenters, and minorities.

Compliance with this legislation demonstrates yet another instance of social media companies prioritizing their business interests over consumer protection. It is imperative that Congress hold these platforms accountable to the safety of their users. In particular, the IT Rules of 2021 put forth a series of problematic measures that include appointing a Chief Compliance Officer (CCO) who is legally responsible for its employer's actions. In other words, if Facebook, Twitter, or Google does not present the Indian government the requested user information in 36 hours, the CCO will face legal punishment.⁶⁷

The CCO is also responsible for ensuring that its employer's platform resolves broader content grievances flagged by the Indian government within 15 days. However, given the sheer amount of content regularly published on these platforms, this places an incredibly onerous burden on social media companies, calling into question whether these platforms will be able to accurately determine if content is worthy of being removed.⁶⁸ This policy is contributing to what some critics are calling a slippery slope: since social media companies and its respective employees do not have enough time to critically examine whether certain flagged content is verifiably problematic, this requirement may lead to otherwise benign content getting censored both in India and abroad. The aforementioned issue is further compounded by the fact that this legislation does not have a mechanism to prevent the lodging of frivolous and baseless grievances.⁶⁹

Equally concerning is their first originator clause that demands platforms to provide the Indian government with the information of the original poster for any flagged content that is deemed problematic by the Indian government. In order to obtain this information, platforms like WhatsApp would be required to break down its end-to-end encryption that has historically served to protect its users.⁷⁰ Of grave importance to Congress is the substantial threat this requirement poses to American users' privacy and safety: given the quick turnaround time legislated by the 2021 IT Rules, it is very plausible that social media platforms may overshare

⁶⁶ Seah, Jessica. "'Future Police State': What India's New Internet Rules Mean for Twitter, Facebook." *Law.com International*, 17 Mar. 2021, www.law.com/international-edition/2021/03/17/future-police-state-what-indias-new-internet-rules-mean-for-twitter-and-facebook/.

⁶⁷ Makkar, Angad. "INFORMATION TECHNOLOGY RULES 2021- USHERING IN A STRICT REGIME OF INTERNET CENSORSHIP FOR INTERMEDIARIES AND DIGITAL MEDIA." *IPRMENTLAW*, 7 Mar. 2021, iprmentlaw.com/2021/03/07/information-technology-rules-2021-ushering-in-a-strict-regime-of-internet-censorship-for-intermediaries-and-digital-media/.

⁶⁸ Ibid.

⁶⁹ Ibid.

⁷⁰ Pahwa, Nikhil. "View: New IT Rules Are an Overreach, Will Impact Our Freedoms." *The Economic Times*, Economic Times, 14 Mar. 2021, economictimes.indiatimes.com/news/politics-and-nation/view-new-it-rules-are-an-overreach-will-impact-our-freedoms/articleshow/81491676.cms?from=mdr.

Statement of SALDEF
March 25, 2021

first originator information, which could ultimately be used against the originator or their family members within the borders of India.

With the Indian ministry gaining full authority to block any content it deems offensive, it has gained with it the excessive power to control the narrative of online content.⁷¹ Whenever freedom of speech, protest, and assembly are taken from the people—and placed in the hands of social media companies themselves or their government allies—the very foundation of democracy is threatened. Especially in today's globalized world, the 2021 IT Rules threaten the ability of those even outside the borders of India. For this reason, it is even more critical that we hold social media companies accountable to our democratic values, as well as the safety and security of its users across marginalized communities.

Recommendations

In light of the systematic increase in censorship of and disinformation against the Sikh community, SALDEF joins other marginalized groups in calling for the immediate implementation of accountability standards for US social media platforms. Congress should mandate oversight measures to monitor the condition of discourse on social media platforms, with a specific eye towards their impact on minority communities. Specifically, such measures should ensure that benign content is neither flagged nor banned simply due to a lack of cultural accountability in algorithmic standards. Instead, we ask for an explicit commitment from these organizations to roll out new content moderation standards that prevent violence against marginalized groups while protecting the safety of users' rights to speech and congregation. A prerequisite for such standards should be prioritizing working with community-based organizations to ensure they have access to the appropriate datasets and algorithmic inputs that would allow for efficient monitoring of discourse across their platforms.

At the same time, it is imperative that these companies implement stronger systems to remove objectionable rhetoric from its platforms whose sole purpose is to spam online spaces for minority community-based organizing. Oftentimes, this spamming takes place in the form of user-generated, mass-file reports against benign content, resulting in their removal. With this in mind, SALDEF urges Facebook, Google, and Twitter to implement more rigorous moderation systems to prevent the misuse of its digital compliance infrastructure. Simultaneously, these platforms should work with minority communities to ensure they have a proper path of recourse to revive their appropriate content.

Additionally, SALDEF calls for transparency in both the decision-making behind and implementation of its content moderation standards and policies. As outlined throughout this document, Sikh Americans are especially concerned with how the standards mandated by foreign governments have and will continue to impact their ability to communicate, organize, and post online. In particular, it has become clear that the censorship of content in India has biased algorithmic content to automatically censor the same content in other regions of the world, including the United States. Moving forward, we hope that Congress will urge these

⁷¹ Ibid (Pahwa).

Statement of SALDEF
March 25, 2021

platforms to share their plans to prevent the 'spillover' of content moderation outside of the borders of specific countries and into the United States. Moreover, SALDEF joins other community organizations in calling for Facebook, Google, and Twitter to specifically outline how they will ensure those in power are not favored at the expense of minority communities.

SALDEF also joins the Asian American and Pacific Islander community in calling for increased institutionalized civil rights protections in American telecommunications monitoring. Section 230's current formulation has allowed for unchecked moderation power on the parts of social media platforms with little demonstrated interest in American civil liberties. Additionally, the FCC has no codified civil rights working group to monitor ongoing potential concerns. We call on Congress to pass legislation that ensures these regulatory gaps are filled.

Conclusion

SALDEF thanks the Subcommittee on Consumer Protection and Commerce and the Subcommittee on Communication and Technology for bringing awareness to the perpetuation of disinformation on social media platforms, especially as it relates to on-the-ground, real-life harm against individuals. We urge members of these Subcommittees to bear in mind the disproportionate amount of violence faced by minority communities due to these very issues, including the Sikh American community. With the facts presented during Thursday's hearing and submitted through this testimony, we hope that you will hold Facebook, Twitter, and Google accountable to culturally-competent policies; call for greater transparency in their decision-making; and implement the necessary systems to take into account greater community feedback and improve algorithmic standards.

Respectfully submitted,
Kiran Kaur Gill
Executive Director | SALDEF

March 24, 2021

Dear Chairman Pallone, Chairwoman Schakowsky, and Members of the House Energy and Commerce Committee,

We are writing to you, exasperated by the inaction or lack of sufficient action by social media platforms, in stopping the spread of disinformation and hate on their platforms. We are writing to you as direct survivors of the hate, lies and incitement to violence that have been allowed to reach millions of people online, and gravely harm many lives offline, including ours and those of our families, patients and communities. The decisions and choices that Mark Zuckerberg, Jack Dorsey, and Sundar Pichai have made or approved in building Facebook, Twitter and YouTube, respectively, have allowed bad actors to weaponize social media platforms, spread misinformation, and cause harm to our nation's democracy, to each of us, our families, and communities, and to millions of people across the country and around the world.

Ultimately, we write to you because **you, as our elected officials, have the power and responsibility to fix this.** For far too long, tech companies have been allowed to make decisions about their platforms guided primarily by their business models. As your constituents, we ask that you rein in their power by adopting smart tech regulation that places human lives first and holds tech companies responsible and accountable for their decisions.

We bring you our stories, and urge you to listen to the pain, death, and disease these platforms have directly contributed to.

- **We are doctors in Pennsylvania and New York who are struggling to counter the spread of disinformation about Covid-19 on Facebook, Instagram, YouTube and Twitter.** We constantly hear from patients and co-workers who cite social media posts claiming that masks don't work in preventing the spread of Covid-19, that we health care workers are lying about the pandemic, that the vaccines are dangerous and ineffective - and unfortunately so much more. Misinformation about science and health has resulted in many deaths and will continue to cause pain and suffering if your platforms do not actively and persistently crackdown on this harmful content.
- **We are parents of autistic children in North Carolina and Florida who spend hours countering dangerous misinformation about miracle cures for autism on Facebook and Instagram.** Hundreds and thousands of children are being subjected to charlatans who spread misinformation through Facebook groups. These individuals claim that giving autistic children bleach, turpentine, Chelation, and other harmful and deadly chemicals will cure them of their autism. We have repeatedly reported this dangerous content to Facebook content moderators to no avail, Facebook's algorithms continue to show disinformation about autism to users, Facebook's ad policy preventing targeting based on disability remains unenforced, and in at least one case we've documented, Facebook has taken ad money for an event explicitly spreading autism misinformation.
- **My daughter was killed in the Parkland school shooting and my family in Florida was aggressively stalked and harassed by an Instagram user.** Even though the individual is now serving a multi-year prison sentence and was deemed to present a credible threat to me and my family, Instagram refused to cooperate with law enforcement officials until they secured a search warrant. The individual destroyed my wife and my son emotionally for the better part of several weeks.
- **My daughter was killed in Virginia on live television and Facebook, Google and YouTube have failed to remove footage of her murder from their platforms.** The recording of my daughter's murder continues to proliferate online and I have spent 5 years working to get this footage removed. YouTube and Facebook continue to profit from my daughter's murder.
- **I ran for local office in Alabama and those who wanted me to lose used Facebook groups to spread lies and disinformation about me and my family.** Facebook empowered my political opponents to establish local group pages that spread misinformation about my views and painted me as an angry Black woman seeking to divide our small town. People I've known my entire life stopped talking to me. What happened here is just a microcosm of what's happening all across our country. January 6th was a sad day, but it's been happening all over the nation.

- **I'm the pastor of a Black church in Washington D.C. that was defaced by extremists who organized on Facebook and other social media platforms.** The Proud Boys used Facebook, Instagram, and other social media platforms to organize and build power, eventually destroying a Black Lives Matter sign from a Black church in an effort to intimidate our congregants. It was an act of political violence by people who were mobilized and rallied others using technology platforms. This isn't about free speech. This is about human lives being protected, about people being able to live in this nation freely.
- **My partner was killed in Kenosha, Wisconsin by an armed teenager who associated with the Proud Boys.** The Kenosha Guard event page on Facebook that served as a call to arms globally, and incited the civilian militia in Kenosha to show up at a peaceful protest in the wake of Jacob Blake's shooting was flagged 455 times by Facebook users but was not taken down.
- **I lost my father to baseless Qanon conspiracy theories on YouTube.** When Covid hit, he believed the videos more than his own child. As of writing this, it's been a month since he's said a word to me. Though I've lived at home as his caregiver for years, I don't recognize the person in dad's chair.

Social media may have been created to connect people and make our worlds bigger. But as our stories indicate, the world is now more hate-filled and divided as a result of business decisions these tech companies have made. In the same way that a company that pollutes our air and water must be held accountable for its actions, these social media platforms must be held accountable for creating products designed to pollute our society and our communities with dangerous misinformation.

And we are not alone. Indeed, a movement of survivors of tech harm is growing, and a national chorus of voices coming together with a unified message to Congress: Stop letting big tech off the hook. Protect your constituents. Regulate tech platforms now.

We would welcome the opportunity to meet with you and to more fully share our experiences of being harmed by social media platforms.

Sincerely,

Meenakshi Bewtra, MD, MPH
 Melissa Eaton
 Fred Guttenberg
 Hannah Gittings
 Joyce Jones
 Rev. William H. Lamar IV
 Duncan Maru, MD, PHD
 Andy Parker
 Amanda Siegler

Congress of the United States
Washington, DC 20515

January 21, 2021

Mr. Sundar Pichai, CEO
 Google, LLC
 Alphabet, Inc.
 1600 Amphitheatre Parkway
 Mountain View, California 94043

Ms. Susan Wojcicki, CEO
 YouTube Inc.
 901 Cherry Avenue
 San Bruno, California 94066

Dear Mr. Pichai and Ms. Wojcicki,

On Wednesday, January 6th the United States Capitol was attacked by a violent, insurrectionist mob radicalized in part in a digital echo chamber that your company designed, built, and maintained. YouTube is among the online services most responsible for spreading fringe conspiracy theories at scale and for radicalizing some of its users to commit real-world, physical violence.

We recognize the steps YouTube has taken in recent months to limit, though not eliminate, videos perpetuating dangerous conspiracy theories, including those related to QAnon.¹ But content moderation on a service with more than *five-hundred hours* of video uploaded *every minute*² is a whack-a-mole answer to a systemic problem, one that is rooted in the very design of YouTube.

The fundamental problem is that YouTube, like other social media platforms, sorts, presents, and recommends information to users by feeding them the content most likely to reinforce their existing political biases, especially those rooted in anger, anxiety, and fear. The algorithms YouTube uses to maximize user engagement on its platform undermine our shared sense of objective reality, intensify fringe political beliefs, facilitate connections between extremist users, and, tragically, lead some of them to commit real-world, physical violence, such as what we experienced firsthand on January 6th.

YouTube's Chief Product Officer has stated that more than 70% of viewing time on the platform is attributable to recommendations.³ After the company announced that users were watching more than one billion hours of videos per day, the same executive said, "[t]he corpus of content continues to get richer and richer by the minute, and machine-learning algorithms do a better and better job of surfacing the content that an individual

¹ Elias, Jennifer, "YouTube Tightens Rules on Conspiracy Videos, but Stops Short of Banning QAnon." *CNBC*. October 15, 2020. <https://www.cnbc.com/2020/10/15/youtube-tightens-rules-on-conspiracy-videos-but-no-qanon-ban.html>.

² YouTube Official Blog. "YouTube for Press." <https://blog.youtube/press>

³ Solsman, Joan E., "YouTube's AI is the Puppet Master Over Most of what you Watch." *CNET*. January 10, 2018. <https://www.cnet.com/news/youtube-ces-2018-neal-mohan/>.

user likes.”⁴ These systems include a feature enabled by default that auto-plays videos one after another until the user exits or clicks to another video. This system, which was clearly designed to maximize the amount of time users spend on YouTube, also has the effect of trapping some in increasingly extremist echo chambers, a phenomenon which tragically leads some to commit the sort of violence we experienced at the Capitol on January 6th. Last year, the *New York Times* launched an entire podcast series about radicalization on YouTube, appropriately titled “Rabbit Hole.”

While YouTube has taken steps to reduce recommendations of conspiracy-related videos, leading researchers studying the problem have found that, “the overall volume of conspiratorial content recommended from informational channels remains relatively high.”⁵ Just after the attack on the Capitol, employees of YouTube and parent company Alphabet stated that YouTube continues to demonstrate a “policy of selective and insufficient enforcement of its guidelines against the use of the platform to spread hatred and extremism.”⁶

We believe YouTube should immediately make additional permanent changes to its recommendation systems, including disabling auto-play by default and ceasing all recommendations of conspiratorial material on users’ homepages and alongside videos. If those are too difficult to identify using automated processes, the company should cease all recommendations until an effective, technical solution is developed. More broadly, it is our hope that YouTube will begin a fundamental reexamination of maximizing user engagement as the basis for algorithmic sorting and recommendation.

Sincerely,



Tom Malinowski
Member of Congress



Anna G. Eshoo
Member of Congress

⁴ Nicas, Jack, “YouTube Tops 1 Billion Hours of Video a Day, on Pace to Eclipse TV.” *The Wall Street Journal*. February 27, 2017. <https://www.wsj.com/articles/youtube-tops-1-billion-hours-of-video-a-day-on-pace-to-eclipse-tv-1488220851>

⁵ Faddoul, Marc; Guillaume Chaslot; Hany Farid, “A Longitudinal Analysis of YouTube’s Promotion of Conspiracy Videos.” *ArXiv:2003.03318 [Cs]*. March 6, 2020. <http://arxiv.org/abs/2003.03318>.

⁶ Alphabet Workers Union (@AlphabetWorkers), Tweet, January 7, 2021, 6:57pm, <https://twitter.com/AlphabetWorkers/status/1347331587315171330>.

Barbara Lee
Member of Congress

David Trone
Member of Congress

Doris Matsui
Member of Congress

Peter Welch
Member of Congress

Rashida Tlaib
Member of Congress

Kaiali‘i Kahele
Member of Congress

Bonnie Watson Coleman
Member of Congress

Mark DeSaulnier
Member of Congress

Donald S. Beyer Jr.
Member of Congress

Veronica Escobar
Member of Congress

Mike Levin
Member of Congress

Ritchie Torres
Member of Congress

Haley M. Stevens
Member of Congress

Nydia M. Velázquez
Member of Congress

Yvette D. Clarke
Member of Congress

Sara Jacobs
Member of Congress

Jared Huffman
Member of Congress

Mary Gay Scanlon
Member of Congress

Debbie Wasserman Schultz
Member of Congress

Katie Porter
Member of Congress

André Carson
Member of Congress

Jerry McNerney
Member of Congress

David N. Cicilline
Member of Congress

Kathleen M. Rice
Member of Congress

Lori Trahan
Member of Congress

Grace Meng
Member of Congress

Bill Foster
Member of Congress

Kim Schrier, M.D.
Member of Congress

Sylvia R. Garcia
Member of Congress

Debbie Dingell
Member of Congress

Alcee L. Hastings
Member of Congress

Jahana Hayes
Member of Congress

Congress of the United States
Washington, DC 20515

January 21, 2021

Mr. Mark Zuckerberg, Chairman and CEO
 Facebook, Inc.
 1 Hacker Way
 Menlo Park, California 94025

Dear Mr. Zuckerberg,

On Wednesday, January 6th the United States Capitol was attacked by a violent, insurrectionist mob radicalized in part in a digital echo chamber that your company designed, built, and maintained. Perhaps no single entity is more responsible for the spread of dangerous conspiracy theories at scale or for inflaming anti-government grievance than the one that you started and that you oversee today as Chairman and Chief Executive Officer.

We recognize the recent steps Facebook has taken to crack down on harmful accounts such as those related to QAnon, by removing specific posts that incite violence and banning specific users. But content moderation on a service with more than 2.7 billion monthly users is a whack-a-mole answer to a systemic problem, one that is rooted in the very design of Facebook.

The fundamental problem is that Facebook, like other social media platforms, sorts and presents information to users by feeding them the content most likely to reinforce their existing political biases, especially those rooted in anger, anxiety, and fear. The algorithms Facebook uses to maximize user engagement on its platform undermine our shared sense of objective reality, intensify fringe political beliefs, facilitate connections between extremist users, and, tragically, lead some of them to commit real-world physical violence, such as what we experienced firsthand on January 6th.

Facebook has known about the dangers of its algorithmic recommendation engine for years. An internal company presentation from 2018 found that “64% of all extremist group joins are due to our recommendation tools... [o]ur recommendation systems grow the problem.”¹ The presentation further noted that “[o]ur algorithms exploit the human brain’s attraction to divisiveness.”² Facebook executives reportedly blocked efforts at the time to address the issues raised in the presentation.³ We are left to wonder, sadly, whether we would be in a different place today if these warnings had been fully heeded.

¹ Horwitz, Jeff and Deepa Seetharaman, “Facebook Executives Shut Down Efforts to Make the Site Less Divisive.” *The Wall Street Journal*. May 26, 2020. <https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499>.

² *Id.*

³ *Id.*

Facebook has shown that it is capable of dampening the harmful effects of its product, when it wants to. For example, last year, Facebook briefly tested a new machine-learning algorithm that demoted posts its users would deem “bad for the world.”⁴ It scrapped the algorithm, when it became clear that it meant users were spending less time on the site.⁵ (The company instead approved a less effective algorithm that didn’t reduce time spent among users.⁶) Further, before the 2020 elections, Facebook stopped recommending that users join political and social issue groups, a tacit acknowledgement that its recommendation system can be harmful.⁷ Again, this change was temporary. Finally, ahead of the U.S. Senate elections in Georgia, Facebook turned off a safeguard it had in place to limit the spread of election-related misinformation. Not surprisingly, the result was a spike in partisan political content and a decline in authoritative news sources in users’ newsfeeds.⁸

It is our hope that Facebook will immediately make permanent and universal these and other changes to its recommendation system which have been implemented temporarily or on a trial basis in the past, and that you begin a fundamental reexamination of maximizing user engagement as the basis for algorithmic sorting and recommendation.

Sincerely,



Tom Malinowski
Member of Congress



Anna G. Eshoo
Member of Congress

⁴ Roose, Kevin; Isaac, Mike; Frenkel, Sheera, “Facebook Struggles to Balance Civility and Growth.” *The New York Times*. November 24, 2020. <https://www.nytimes.com/2020/11/24/technology/facebook-election-misinformation.html>

⁵ *Id.*

⁶ *Id.*

⁷ Mac, Ryan and Craig Silverman, “Facebook Quietly Suspended Political Group Recommendations Ahead of the US Presidential Election.” *Buzzfeed News*. October 30, 2020. <https://www.buzzfeednews.com/article/ryanmac/facebook-suspended-group-recommendations-election>

⁸ Faife, Corin, “In Georgia, Facebook’s Changes Brought Back a Partisan News Feed.” *The Markup*. January 5, 2021. <https://themarkup.org/citizen-browser/2021/01/05/in-georgia-facebooks-changes-brought-back-a-partisan-news-feed>

Jackie Speier
Member of Congress

Yvette D. Clarke
Member of Congress

Doris Matsui
Member of Congress

Alcee L. Hastings
Member of Congress

Nydia M. Velázquez
Member of Congress

Veronica Escobar
Member of Congress

Jahana Hayes
Member of Congress

Peter Welch
Member of Congress

Mary Gay Scanlon
Member of Congress

Donald S. Beyer Jr.
Member of Congress

Mikie Sherrill
Member of Congress

Mark DeSaulnier
Member of Congress

Barbara Lee
Member of Congress

Debbie Dingell
Member of Congress

Sean Casten
Member of Congress

Cindy Axne
Member of Congress

Sylvia R. Garcia
Member of Congress

Grace Meng
Member of Congress

Kim Schrier, M.D.
Member of Congress

Kathleen M. Rice
Member of Congress

Lori Trahan
Member of Congress

Albio Sires
Member of Congress

Katie Porter
Member of Congress

Bill Foster
Member of Congress

Rashida Tlaib
Member of Congress

Debbie Wasserman Schultz
Member of Congress

Mike Levin
Member of Congress

Sara Jacobs
Member of Congress

David Trone
Member of Congress

Kaiali'i Kahele
Member of Congress

Haley M. Stevens
Member of Congress

Abigail D. Spanberger
Member of Congress

Jerry McNerney
Member of Congress

Jared Huffman
Member of Congress

Bonnie Watson Coleman
Member of Congress

Ritchie Torres
Member of Congress

André Carson
Member of Congress

David N. Cicilline
Member of Congress

Congress of the United States
Washington, DC 20515

January 21, 2021

Mr. Jack Dorsey, CEO and Founder
Twitter, Inc.
1355 Market Street, Suite 900
San Francisco, California 94103

Dear Mr. Dorsey,

On Wednesday, January 6th the United States Capitol was attacked by a violent, insurrectionist mob radicalized in part in a digital echo chamber that your company designed, built, and maintained. Twitter is among the online services most responsible for spreading fringe conspiracy theories at scale and for radicalizing some of its users to commit real-world, physical violence.

Following the attack on the Capitol, Twitter took action to remove more than 70,000 accounts associated with the dangerous QAnon movement.¹ While we welcome this move, it came six months after Twitter first announced its crackdown on QAnon, which suggests a failure to meaningfully enforce the policy after it was enacted, and after *years* of allowing QAnon and other harmful, conspiratorial content to flourish on the site. Content moderation on a service that hosts hundreds of millions of tweets per day is a whack-a-mole answer to a systemic problem, one that is rooted in the very design of Twitter.

The fundamental problem is that Twitter, like other social media platforms, sorts, presents, and spreads information to users by feeding them the content most likely to reinforce their existing political biases, especially those rooted in anger, anxiety, and fear. The algorithms Twitter uses to maximize user engagement on its platform undermine our shared sense of objective reality, intensify fringe political beliefs, facilitate connections between extremist users, and, tragically, lead some of them to commit real-world physical violence, such as what we experienced firsthand on January 6th.

Extreme, inflammatory tweets that trigger emotions like anger and fear often result in high levels of engagement on the platform, and Twitter's algorithm too often amplifies white supremacist, anti-Semitic, and other conspiracy-oriented material that can lead people to commit offline violence. Even if tweets fail to achieve mass scale virality, users can still become trapped in silos that intensify fringe views. Removing QAnon is not enough. Twitter must rethink and reengineer the fundamental architecture of its service which continues to allow for the frictionless spread of misinformation and radicalization at scale.

¹ Conger, Kate, "Twitter, in Widening Crackdown, Removes Over 70,000 QAnon Accounts." *The New York Times*, January 11, 2021, <https://www.nytimes.com/2021/01/11/technology/twitter-removes-70000-qanon-accounts.html>.

Leading up to the November 2020 elections, Twitter made a number of product changes designed to stem the spread of misinformation, including prompting users to quote tweets rather than simply retweet, removing recommendations in users' timelines and notifications, and adding context to "Trends" in the "For You" part of its platform. Prompting quote tweets over retweets reduced overall retweets and quote tweets by 20%, which the company found "slowed the spread of misleading information by virtue of an overall reduction in the amount of sharing on the service."² This change was reversed following the election.

Experts have rightly suggested that the platform needs to make permanent, fundamental design changes to limit the spread of harmful content, such as halting recommendations, limiting shares, and adding a circuit breaker-like function to slow the spread of the most viral and potentially dangerous content.³ One independent disinformation expert bluntly stated, "Twitter doesn't yet seem to understand it's a platform optimized for radicalization."⁴ It is our hope that Twitter will immediately make permanent changes to limit the spread of misinformation and other forms of harmful content, and that the company will begin a fundamental reexamination of maximizing user engagement as the basis for algorithmic sorting and recommendation.

Sincerely,



Tom Malinowski
Member of Congress



Anna G. Eshoo
Member of Congress

² Gadde, Vijaya and Kayvon Beykpour, "An Update on Our Work around the 2020 US Elections." *Twitter* (blog), accessed January 15, 2021. https://blog.twitter.com/en_us/topics/company/2020/2020-election-update.html.

³ Kornbluh, Karen and Ellen P. Goodman, "Three Steps to Help Treat America's Debilitating Information Disorder." *The Washington Post*. January 13, 2021, sec. Opinion, <https://www.washingtonpost.com/opinions/2021/01/13/three-steps-help-treat-americas-debilitating-information-disorder/>.

⁴ Troy, Dave, "A Warning About Twitter and Radicalization." *Medium*. July 11, 2020. <https://davetroy.medium.com/a-warning-about-twitter-and-radicalization-831b724612ba>.

Barbara Lee
Member of Congress

David Trone
Member of Congress

Doris Matsui
Member of Congress

Peter Welch
Member of Congress

Rashida Tlaib
Member of Congress

Kaiali‘i Kahele
Member of Congress

Bonnie Watson Coleman
Member of Congress

Mark DeSaulnier
Member of Congress

Donald S. Beyer Jr.
Member of Congress

Veronica Escobar
Member of Congress

Mike Levin
Member of Congress

Ritchie Torres
Member of Congress

Haley M. Stevens
Member of Congress

Nydia M. Velázquez
Member of Congress

Yvette D. Clarke
Member of Congress

Sara Jacobs
Member of Congress

Jared Huffman
Member of Congress

Mary Gay Scanlon
Member of Congress

Debbie Wasserman Schultz
Member of Congress

Katie Porter
Member of Congress

André Carson
Member of Congress

Jerry McNerney
Member of Congress

David N. Cicilline
Member of Congress

Kathleen M. Rice
Member of Congress

Lori Trahan
Member of Congress

Grace Meng
Member of Congress

Bill Foster
Member of Congress

Kim Schrier, M.D.
Member of Congress

Sylvia R. Garcia
Member of Congress

Debbie Dingell
Member of Congress

Alcee L. Hastings
Member of Congress

Jahana Hayes
Member of Congress

A longitudinal analysis of YouTube's promotion of conspiracy videos

Marc Faddou¹, Guillaume Chaslot³, and Hany Farid^{1,2}

Abstract

Conspiracy theories have flourished on social media, raising concerns that such content is fueling the spread of disinformation, supporting extremist ideologies, and in some cases, leading to violence. Under increased scrutiny and pressure from legislators and the public, YouTube announced efforts to change their recommendation algorithms so that the most egregious conspiracy videos are demoted and demonetized. To verify this claim, we have developed a classifier for automatically determining if a video is conspiratorial (e.g., the moon landing was faked, the pyramids of Giza were built by aliens, end of the world prophecies, etc.). We coupled this classifier with an emulation of YouTube's watch-next algorithm on more than a thousand popular informational channels to obtain a year-long picture of the videos actively promoted by YouTube. We also obtained trends of the so-called filter-bubble effect for conspiracy theories.

Keywords

Online Moderation, Disinformation, Algorithmic Transparency, Recommendation Systems

Introduction

By allowing for a wide range of opinions to coexist, social media has allowed for an open exchange of ideas. There have, however, been concerns that the recommendation engines which power these services amplify sensational content because of its tendency to generate more engagement. The algorithmic promotion of conspiracy theories by YouTube's recommendation engine, in particular, has recently been of growing concern to academics^{1–7}, legislators⁸, and the public^{9–14}. In August 2019, the FBI introduced fringe conspiracy theories as a domestic terrorist threat, due to the increasing number of violent incidents motivated by such beliefs¹⁵.

Some 70% of watched content on YouTube is recommended content¹⁶, in which YouTube algorithms promote videos based on a number of factors including optimizing for user-engagement or view-time. Because conspiracy theories generally feature novel and provoking content, they tend to yield higher than average engagement¹⁷. The recommendation algorithms are thus vulnerable to sparking a reinforcing feedback loop¹⁸ in which more conspiracy theories are recommended and consumed¹⁹.

YouTube has, however, contested this narrative with three main counter-arguments²⁰: (1) According to YouTube's Chief Product Officer Neal Mohan, "it is not the case that extreme content drives a higher version of engagement"; (2) The company claims that view-time is not the only metric accounted for by the recommendation algorithm; and (3) Recommendations are made within a spectrum of opinions, leaving users the option to engage or not with specific content.

We are skeptical that these counter-arguments are consistent with what we and others qualitatively have been seeing play out on YouTube for the past several years. In particular: (1) according to Facebook's CEO Mark Zuckerberg, extreme content does drive more engagement on

social media²¹; (2) Although view-time might not be the only metric driving the recommendation algorithms, YouTube has not fully explained what the other factors are, or their relative contributions. It is unarguable, nevertheless, that keeping users engaged remains the main driver for YouTube's advertising revenues^{22,23}; and (3) While recommendations may span a spectrum, users preferably engage with content that conforms to their existing world view²⁴.

Nonetheless, in January of 2019 YouTube announced efforts to reduce "recommendations of borderline content and content that could misinform users in harmful ways – such as videos promoting a phony miracle cure for a serious illness, claiming the earth is flat, or making blatantly false claims about historic events like 9/11"²⁵. This effort complemented a previous initiative to include direct links to Wikipedia with videos related to conspiratorial topics.²⁶ In June of 2019, YouTube announced that their efforts led to a reduction of view-time from these recommendations by over 50%²⁷. In December of 2019, YouTube updated this estimate to 70%²⁸. Our analysis aims to better understand the nature and extent of YouTube's promotion of conspiratorial content.

Materials & Methods

Recommendations

YouTube makes algorithmic recommendations in several different places. We focus on the *watch-next* algorithm, which is the system that recommends a video to be shown

¹School of Information, University of California, Berkeley

²Electrical Engineering & Computer Sciences, University of California, Berkeley

³Mozilla Foundation

Corresponding author:

Hany Farid, School of Information, UC Berkeley

Email: hfarid@berkeley.edu

next when auto-play is enabled. YouTube distinguishes between two types of recommendations: *recommended-for-you* videos are computed based on the user's previous viewing history and *recommended* are not individualized. Our requests are made with a U.S.-based IP addresses, without any identifying cookie. There are, therefore, no *recommended-for-you* videos.

Our method to emulate the recommendation engine is a two step process: we start by gathering a list of seed channels, and then generate recommendations starting from the videos posted by these channels.

The list of seed channels is obtained with a snowball method. We start with an initial list of 250 of the most subscribed English YouTube channels. The last video posted by each of these seed channels is retrieved and the next 20 watch-next recommendations are extracted. The channels associated with these recommendations are ranked by number of occurrences. The channel that has the largest number of recommendations, and is not part of the initial seed set, is added to the set of seed channels. This process is repeated until 12,000 channels are gathered.

To focus our computational resources on the parts of YouTube that are relevant to information and disinformation, we perform a cluster analysis²⁹ on these 12,000 channels. We retain a single cluster of 1103 channels which corresponds to news and information channels (e.g., BBC, CNN, FOX...). Since the unsupervised clustering is not perfect, we manually added 43 channels that we considered to be consistent with the other information channels. This yielded a final list of 1146 seed channels, then reduced to 1080 by the end of the analysis after some channels were deleted or stalled.

*

We then gathered the 20 first recommendations from the watch-next algorithm starting from the last video uploaded by each of the seed channels everyday from October 2018 to February 2020. The top 1000 most recommended videos on a given day were retained and used in our analysis. As described below, these videos were analyzed to determine which were predicted to be conspiratorial in nature.

Training Set

We collected a training set of conspiracy videos in an iterative process. An initial set of 200 videos was collected from a book referencing top conspiracy theories on YouTube³⁰, and a set of videos harvested on 4chan and on the sub-reddits r/conspiracy, r/conspiracyhub, and r/HealthConspiracy. A comparable set of 200 non-conspiratorial videos was collected by randomly scraping YouTube videos. These videos were manually curated to remove any potentially conspiratorial videos. As we began our analysis, we augmented these initial videos by adding any obviously mis-classified videos into the appropriate conspiratorial or non-conspiratorial training set, yielding a final set of 542 conspiratorial videos and 568 non-conspiratorial videos.

We are sensitive to the fact that classifying a video as conspiratorial is not always clear-cut. We endeavored to limit our training set to videos whose underlying thesis, by and large, satisfies the following criteria: (1) Explains events as secret plots by powerful forces rather than as overt

activities or accidents; (2) Holds a view of the world that goes against scientific consensus; (3) Is not backed by evidence, but instead by information that was claimed to be obtained through privileged access; (4) Is self-filing or unfalsifiable.

Text Classification

A key component of our video classifier is *fastText*, a text-based classifier³¹. This classifier takes a text sample as input, and predicts the probability that the sample belongs to a given class (e.g., a conspiratorial video).

The classifier begins by parsing the training data to define a vocabulary. Input text samples are then represented by a concatenation of a bag-of-words and bag of *n*-grams, as defined by the vocabulary. An embedding matrix projects this representation into a lower-dimensional space, after which a linear classifier is used to classify the text into one of two (or more) classes.

Video Classification

Our video classifier analyzes various text-based components of a video using individual classifier modules for each. These modules, described next, are followed by a second layer that combines their outputs to yield a final conspiracy likelihood.

1. **The transcript of the video**, also called subtitles, can be uploaded by the creator or auto-generated by YouTube, and captures the content of the video. The transcript is scored by a *fastText* classifier.
2. **The video snippet** is the concatenation of the title, the description, and the tags of the video. The snippet renders the language used by the content creator to describe their video. The snippet is also scored by a *fastText* classifier.
3. **The content of the 200 top comments** defined by YouTube's relevance metric (without replies). Each comment is individually scored by a *fastText* classifier. The score of a video is the median score of all its comments.
4. **The perceived impact of the comments**. We use Google's Perspective API³² to score each comment on the following properties: (1) toxicity; (2) spam; (3) unsubstantial; (4) threat; (5) incoherent; (6) profanity; and (7) inflammatory. This set of seven perspective scores for each comment is converted into a 35-D feature vector for the whole video by taking the median value and standard deviation of each property (14 features) as well as the median value of the pairwise products of each property (21 features). A logistic regression classifier is trained to predict the conspiracy likelihood of the video from this 35-D feature vector.

The output of these four modules is then fed into a final logistic regression layer to yield a prediction for the entire video.

The two layers of the pipeline are trained on distinct videos with a 100-fold cross validation. Specifically, our training set of 1095 videos is randomly split into a 60/40

* The list of seed channels and the training set are available at <https://github.com/youtube-dataset/conspiracy>

	Comments	Snippets	Transcripts
Positive	<i>illuminati, evil, told, research, deep, hoax, global, control, killed, believe, autism, satanic, they, aliens, info</i>	<i>conspiracy, warning, qanon, truth, hoax, prophecy, illuminati, supernatural, report, jfk, deception, ufo, evidence, energy, mystery</i>	<i>information, all, nasa, weather, nothing, footage, see, warming, evidence, know, climate, vaccines, ancient, look, aluminum</i>
Negative	<i>cute, universe, eat, future, dog, left, content, game, cool, imagine, food, better, loved, quality, pay</i>	<i>biggest, policy, big, sea, camera, sermon, party, round, november, live, hot, process, model, culture, duty</i>	<i>gonna, really, like, sea, young, side, him, black, live, early, policy, think, away, agents, thank</i>

Table 1. Most discriminating words in the training set for positive (conspiratorial) and negative labels, ranked by TFIDF.

split. The 60% is used to train the four modules of the first layer. The remaining 40% of videos are scored by these four classification modules. These scores are then standardized into four feature vectors each with a mean of zero and unit variance. The zero-mean ensures that missing attributes have a null contribution (e.g., transcripts can be unavailable), while the unit variance allows us to compare the relative importance of each attribute in the model. The final logistic regression is then trained on the 40% split to predict if a video is conspiratorial. We repeat this process with 100 different 60/40 splits. By averaging the 100 logistic regression models, we obtain the final regression coefficients. Their relative weights are 52% for the comments, 22% for the snippet, 14% for the caption and 12% for the perspective score.

Model Accuracy

To test the accuracy of our model, we manually classified 340 videos not used in the training set. These videos were randomly sampled so that their score distribution is uniform between 0 and 1. Shown in Fig. 1 is the correlation between the conspiracy likelihood of the classifier (horizontal axis) and the percentage of videos rated as conspiratorial by a human annotator (vertical axis). With small fluctuations, our predicted conspiracy likelihood accurately predicts the actual likelihood of a video being conspiratorial, for example, 70% of videos with a likelihood score of 0.7 will be conspiratorial. With a threshold at 0.5, the conspiracy classifier has a precision of 78% and a recall of 86%.

From a more qualitative perspective, Table 1 shows the words that are most statistically relevant to discriminating between conspiratorial and non-conspiratorial videos, as determined by *term frequency inverse document frequency* (TFIDF)³³. Words that identify conspiracies seem reasonably diagnostic: they are either specific to a topic (e.g., *aliens, deep - for Deep State, autism - for vaccines*), generic to conspiratorial narratives (e.g., *deception, control*) as well as, ironically, words that characterize information (e.g., *truth, know, hoax*). It is worth noting that despite being an omnipresent pronoun, the word *they* is a highly discriminating word for conspiratorial comments. This denotes the ubiquity of the narrative *they against us*. Both *all* and *nothing* in the transcript are also strong indicators for conspiracy, hinting at a lack of nuance. Words that characterize non-conspiratorial content are more random, reflecting the fact that the negative training set is mostly not cohesive.

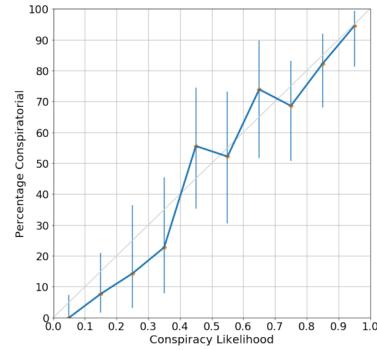


Figure 1. Percentage of videos labeled as conspiratorial by a human annotator plotted as a function of the estimated conspiracy likelihood, on a total of 340 out-of-sample videos. The error bars correspond to Clopper-Pearson 95% confidence intervals based on Beta distribution.

Results

We analysed more than 8 million recommendations from YouTube's watch-next algorithm over 15 months. Recommendations were collected daily, starting from the most recent videos posted by a set of 1000+ of the most popular news and informational channels in the U.S. The recommended videos were then fed to a binary classifier trained to detect conspiratorial content based on the video title, description, tags, transcript, and comments (see Methods). The classifier returns the likelihood that a given video is conspiratorial, a score between 0 (minimal likelihood) and 1 (maximal likelihood).

Longitudinal Trends

Shown in Fig. 2 is our estimate of the percentage of conspiratorial videos recommended by YouTube on information channels, between October 2018 and February 2020 (*Raw Frequency*). Also shown is a weighted version of this estimate which accounts for the popularity of the source video (*Weighted Frequency*).

The *Raw Frequency* is computed as the product of the number of times a video was recommended and the probability that each video is conspiratorial, Fig. 1. Only videos with a likelihood greater than 0.5 are counted, providing a conservative estimate (see Methods). The

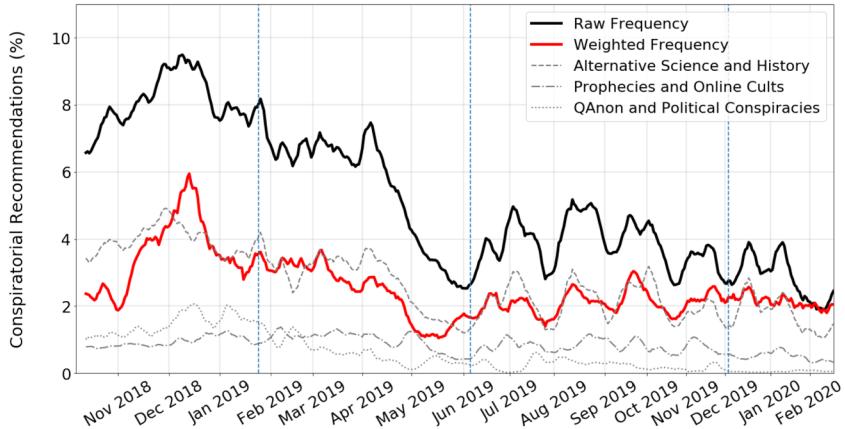


Figure 2. Longitudinal trends of conspiratorial recommendations from informational channels on YouTube, in which each data point corresponds to a rolling seven day average. The **raw frequency** is an estimate of the percentage of conspiratorial recommendations obtained by weighting all recommendations classified as conspiratorial by their likelihood. This frequency represents the propensity of the YouTube algorithm to recommend conspiratorial content. The **weighted frequency** is an estimate of the percentage of conspiratorial weighted by the number of views of the source video. The **three dashed and dotted lines** correspond to the raw frequency for the top three topics: (1) Alternative Science and History, (2) Prophecies and Online Cults, and (3) QAnon, Deepstate, and New World Order (see Table 2). The **three vertical lines** represent the three YouTube announcements related to their efforts to fight conspiratorial content, on January 25th, June 5th and Dec 3rd of 2019.

Topic	Top Words	% Rec	% Vid
Alternative Science and History	moon, aliens, flat, space, ufo, ancient, nasa, sun, alien, built, pyramids, planet, technology, mars, david, pyramid, water, history, humans, human, science, evidence, energy, sky, stone	51.7%	28.7%
Prophecies and Online Cults	jesus, christ, lord, church, bible, shall, spirit, holy, amen, father, pray, satan, heaven, israel, word, brother, son, pastor, temple, unto, rapture, christians, praise, revelation, faith	19.1%	14.9%
Political Conspiracies and QAnon	trump, president, wwg1wg, dave, america, country, patriots, bush, deep, mueller, obama, potus, justice, american, law, vote, clinton, hillary, military, fbi, plan, media, democrats, war, gold	12.6%	25.9%

Table 2. The top three topics identified by an unsupervised topic modelling algorithm. Each topic is listed with its 25 most discriminant words and the percentage of recommendations (% Rec) and videos (% Vid) that are within this topic among all the conspiratorial videos we identified.

Weighted Frequency is computed by weighting the *Raw Frequency* by the number of views of the source video. This weighting captures the fact that recommendations made from more popular videos have more impact on viewership.

Both of these trends indicate that YouTube experienced a conspiracy boom at the end of 2018. The raw and weighted frequency of conspiratorial recommendations reached a maximum of almost 10% and 6%, Fig. 2. Shortly after this, YouTube announced on January 25, 2019 their forthcoming effort to recommend less conspiratorial content.

Starting in April 2019, we monitored a consistent decrease in conspiratorial recommendations until the beginning of June 2019 when the raw frequency briefly hit a low point of 3%. Between June and December of 2019, YouTube announced that view-time of conspiratorial

recommendations had decreased by 50% and then 70%²⁷, a statement mostly consistent with our analysis. The weighted frequency trend that we observed, however, tempers these otherwise encouraging reductions. When the popularity of the source video is accounted for, the proportion of conspiratorial recommendation has steadily rebounded since its low point in May 2019, and are now only 40% less common than when the YouTube's measures were first announced.

Content

To understand the nature of the conspiracy videos that we uncovered, we used a topic modelling technique called non-negative matrix factorization (NMF). This algorithm approximates a term-document matrix as the product of a

document-topic matrix multiplied by a topic-terms matrix, thus discerning the main topics from the latent semantic structure of the data³⁴.

This analysis led to three major topics: (1) alternative science and history; (2) prophecies and online cults; and (3) political conspiracies. Shown in Table 2 are the top 25 words from the comments section that are the most discriminating to cluster conspiratorial videos in topics (but not to detect conspiracies). The first major topic is the redefinition of the mainstream historical narrative of human civilization and development. This content uses scientific language, without the corresponding methodology, often to reach a conclusion that supports a fringe ideology less well served by facts. For example, the refuting of evolution, the claim that Africa was not the birthplace of the human species or arguments that the pyramids of Giza are evidence of a past high-technology era. Conspiracies relating to climate are also common, ranging from claims of governmental climate engineering – including chemtrails – to the idea that climate change is a hoax, and that sustainable development is a scam propagated by the ruling elite. A number of videos address purported NASA secrets, for instance refuting the U.S. moon landing or claiming that the U.S. government is secretly in contact with aliens.

The second topic includes explanations of world events as prophetic, such as claims that the world is coming to an end or that natural catastrophes and political events are religious realisations. Many videos from this category intertwine religious discourse based on scripture interpretations with conspiratorial claims, such as describing world leaders as Satan-worshippers, sentient-reptiles or incarnations of the anti-Christ. These videos rally a community around them, strengthened by an '*Us vs. Them*' narrative that is typically hostile to dissenting opinions, in ways similar to cult recruitment tactics³⁵. We emphasize that most of the religious content found on YouTube does not fall into this category.

The third main topic is comprised of political conspiracies, the most popular of which is QAnon, a conspiracy based on a series of ciphered revelations made on the 4chan anonymous message board by a user claiming to have access to classified U.S. government secrets. These videos are part of a larger set of conspiratorial narratives targeting governmental figures and institutions, such as the Pizzagate, allegations that a deep state cabal and the United Nations are trying to rule a new world order, or claims the Federal Reserve and the media are acting against the interests of the United States.

We found relatively few instances of promotion of conspiratorial videos about the three topics explicitly cited by YouTube in their public statement: flat-earth, miracle cures and 9/11²⁵. Other common conspiratorial themes such as alternative theories on the JFK assassination or denial of the Sandy Hook shooting are also rarely promoted. This seems to suggest that highly publicized topics fall under closer scrutiny, while other conspiracies are still regularly recommended.

The three examples listed by YouTube illustrated conspiracies which could *misinform users in harmful ways*. Tribute ought to be paid to YouTube for effectively filtering out some dangerous themes, such as claims that vaccines cause autism. Nonetheless, other themes which we showed to be actively promoted by YouTube were described by the FBI

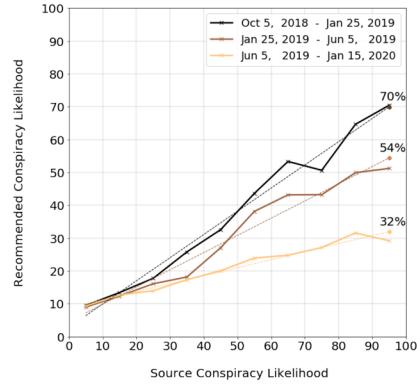


Figure 3. Proportion of conspiratorial recommendations conditioned on the conspiracy likelihood of the source video, for the three time periods between the YouTube announcements. Higher values on the right-side of the graph indicate a stronger 'filter bubble'.

as very likely to motivate some domestic extremists to commit criminal, sometime violent activity¹⁵. The report explicitly cites QAnon and Pizzagate conspiracies, depictions of the New World Order, and the United Nations as an organization for the elites to establish a global rule. Similarly, conspiracy-driven online cults have motivated a matricide³⁶. And, seemingly more innocuous conspiracies can also cause unrest, such as when 1.5 million people gathered on a Facebook group pledging to run onto the military facility Area 51 in a quest to "see them aliens", forcing the U.S. Air Force to threaten them with the use of force³⁷.

Filter Bubble

There is a clear positive correlation between the conspiracy likelihood of the source video and the conspiracy likelihood of the recommended video, Fig. 3. Although it is an expected feature for a recommendation engine to suggest videos that are similar to the previously watched video, overly selective algorithmic recommendations can lead to a state of informational isolation - a phenomenon called *filter bubble* (or *echo chamber*).

Shown in Fig. 3 is a quantification of this filter-bubble effect in which we see a clear correlation between the proportion of conspiratorial content that is recommended after a conspiratorial video is watched. This correlation is most striking for the time window between October 2018 through January 2019, but has also decreased proportional to the overall reduction shown in Fig. 2.

Discussion

Limitations

Our data set of recommendations is aimed at emulating the default behavior of YouTube's watch-next algorithm using a set of 1146 channels as the roots of the recommendation

tree. Although this set constitutes a small subset of YouTube and is not necessarily a complete representation of the entire informational landscape, it was obtained through recursive iterations on the watch-next algorithm, starting from the 250 most followed channels (see Recommendations in Methods). It should, therefore, be by construction, representative of the most commonly recommended informational channels.

Our conspiracy classifier was trained on a set of what we believe to be "clear-cut" conspiracy-theory videos. We recognize that there is an inherent subjectivity in labeling whether a theory is conspiratorial. Many conspiracies, for example, intertwine objective facts with fabricated and far-fetched claims. We have, nevertheless, attempted to categorize a video as conspiratorial based on some objective guidelines (see Data Set in Methods).

Although some topics are more nuanced than others, our conspiracy classifier achieves a relatively high accuracy ($F1 = 0.82$), largely by leveraging the presence of discriminating language as well as references to other conspiratorial topics in the video comments. Nonetheless, the classifier does make mistakes: For instance, videos that debunk conspiracy theories are sometimes mis-classified. We have adjusted for these mistakes by weighting the detected conspiratorial videos by the expected detection accuracy, Fig. 1. Since we have accounted for false positives (incorrectly classifying a video as conspiratorial) but not for false negatives (failing to detect a video as conspiratorial), it is likely that our estimates of conspiratorial content are conservative. Moreover, videos with comments disabled or ones taken down by the author or by the platform before we analyse them are also missing from our analysis, which is more common than average for conspiratorial videos. Another limitation is that personalised recommendations, which we don't account for, can significantly impact the experience for individual users: those with a history of watching conspiratorial content will see higher proportions of recommended conspiracies. Our analysis does not capture whether personalised recommendations have changed at the same pace as non-personalized watch-next recommendations.

Policy Implementation

Our analysis corroborates that YouTube acted upon its policy and significantly reduced the overall volume of recommended conspiratorial content. The rebound that we observed after the low-point concomitant with the second YouTube announcement²⁷ could be caused by (1) Content creators reverse-engineering the moderation process to work around it; (2) YouTube trying to automate a manual moderation process which was in place the previous months; or (3) YouTube relaxing its criteria because of lower engagement or user discontentment. Despite this downturn over the past year, the overall volume of conspiratorial content recommended from informational channels remains relatively high. Additionally, the weighted frequency of conspiratorial recommendations - which accounts for the popularity of the source video - has rebounded in the months following the YouTube announcement.

Given the massively superior data, labelling and computational resources available to the company, we can affirm that YouTube is technically capable of detecting conspiratorial

topics with high accuracy. In fact, for certain topics which seem to fall under particularly close scrutiny, recommended videos are effectively stripped from disinformation. For instance, We did not surface any conspiratorial recommendation about the Corona-virus outbreak, despite the presence of many such videos on the platform. It is encouraging to see that YouTube is willing to target specific issues effectively and in a timely fashion. Deciding what to demote, is therefore a question of policy more than technology.

The reduction of borderline policy is in fact implemented selectively. Our analysis indicates that the selection is mostly happening at the channel level, in line with YouTube's strategy to focus on 'authoritative sources'²⁸. On the one hand, some conspiratorial channels have been completely banned from the default recommendation system. In fact, the ten channels which had most conspiratorial recommendations before April 2019[†] and together accounted for more than 20% of all recommended conspiracies now make up for less than 0.5% recommended conspiracies.

On the other hand, since the policy update a set of five channels[‡] account for 25% of all conspiratorial recommendations, whereas they previously represented less than 0.5%. Most of these rising channels intertwine legitimate videos and conspiracies, and seem to be benefiting from a white-listed status to have increasingly borderline content be recommended. Many of these large channels can funnel traffic from mainstream channels, which explains why the gap between the raw and the weighted frequency has been narrowing, Fig. 2. Lastly, some conspiratorial channels have been continuously recommended throughout our analysis and seem to have escaped notice, including some that promote particularly insidious disinformation.[§]

Filter Bubble

It is true that YouTube, overall, no longer recommends conspiratorial videos with a higher likelihood than what was previously watched²⁹. This result is in line with recent research which did not find strong quantitative evidence of a systematic push towards right-wing political content³⁰. Our analysis, however, shows that after a conspiratorial video is clicked, there is a high - yet decreasing - likelihood that the algorithm will recommend another one. For those with a history of watching conspiratorial content, the filter-bubble effect is strongly reinforced by personalized recommendations, which we don't capture in this study¹⁸.

It is hard to say if this selective exposure is more pronounced for conspiratorial content than for other categories. Filter bubbles and its impact in shaping political opinions might have been overstated^{39,40}, but the fact that the filter-bubble effect (Fig. 3) has decreased over the past year in proportions similar to the raw frequency indicates that it might have been an important driver of conspiratorial

[†]Anonymous Official, X22Report, Disclosed TruthTV, Edge of Wonder, Truthstream Media, ZEG TV HIDDEN FROM THE PUBLIC, Matrix Wisdom, THAT IS IMPOSSIBLE, David Icke, UAMN TV

[‡]Fox News, Science Channel, London Real, The Nimitz Encounters, After Skool

[§]Perry Stone, A Rood Awakening!, Sid Roth's It's Supernatural!, Zohar StarGate Ancient Discoveries, DTBM OnlineVideoTraining

viewership. Moreover, we argue that the repercussions of selective exposure may be stronger with conspiracy theories than they are with more typical political content, because conspiratorial narratives are rarely challenged or even addressed on other media. Conspiracy theories also tend to be unfalsifiable in the sense that evidence against a conspiracy can often be interpreted as evidence of its truth. Presenting opposing views, therefore, may not affect the faith in the conspiracy.

Summary

The overall reduction of conspiratorial recommendations is an encouraging trend. Nonetheless, this reduction does not make the problem of radicalization on YouTube obsolete nor fictional, as some have claimed⁴¹. Aggregate data hide very different realities for individuals, and although radicalization is a serious issue, it is only relevant for a fraction of the users. Those with a history of watching conspiratorial content can certainly still experience YouTube as filter-bubble, reinforced by personalized recommendations and channel subscriptions. In general, radicalization is a more complex problem than what an analysis of default recommendations can scope, for it involves the unique mindset and viewing patterns of a user interacting over time with an opaque multi-layer neural network tasked to pick personalized suggestions from a dynamic and virtually infinite pool of ideas.

With two billion monthly active users on YouTube, the design of the recommendation algorithm has more impact on the flow of information than the editorial boards of traditional media. The role of this engine is made even more crucial in the light of (1) The increasing use of YouTube as a primary source of information, particularly among the youth⁴²; (2) The nearly monopolistic position of YouTube on its market; and (3) The ever-growing weaponization of YouTube to spread disinformation and partisan content around the world⁴³. And yet, the decisions made by the recommendation engine are largely unsupervised and opaque to the public.

This research is an effort to make the behavior of the algorithm more transparent so that YouTube can be held accountable for their statements. ⁴ We hope it will fuel a public discussion, not about whether YouTube should allow for conspiratorial content on the platform, but about whether such content is appropriate to be part of the baseline recommendations on the informational YouTube

References

1. Lewis R. Alternative Influence. *Data & Society* 2018; .
2. Bessi A, Zollo F, Vicario MD et al. Users Polarization on Facebook and YouTube. *Plos One* 2016; 11(8).
3. Song MYJ and Grudz A. Examining Sentiments and Popularity of Pro- and Anti-Vaccination Videos on YouTube. *Proceedings of the 8th International Conference on Social Media and Society* 2017; .
4. O'Callaghan D, Greene D, Conway M et al. Down the (White) Rabbit Hole: The Extreme Right and Online Recommender Systems. *Social Science Computer Review* 2014; 33(4): 459-478.
5. Samory M and Mitra T. Conspiracies Online: User Discussions in a Conspiracy Community Following Dramatic Events. *ICWSM 2018* 2018; .
6. Tufekci Z. YouTube, the Great Radicalizer. *The New York Times* 2018; .
7. Allgaier J. Strategically Distorted Communications in Online Videos on Climate Change and Climate Engineering. *Frontiers in Communication* 2019; 4: 36.
8. Lewis P. Senator Warns YouTube Algorithm may Be Open to Manipulation by 'Bad Actors'. *The Guardian* 2018; .
9. Geurkink B. Our Recommendation to YouTube. *Mozilla Foundation* 2019; .
10. Lewis P. Fiction is Outperforming Reality: How YouTube's Algorithm Distorts Truth. *The Guardian* 2018; .
11. O'Donovan C, Warzel C, McDonald L et al. We Followed YouTube's Recommendation Algorithm Down The Rabbit Hole. *BuzzFeed News* 2019; .
12. Roose K. YouTube Unleashed a Conspiracy Theory Boom, can It Be Contained? *The New York Times* 2019; .
13. Ellis EG. Online Conspiracy Theories: The WIRED Guide. *Wired* 2018; .
14. AvaaZ. Why is YouTube Broadcasting Climate Misinformation to Millions? 2020.
15. FBI Phoenix Field Office. Anti-Government, Identity Based, and Fringe Political Conspiracy Theories Very Likely Motivate Some Domestic Extremists to Commit Criminal, Sometimes Violent Activity, 2019.
16. Solsman JE. YouTube's AI is the Puppet Master Over Most of What You Watch. *CNET* 2018; .
17. Hussain MN, Tokdemir S, Agarwal N et al. Analyzing Disinformation and Crowd Manipulation Tactics on YouTube. *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* 2018; .
18. Zhao Z, Hong L, Wei L et al. Recommending What Video to Watch Next: A Multitask Ranking System. In *Proceedings of the 13th ACM Conference on Recommender Systems*. RecSys '19, New York, NY, USA: ACM, pp. 43-51.
19. Chaslot G. How YouTube's A.I. Boosts Alternative Facts. *Medium* 2017; .
20. Roose K. YouTube's Product Chief on Online Radicalization and Algorithmic Rabbit Holes. *The New York Times* 2019; .
21. Zuckerberg M. A Blueprint for Content Governance and Enforcement. *A Blueprint for Content Governance and Enforcement* 2018; .
22. YouTube Now: Why We Focus on Watch Time, 2012.
23. Covington P, Adams J and Sargin E. Deep Neural Networks for YouTube Recommendations. In *Proceedings of the 10th ACM Conference on Recommender Systems - RecSys '16*. Boston, Massachusetts, USA: ACM Press, pp. 191-198.
24. Schwind C and Budet J. Reducing Confirmation Bias and Evaluation Bias: When Are Preference-Inconsistent Recommendations Effective and When Not? *Computers in Human Behavior* 2012; 28(6): 2280-2290.
25. Continuing our Work to Improve Recommendations on YouTube, 2019.
26. Matsakis L. YouTube Will Link to Wikipedia to Fight Conspiracy Theories. *Wired* 2018; .

⁴The full list of recommended videos we detected with a conspiracy likelihood above 0.5 is available at <https://github.com/youtube-dataset/conspiracy>

27. Our Ongoing Work to Tackle Hate, 2019.
28. Raising Authoritative Content and Reducing Borderline Content and Harmful Misinformation, 2019.
29. Blondel VD, Guillaume JL, Lambiotte R et al. Fast Unfolding of Communities in Large Networks. *Journal of statistical mechanics: theory and experiment* 2008; 2008(10): P10008.
30. Jackson LL. *Top 201 Conspiracy Theory Videos on YouTube*. Amazon, 2017.
31. Joulin A, Grave E, Bojanowski P et al. Bag of tricks for efficient text classification. In *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 2, Short Papers*. Association for Computational Linguistics, pp. 427–431.
32. Jigsaw, PerspectiveAPI.com, 2019.
33. Sparck Jones K. A Statistical Interpretation Of Term Specificity And Its Application In Retrieval. *Journal of Documentation* 1972; 28(1): 11–21.
34. Lee DD and Seung HS. Learning the Parts of Objects by Non-Negative Matrix Factorization. *Nature* 1999; 401(6755): 788–791.
35. DiResta R. Online Conspiracy Groups Are a Lot Like Cults. *Wired* 2018; .
36. Flanagan J. How YouTube Became a Breeding Ground for a Diabolical Lizard Cult. *The New Republic* 2019; .
37. CNN. Area 51 Fast Facts, 2019.
38. Ribeiro MH, Ottoni R, West R et al. Auditing Radicalization Pathways on YouTube. *arXiv:190808313 [cs]* 2019; ArXiv: 1908.08313.
39. Guess A and Nyhan B. Why Selective Exposure to Like-Minded Political News is Less Prevalent than You Think, 2018.
40. Munger K and Phillips J. A Supply and Demand Framework for YouTube Politics, 2019.
41. Ledwich M and Zaitsev A. Algorithmic Extremism: Examining YouTube's Rabbit Hole of Radicalization. *pre-print* 2019; .
42. Smith A, Toor S and Kessel Pv. Many Turn to YouTube for Children's Content, News, How-To Lessons. *Pew Research Center: Internet, Science and Tech* 2018; .
43. Bradshaw S and Howard P. The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation, 2019.



March 18, 2021

Ranking Member Cathy McMorris Rodgers
 House Committee on Energy and Commerce
 2322 Rayburn House Office Building
 Washington, D.C. 20515

Dear Ranking Member McMorris Rodgers,

On behalf of the [Alliance for Safe Online Pharmacies \(ASOP Global\)](#), thank you for soliciting stakeholder input ahead of your committee's hearing scheduled for Thursday, March 25, 2021 with the CEOs of Facebook, Twitter, and Google on the misinformation plaguing online platforms. ASOP Global is a nonprofit organization dedicated to public health and requests that you consider raising the dangers of prescription medicines and drugs sold illegally via online platforms during this important hearing.

The Alliance for Safe Online Pharmacies was established in 2009 to combat illegal online pharmacies and counterfeit medicines and to make the internet safer for patients worldwide through research, education, advocacy, and collaboration. ASOP Global's U.S.-based members include 30+ nonprofit groups, prescription discount programs, academic institutions, patient organizations, telehealth companies, pharmaceutical manufacturers, health care providers, pharmacy organizations, shippers, payment processors, and internet security companies. To date, U.S. policy has failed to protect Americans from illegal internet drug sellers who profit at the expense of patients' safety. This is especially concerning given that the internet and social media platforms are now more than ever relevant to patient access to care and the dissemination of public health information.

Each platform testifying at the March 25 hearing claims to have policies in place to prohibit the sale of prescription or illegal drugs, but, in our experience, their enforcement has been inconsistent. Bad actors have taken advantage of platforms' inconsistent policy enforcement to prey on Americans who have become increasingly dependent on Facebook, Twitter, and Google to make online purchases and health care decisions. Due to interpretation of Section 230 of the Communications Decency Act, internet platforms have been shielded from accountability when they fail to enforce their own policies.

Unsuspecting Consumers Are Targeted Online

Alliance for Safe Online Pharmacies (ASOP)

www.BuySafeRx.pharmacy

Page 1



Americans are increasingly looking to the internet to purchase their drugs.¹ However, at any given time, 95% of the roughly 35,000 online pharmacies worldwide operate illegally, in violation of state and/or federal law and pharmacy practice standards.² Equally as concerning is the fact that consumers are unfortunately ill-informed as to how to authenticate their purchases and how search engine algorithms work. Findings from our ASOP Global Consumer Behavior survey from June 2020 illustrated that nearly three quarters of Americans (71%) have never experienced, read, or heard about the risks of receiving a substandard or counterfeit prescription medication from an online drug seller. Four in ten Americans believe incorrectly that all websites offering healthcare services and/or prescription medications via the internet have Food and Drug Administration (FDA) or state regulator sign off. Further, seven in ten respondents to the survey erroneously believe that if an online pharmacy website appears in the top pages of a search result it is likely to be legitimate.³ This is not necessarily true. For example, Google's top page search results on March 18, 2021 for "get Canadian medicines online" yields businesses operating out of compliance with U.S. law and pharmacy practice standards.

Though social media platforms prohibit the sale of drugs on their applications, Laura Berman, who recently lost her 16-year old son after being sold a prescription drug laced with fentanyl via a social media app, would say otherwise.⁴ WhatsApp, a Facebook-owned platform, prohibits the sale of "drugs, drug paraphernalia, and prescriptions,"⁵ and Snapchat claims to have a zero-tolerance policy for using the platform for illegal drug sales.⁶ However, many college students still report buying illegal drugs on these platforms and are encouraged by the convenience and success of their purchases to experiment using other social media platforms to do the same.⁷ Buyers commonly mistake high-quality advertising pictures of drugs on WhatsApp, Instagram, and Snapchat, for being safe, authentic medications.⁸

Certain algorithms and features of social media applications make the platforms helpful to sellers and enticing to buyers. Instagram algorithms are intended to enhance the user's searches so if an individual has looked for drugs on the app, the app will deliver more drug-related ads, pages, and hashtags into a user's feed even when they are not actively searching.⁹

¹ https://buysafexrx.pharmacy/wp-content/uploads/2020/10/ASOP-Global-Survey-Key-Findings_October-2020-FINAL.pdf

² <https://nabp.pharmacy/wp-content/uploads/2018/09/Internet-Drug-Outlet-Report-September-2018.pdf>

³ https://buysafexrx.pharmacy/wp-content/uploads/2020/10/ASOP-Global-Survey-Key-Findings_October-2020-FINAL.pdf

⁴ <https://www.today.com/parents/dr-laura-berman-tested-son-drugs-fentanyl-death-1209764>

⁵ <https://www.whatsapp.com/legal/commerce-policy/?lang=en>

⁶ <https://snap.com/en-US/community-guidelines>

⁷ <https://www.basisonline.org/2019/09/social-media-messaging-smartphones-illicit-drugs.html>

⁸ http://www.monitoringthefuture.org/pubs/monographs/mtf-vol2_2018.pdf

⁹ <https://www.bostonmagazine.com/health/2019/10/15/instagram-drug-market/>



Online sellers leverage the comment section of Instagram posts that mention opioid and other illegal drug sales to conduct business and solicit transactions.¹⁰ Certain features, like those found on Instagram and Snapchat, allow messages and images to disappear after twenty-four hours and have been found to be particularly effective for counterfeit sellers to peddle their products.¹¹ This only makes it easier for digital drug dealers to prey on teens as the evidence vanishes the minute it is seen.

With hundreds of profiles on the platform and minimal verification of identity, platforms have created a safe haven for illegal drug sales. Even when a bad actor is identified and shutdown, the same user can create a different profile and continue their business. Many of these actors use multiple platforms, including various Facebook-owned ones, allowing sellers to continue transactions even when one of their profiles gets shutdown.¹² This has made it increasingly difficult for law enforcement to investigate, identify, and catch criminals as they scramble to gather enough evidence to pinpoint dealers' locations.¹³

The ongoing COVID-19 pandemic has only worsened matters, with digital drug dealers preying upon a population desperate for safety and health security. Early in the pandemic, as people searched for answers to how to keep themselves and their families safe, Americans turned to Google for information and guidance. Unfortunately, searches were flooded with misinformation with little credibility or evidence.¹⁴ On Thursday, March 17 2021, Google claims to have blocked over 99 million COVID-19 related ads last year, including those claiming to offer COVID cures, authentic N95 masks, effective vaccines, and much more.¹⁵

While we applaud the efforts internet platforms have made to date to curb healthcare misinformation and illegal online drug sales, the solutions have so far been insufficient to prevent consumer harm.

Responsibility & Enforcement are Sporadic

The FDA issues warning letters when it identifies a violation by a company or manufacturer, such as incorrect claims being made about a product. These letters are essential for the agency to protect Americans from scams and counterfeit products. In 2018, in corporation with the FDA, Google agreed to deindex domain names that are listed in FDA warning letters. This is a meaningful step and one that ASOP Global applauds. However, a 2019 review conducted by

¹⁰ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6598421/>

¹¹ https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf

¹² https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2704/RAND_RR2704.pdf

¹³ <https://pubmed.ncbi.nlm.nih.gov/28089207/>

¹⁴ https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/A_Shot_from_the_Darkest_Corner_of_the_Internet_Report.pdf

¹⁵ https://services.google.com/fh/files/misc/ads_safety_report_2020.pdf



ASOP Global found that Google had taken action on only 63% of sites listed within FDA's warning letters, leaving hundreds of websites, already flagged by the FDA as being out of compliance, still accessible to American consumers via Google searches. FDA warning letters for selling dangerous products like tramadol, abortion drugs, cancer drugs, and other painkillers and are still fully available on Google to this day, and a fraction of them have been highlighted in the table below (first five rows).

Thank you again for the opportunity to provide you, your staff, and the members of your committee with this information. ASOP Global recognizes you will receive countless responses from interested stakeholders and will have many interests to consider as you prepare for this hearing. At the end of this letter, we have compiled a list of some examples of how online platforms have allowed illegal drug sellers to peddle illegal drugs to consumers. **We do request that you raise the issue of illegal drugs sold via online platforms during the hearing and that this letter and the accompanying examples be submitted to the hearing record on March 25.** Should you or your staff have any questions related to illegal drug sales online and how platforms facilitate these dangerous practices, please view ASOP Global as a resource. We look forward to working with you to advance public health and patient safety.

Respectfully,

A handwritten signature in black ink, appearing to read "John B. Hertig".

John B. Hertig, PharmD, MS, CPPS, FASHP
 Board President, ASOP Global Board of Directors
 Vice-Chair and Associate Professor, Department of Pharmacy Practice
 Butler University College of Pharmacy and Health Sciences
jhertig@butler.edu



Examples of illegal online drugs

Platform	Illegal Drug Sale	Link
Google	Tramadol: FDA sent a warning letter stating the website operates in violation of the Food, Drug, and Cosmetic Act and was selling unapproved opioids online availablepharmacy.com is still available on Google as of 3/17/21	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/ipharmacy-05292018
Google	Abortion pills: FDA sent the operators of this website a warning letter citing Food, Drug, and Cosmetic Act violations, including the sale of misbranded and unapproved drugs goabortion.com is still available on Google as of 3/17/21	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/rablon-1111111-03082019
Google	Breast cancer and antiviral drugs: FDA sent a warning letter stating the website operates in violation of the Food, Drug, and Cosmetic Act and was selling unapproved and misbranded drugs online canadianqualitydrugs.net is still available on Google as of 3/17/21	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/icepx-1111111-10092018
Google	Tramadol and unapproved HIV treatment drugs: FDA sent a warning letter stating the website operates in violation of the Food, Drug, and Cosmetic Act and was selling unapproved and misbranded drugs online buymeds247online.com is still available on Google as of 3/17/21	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/farma-glow-1111111-10092018
Google	Misbranded Oxycodone: FDA sent a warning letter stating the website operates in violation of the Food, Drug, and Cosmetic Act and was selling unapproved and misbranded drugs online aaapharm-palace365.ru is still available on Google as of 3/17/21 and is now selling Cialis.	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/discount-pharmacy-1111111-10092018
Facebook	"Drugs:" Chicago police on Tuesday announced their latest arrests for illegally selling guns and drugs through private Facebook groups Facebook claims to monitor these groups, but CPD detectives have labeled these private hidden sites as a version of the dark web that's more accessible for everyday users	https://www.chicagotribune.com/news/breaking/ct-guns-drugs-facebook-bust-20191203-vrhgb7q2hng5hasfb7mfovcaq-story.html
Facebook	Tramadol and Carisoprodol: Snyder and the conspirators communicated concerning shipments of Tramadol and Carisoprodol tablets using social media, including Facebook	https://www.justice.gov/usa-mdpa/pr/snyder-county-man-charged-conspiracy-distribute-over-100000-prescription-pain-pills
Facebook	COVID vaccines and meds: The offers ranged from Facebook page operators willing to ship Sinovac Covid-19 vaccine—which is not authorized for use in the United States—from China, to apparent scammers on Telegram claiming to have access to Moderna, Pfizer, and AstraZeneca's vaccines	https://www.wired.com/story/covid-19-vaccine-scams-spread-facebook-telegram/
Facebook	COVID vaccine: Office for the Western District of Kentucky has filed a lawsuit in federal court in Louisville, Kentucky to shut down a webpage, six related web addresses and a related Facebook page that the suit says are attempting to lure consumers to "pre-register" for a non-existent COVID-19 vaccine in exchange for \$100 worth of Bitcoin	https://www.justice.gov/usa-wdky/cr/us-attorneys-office-shuts-down-multiple-websites-claiming-offer-preorders-covid-19
Facebook	COVID products: Herbal products, including "Carahhealth Immune," which is also referred to as "Immune Tonic" on the website, for sale in	https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/immunetonic-1111111-10092018



	the United States and that these products are intended to mitigate, prevent, treat, diagnose, or cure COVID-19	criminal-investigations/warning-letters/carahealth-605826-03262020
Facebook and Instagram	Counterfeit Pfizer medications: Illegal online sales have moved from websites to social media platforms. From 2015-2018, more than 10,000 Facebook accounts selling counterfeit Pfizer medications were identified, while during a six-month period in 2018, 1,000 Instagram accounts were also reported	https://bopp.msu.edu/magazine/industry-sector-update-what-health-professionals-need-to-know/
Instagram	Opioids: A new study used machine learning to flag Instagram posts mentioning opioid and other illegal drug sales — and roughly 10 percent, or more than 12,000 posts were from users advertising drugs, researchers found. Buyers and sellers also discussed transactions in the comments; researchers recommended that social media platforms crack down on illegal sales on their sites	https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6598421/
Instagram	Counterfeit steroids: Ensuing posts included hashtags such as #steroids, #gains, and #trenhard—a reference to trenbolone, the most powerful anabolic steroid on the market. So far, though, Silicon Valley's response has been sluggish at best. The tech giants claim immunity under a law that likens social media companies to newsstands rather than to publishers responsible for the content on their platforms. In other words, they argue, social media companies don't create the offensive material that ends up on their pages, so they can't be held liable	https://www.bostonmagazine.com/health/2019/10/15/instagram-drug-market/
Facebook and Instagram / WhatsApp and WeChat	All drugs / other products: On Facebook and Instagram, it's common for traffickers to post their WhatsApp or WeChat numbers alongside their goods, a signal to prospective buyers to connect in a more private forum. From orangutans and cheetah cubs to opioids and ancient Middle Eastern antiquities, if something can be sold illegally, researchers say, it's likely being sold somewhere on Facebook or Instagram	https://www.bloomberg.com/news/articles/2019-07-11/wildlife-traffickers-use-facebook-instagram-to-find-black-market-buyers
Instagram, Snapchat, Facebook, Tik Tok	Benzos: Teen addiction to benzodiazepines, called "benzos" for short, is on the rise, and these drugs are easier for teens to access—and get addicted to—than most parents think. In fact, they can be as easy to order as direct-messaging a dealer on Instagram. Even if teens do not have direct access to a prescription, finding a supplier can be as simple as logging into their social networks like Snapchat, TikTok, Facebook, and Instagram Facebook, which owns Instagram, says they are working to ensure illicit drug sales do not happen on the platform. "As our Regulated Goods policy explains, we prohibit attempts by individuals, manufacturers, and retailers to purchase, sell, or trade non-medical drugs and pharmaceutical drugs," says a Facebook spokesperson. "We also have a strict Advertising Policy and a Commerce Policy that prohibits the sale of opioids, prescription drugs, or the operation of online pharmacies without prior permission. We have proactive detection technology in place to find and remove such content before anyone sees it, we are constantly working to improve this technology to find more content, quickly."	https://www.yahoo.com/lifestyle/benzos-rising-popularity-among-teens-174346047.html
Twitter, Facebook, Instagram, Snapchat, Fortnite, YouTube, Tumblr and Reddit	Fentanyl: The Fentanyl crisis and the explosion of social media in just five years has transformed drug-pushing online. In fact, those who track illicit internet drug-selling know that drug dealers from China and within the U.S. use social media as the new street corner, concomitantly expanding their geographic, age and social reach	https://www.dispatch.com/opinion/20191109/column-third-parties-should-monitor-online-drug-sales



Instagram and YouTube	COVID cure: The DOJ charged Keith Lawrence Middlebrook, 53, with soliciting investments in a company called Quantum Prevention CV Inc. (QP20) through videos on YouTube and Instagram where he said he possessed a cure for COVID-19. Middlebrook claimed he planned to sell an injectable cure for the virus and a pill that would prevent infection, the department said. "The videos had more than 1 MILLION views	https://www.justice.gov/usao-cdoa/or/southern-man-arrested-federal-charges-alleging-fraudulent-investment-scheme-featuring
Instagram and Twitter	COVID products: The team identified more than 6 million Tweets and 200,000 Instagram posts that promoted possible scams involving COVID-19 treatments and products. The scams they found using AI ranged from dung remedies to do-it-yourself diagnostics. The team identified a total of 1,271 Tweets and 596 Instagram posts that promoted scams and passed that data to the FDA (U.S. Food and Drugs Administration)	https://newslanded.com/2020/08/31/twitter-and-instagram-being-used-to-sell-fake-covid-19-drugs-and-diagnostics-kits-study-finds/
Snapchat	Xanax / Fentanyl / Marijuana / all drugs: "Like yesterday, this person added me and they were selling Xanax," said an eighth-grader. Drug dealers are called "plugs" on social media, sometimes using a plug emoji to describe them. Some plugs "quick add" people on Snapchat, which categorizes users by zip code. "It really can be scary, because anytime, like, you could buy it," said the eighth-grader Snapchat did not provide an official response to questions	https://kutv.com/news/addicted-utah/addicted-utah-drug-dealers-find-potential-young-customers-on-snapchat-social-media
Snapchat	Fentanyl: In April 2020, a San Jose man faced murder charges after selling counterfeit opioid pills containing Fentanyl to an 18-year-old woman and her boyfriend via Snapchat, which caused both individuals to overdose and resulted in the young woman's death	https://www.nbcbayarea.com/news/local/sj-man-faces-murder-charge-after-woman-ods-on-fake-opioids/2272778/
Snapchat	Fentanyl: Berman said a drug dealer had connected with him on Snapchat, and sold him a prescription drug laced with Fentanyl. Snapchat is one of the most popular apps for buying and selling drugs, because the messages automatically disappear	https://www.wdb17.com/2021/02/24/early-years-snapchat-and-other-social-media-being-used-by-drug-dealers-to-target-kids/
Snapchat	Fentanyl: On February 7, Berman announced on Instagram that her "beautiful boy" had overdosed in his bedroom after purchasing fentanyl-laced Xanax from a drug dealer on Snapchat Snapchat said it has a zero-tolerance policy for using the platform to buy or sell illegal drugs. "We are constantly improving our technological capabilities to detect drug-related activity so that we can intervene proactively," the company said in a statement. "We had no higher priority than keeping Snapchat a safe environment and we will continue to invest in protecting our community."	https://www.today.com/parents/dr-laura-berman-tested-son-drugs-fentanyl-death-t209764
Social Media (general)	Xanax, Valium, Hydrocodone, Oxycodone, Percocet, and Adderall: A fair number of the dealers that we catch in this county are young people. They advertise on social media. You have a 20-year-old-dealer and he is going to know 18-year-old students. The word gets out, these young people drive, they do deliveries	https://sanfrancisco.cbslocal.com/2019/10/24/fentanyl-deaths-counterfeit-pills-invading-bay-area-schools/
Online (general)	Phenibut: It "is relatively easy to access online, but it has some pretty serious outcomes," Graves said. "It also seems to be growing in popularity, maybe even more so with the pandemic and people seeking out substances online to help with their stress."	https://news.wsu.edu/2020/09/03/pain-centers-report-big-increase-calls-phenibut/



February 15, 2021

Ms. Irene Khan
Special Rapporteur on the promotion and protection of the right to freedom of opinion
and expression
OHCHR-UNOG
8-14 Avenue de la Paix
1211 Geneve 10, Switzerland

**Re: UN Special Rapporteur's Annual Thematic Report to be Presented to the
Human Rights Council at its 47th Session in June 2021**

To the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,

The Technology and Social Change Team submits the following comment in response to the [UN Special Rapporteur's call](#) for inputs regarding the upcoming report to the Human Rights Council, to be presented in June 2021. The Technology and Social Change team ([TaSC](#)) researches media manipulation and disinformation at scale. TaSC conducts research, develops methods, and facilitates workshops for students, journalists, policy makers, technologists, and civil society organizations on how to detect, document, and debunk media manipulation campaigns that seek to control public conversation, derail democracy, and disrupt society. TaSC is led by sociologist Joan Donovan, PhD, Research Director of Harvard Kennedy School's Shorenstein Center, and a field leading expert in online extremism, media manipulation, and disinformation.

DISINFORMATION AT SCALE THREATENS FREEDOM OF EXPRESSION WORLDWIDE

**Comment of Joan Donovan, Emily Dreyfuss, Gabrielle Lim, and Brian Friedberg of
The Technology and Social Change Team at the Harvard Shorenstein Center¹**

The human right to freedom of expression includes the right to access to such expression. Increasingly, that access is threatened by social inequalities and the technological systems that hold the world's information. Within the fragmented media ecosystem of the 21st century, opaque algorithms, policies, and enforcement mechanisms determine what information is available to whom. These crucial information distribution systems – from search engines to social media, from messaging apps to legacy news publications – are vulnerable to abuse by people wishing to inject false or misleading information into the ecosystem, to cause harm, or further their own agendas. This process is known as disinformation. In the following comment, we argue that mitigating disinformation is not at odds with the right to freedom of expression. Rather, we demonstrate that mitigating disinformation is essential to safeguarding the human right to freedom of expression and access to truth.

Based on our research and domain expertise, disinformation violates the right to freedom of expression and the right to information and truth in the following ways:

1. It makes it harder to access timely, relevant, and accurate information
2. It takes advantage of algorithmic amplification to intentionally mislead
3. It silences its target victims through harassment, incitement of fear, and by crowding out their words, opinions, and other forms of expression

We do not dispute that those wishing to spread disinformation have a right to express themselves. However, we point out that the right to freedom of expression does not convey the right to have that disinformation amplified at scale, and that by doing so, may

¹ Authors thank Spring 2021 Harvard Law School Cyberlaw Clinic students Clara Carvahlo e Silva and Melyssa Eigen for their valuable assistance in preparing this comment.

actually lead to self-censorship, oppression, and other harmful effects that are counter to a democratic society.

This is in large part due to the internet's network effect that can accelerate the spread of disinformation and massively increasing the number of people it may reach. Social media, especially, brings with it mechanisms and tactics that allow for large-scale coordinated disinformation campaigns that are often hard to recognize and nearly impossible to mitigate once they have reached millions. The effect of some disinformation campaigns is real world harm, such as hate crimes, violence, harassment, and the perpetuation of discrimination.

To balance the right to express oneself with the right to access the expressions of others, including time-sensitive true and necessary information, we recommend adopting *community-based curation methods* for internet content. We explain that content moderation – the method for handling disinformation most commonly used and advocated for – is reactive and therefore insufficient. But by adopting a proactive curation policy that is grounded in community input, coupled with moderation when necessary, we can create an information ecosystem that promotes truth over sensationalism, accuracy over popularity, and can additionally be subject to more effective oversight.

1. DISINFORMATION HARMS FREEDOM OF EXPRESSION

Disinformation, defined as spreading information that is deliberately false or misleading,² directly impedes the right to freedom of expression. The international standard for freedom of expression gives all people the right not only to seek but also to “receive . . . information and ideas of all kinds, regardless of frontiers . . . through any [] media of [their] choice.”³ When a person seeks reliable information, such as accurate medical information during a pandemic⁴ or voting information during an election,⁵

² *Definitions*, THE MEDIA MANIPULATION CASEBOOK, <https://mediamanipulation.org/definitions> (last visited Feb. 6, 2021).

³ G.A. Res. 2200A (XXI), International Covenant on Civil and Political Rights, Art. 19 (Dec. 16, 1966).

⁴ See Johnathan Corpus Ong, *Southeast Asia's Disinformation Crisis: Where the State is the Biggest Bad Actor and Regulation is a Bad Word* (Jan. 12, 2021), <https://items.ssrc.org/disinformation-democracy-and-conflict-prevention/southeast-asias-disinformation-crisis-where-the-state-is-the-biggest-bad-actor-and-regulation-is-a-bad-word/>.

⁵ Pam Fessler, *Robocalls, Rumors, and Emails: Last-Minute Election Disinformation Flood Voters*, NPR (Oct. 24, 2020), <https://www.npr.org/2020/10/24/927300432/robocalls-rumors-and-emails-last-minute-election-disinformation-floods-voters>.

disinformation violates their rights by polluting the information ecosystem with false or misleading ideas that make it harder to access timely, relevant, and accurate information. It is commonly argued that mitigating the spread of such false information presents a challenge to freedom of expression and could lead to censorship. Yet disinformation, if left unchecked, may also become a threat to expression and access to information. Interventions to mitigate the spread of misinformation are therefore needed to protect these basic human rights.

Firstly, disinformation at scale can obscure accurate information, which then undermines the ability to receive accurate information. Secondly, false claims that are amplified widely and quickly through the internet and larger media sphere, can imperil the freedom of expression of those individuals and groups targeted, by silencing them, harassing them, and burying their contributions to the information ecosystem under a miasma of misinformation.^{6,7} Mitigating the spread of disinformation, therefore, is not necessarily at odds with freedom of expression, but may – if done with transparency, oversight, community input and expertise, and the goal to protect and encourage civic participation – actually promote it. If left unchecked, however, it would mean continuing the status quo, which not only prioritizes sensationalism and traffic for profit but the amplification of those who have the most money and resources. The result, in some cases, is real world harm, as seen in the persecution against the Rohingya people in Myanmar,⁸ the Capitol Hill siege on January 6, 2021,⁹ and the rise of Islamophobia in India.¹⁰

⁶ See Gina Masullo Chen et al., 'You really have to have a thick skin': A cross-cultural perspective on how online harassment influences female journalists, 21 JOURNALISM 877 (Apr. 2018).

⁷ Toxic Twitter – The Silencing Effect, AMNESTY INTERNATIONAL, <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-5/> (last visited Feb. 15, 2021).

⁸ Paul Mozur, *A Genocide Incited on Facebook, With Posts From Myanmar's Military*, NY TIMES (Oct. 15, 2018), <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>.

⁹ Joan Donovan & Gabrielle Lim, *The Internet Is a Crime Scene* (Jan. 20, 2021), <https://foreignpolicy.com/2021/01/20/internet-crime-scene-capitol-riot-data-information-governance/>.

¹⁰ Alexandre Capron, 'Coronajihad': *Fake news in India accuses Muslims of deliberately spreading Covid-19* (May 13, 2020), <https://observers.france24.com/en/20200513-india-coronajihad-fake-news-muslims-spreading-covid-19>.

1.1. The Findability Problem: Misinformation is easily produced and when amplified, can pollute the online ecosystem and impede the right to receive accurate information.

The right to information is a fundamental element of international and regional human rights law.¹¹ Central to the spirit of this right is the internationally recognized right to the truth,¹² which we interpret as the need for “timely, local, relevant, and accurate” information. However, as news consumers are increasingly moving online, new opportunities for exploitation are available for motivated actors who are intent on seeding false and misleading content. Two key contributing technological factors are (1) the ease with which the internet allows people to share false or misleading information, and (2) the algorithmic amplification of this disinformation.

First, accurate information is often displaced by disinformation during moments of heightened attention to a particular topic. Disinformers and media manipulators often leverage breaking news to set media agendas and generally sow chaos through misidentification or falsification of information. Particularly, on Twitter, disinformation flourishes alongside trending topics, which makes it difficult to find accurate information. On Facebook, disinformation is often seeded into groups and then is shared out on individual pages. As the disinformation campaign reaches more people, it is ranked higher in search and recommendation algorithms, thus reinforcing its prevalence.

Second, recommendation systems and trending algorithms can be gamed to amplify false or misleading content. Media manipulators will create multiple versions of blogs, posts, videos, and images to make the disinformation appear more popular than it really is. Thus, if an ad is repeatedly shown to a user, that user is more likely to take it as the truth.¹³ Misinformation peddlers can take advantage of this tendency by creating false or automated accounts to engineer engagement. One reason disinformation is so pervasive is that the tendency to believe information stems not from the content itself, but the source,¹⁴ making deliberately false information “believable” if it is coming from a trusted

¹¹ See *supra* note 3.

¹² G.A. Res. 68/165, Right to the Truth (Dec. 18, 2013).

¹³ Emily Dreyfuss, *Want to Make a Lie Seem True? Say It Again. And Again. And Again*, WIRED (Feb. 11, 2017), <https://www.wired.com/2017/02/dont-believe-lies-just-people-repeat/>.

¹⁴ *Id.*

source.¹⁵ This is particularly problematic online because so much content lacks proper context and provenance.

While there are many tactics available to disinformers, the truth tends to be static and relatively boring. Because social media and search engines optimize based on a set of signals from users and the content itself, an entire industry has flourished around search engine optimization. The SEO industry has pioneered a number of strategies that advantage disinformers over truthful information. One common tactic for spreading misinformation is inauthentically generated support through bots, which are artificial accounts that use anonymized techniques to amplify content.^{16,17} Manipulating search through keyword squatting, i.e., mislabeling or miscategorizing disinformation on purpose, has been an especially effective strategy for tethering disinformation to the unique names, locations, or breaking news events. When paired together, the manipulation of engagement and search returns displace the truth.

Algorithmic recommendation systems are particularly vulnerable to these tactics because algorithms neither fact-check information,¹⁸ nor have ethics training like that of a professional journalist or librarian,¹⁹ and thus mix disinformation with accurate information. With every share and retweet this information gets amplified quickly and widely regardless of whether it was someone's intention to spread misinformation. For example, during the U.S. capitol riots the "Capitol Meemaw" meme went viral even though the subject of the meme was not actually present at the riots.²⁰ This goes to show that wherever there is an opportunity for misinformation to spread, regardless of intention, it will spread and will displace accurate information. Thus, with a system

¹⁵ Adam M. Enders et al., *The Different Forms of COVID-19 Misinformation and Their Consequences*, HARVARD KENNEDY SCHOOL MISINFORMATION REVIEW (Nov. 16, 2020), <https://misinforeview.hks.harvard.edu/article/the-different-forms-of-covid-19-misinformation-and-their-consequences/>.

¹⁶ See *supra* note 2.

¹⁷ Brian Friedberg & Joan Donovan, *On the Internet, Nobody Knows You're a Bot: Pseudoanonymous Influence Operations and Networked Social Movements*, 6 JIDS (Aug. 7, 2019).

¹⁸ *Id.*

¹⁹ Joan Donovan & danah boyd, *Stop the Presses? Moving From Strategic Silence to Strategic Amplification in a Networked Media System*, AM. BEHAVIORAL SCIENTIST (2019).

²⁰ See David Mack, We Tracked Down "Capitol Meemaw" — Who Was Not Actually At The US Capitol, BUZZFEED NEWS REPORT (Jan. 12, 2021), <https://www.buzzfeednews.com/article/davidmack/capitol-meemaw-meme-topeka-kansas>.

tailored towards virality, content curation is essential to stop the spread of misinformation.

1.2. The Silencing Problem: The current online ecosystem enables targeted harassment, which has a chilling effect on freedom of expression.

Algorithms amplify more than just inaccurate information. When the disinformation in question is targeted harassment, amplification has an additional chilling effect on the right to freedom of expression. Although social media companies often have policies that forbid harassment, they are not evenly enforced, and companies may be slow to remove harassment even when it is coordinated as part of a disinformation campaign.²¹ As a result, targets of such campaigns turn to self-censorship, either by shutting down their accounts completely, altering the content of their expression, or shifting to less public platforms for communication.^{22 23 24}

One example of targeted harassment is that used by political partisans to mobilize their supporters and leverage media manipulation techniques for oppressive means.²⁵ These actors may use short and catchy phrases, known as viral slogans,²⁶ coupled with a coordinated effort to spread the message, a tactic known as swarming,²⁷ to silence dissent.²⁸ Often this takes the form of thousands of people posting the same hateful comment on their target's social media accounts. This technique has been used to swarm women online in underserved Nigerian communities and by "virtual lynch mobs" in Turkey to push its targets into self-censorship.²⁹ Actors use these techniques to flood their targets with violent comments online if they speak out online.³⁰ Absent mitigation,

²¹ Chen, *supra* note 6.

²² Andreas Reventlow, *The chilling effects of online harassment and how to respond* (Dec. 6, 2016), <https://www.mediasupport.org/chilling-effects-online-harassment-address/>

²³ GABRIELLE LIM, SECURITIZE/COUNTER-SECURITIZE THE LIFE AND DEATH OF MALAYSIA'S ANTI-FAKE NEWS ACT, <https://datasociety.net/wp-content/uploads/2020/04/Securitize-Counter-securitize.pdf>.

²⁴ *Troll Patrol Findings*, AMNESTY INTERNATIONAL, https://decoders.amnesty.org/projects/troll-patrol/findings#what_did_we_find_contained (last visited Feb. 15, 2021).

²⁵ See Anthony Nadler et al., *Weaponizing the Digital Influence Machinery The Political Perils of Online Ad Tech* (Oct. 17, 2018), <https://datasociety.net/library/weaponizing-the-digital-influence-machine/>.

²⁶ See *supra* note 2.

²⁷ *Id.*

²⁸ See Ong, *supra* note 4.

²⁹ See Reventlow, *supra* note 22.

³⁰ Chen, *supra* note 6.

this form of amplified disinformation can have a direct chilling effect on freedom of expression.³¹

Compounding the harm, targeted harassment online is frequently directed towards people who have already been marginalized,³² arguably the very people whom human rights law was created to protect. This is happening around the world, where targeted harassment has been used against vulnerable groups to crack down on political dissent,³³ and in some cases are largely led by state actors themselves against their minority populations or political opponents.³⁴ In the Philippines, for example, the arrest of journalist Maria Ressa follows years of intimidation and harassment by supporters of the ruling party.^{35, 36} While she has remained an outspoken figure despite the threats, this climate of fear and intimidation has resulted in a culture of burnout, fear, and self-censorship among the wider media industry in the Philippines.^{37, 38} Thus, if diverse and inclusive opinions online are a concern,³⁹ then allowing amplified disinformation to go unmitigated has a direct silencing effect on the opinions that the UN seeks to protect.

³¹ JON PENNEY, *Online Abuse, Chilling Effects, and Human Rights*, in CONNECTED CANADA: A RESEARCH AND POLICY AGENDA (E. Dubois & F. Martin-Bariteau eds., 2020).

³² *Id.*

³³ See Soma Basu, *Manufacturing Islamophobia on WhatsApp in India*, THE DIPLOMAT (May 10, 2019), <https://thediplomat.com/2019/05/manufacturing-islamophobia-on-whatsapp-in-india/>.

³⁴ See Ronan Lee, *Extreme Speech| Extreme Speech in Myanmar: The Role of State Media in the Rohingya Forced Migration Crisis*, 13 INT'L J. COMM'C'N (2019).

³⁵ Hannah Ellis-Petersen, *Maria Ressa: editor of Rappler news website arrested on 'cyber-libel' charges*, THE GUARDIAN (Feb. 13, 2019), <https://www.theguardian.com/world/2019/feb/13/philippines-journalists-decry-intimidation-as-website-editor-arrested>.

³⁶ Heather Timmons, *Maria Ressa's arrest is a warning to every journalist in a democracy*, QUARTZ (Feb. 13, 2019), <https://qz.com/1549538/maria-ressas-arrest-by-rodrigo-duterte-is-a-warning-to-every-journalist/>.

³⁷ Sheila S. Coronel, *A 'Fraught Time' For Press Freedom in The Philippines*, NPR (Jan. 17, 2018), <https://www.npr.org/sections/parallels/2018/01/17/578610243/a-fraught-time-for-press-freedom-in-the-philippines>.

³⁸ *CPJ mission finds increased intimidation, shrinking space for free press in the Philippines*, COMMITTEE TO PROTECT JOURNALISTS (Apr. 15, 2019), <https://cpj.org/2019/04/cpj-mission-finds-increased-intimidation-shrinking/>.

³⁹ Reventlow, *supra* note 22.

2. HOW TO AMPLIFY THE TRUTH: MOVING TOWARDS A PUBLIC INTEREST INTERNET

The debate over how to stop disinformation includes several proposed remedies to ensure compliance to site policies, local norms, and the law.⁴⁰ In this debate, two words often come to mind: moderation and curation. Moderation is often what people call for when asking governments and companies to remove harmful and false posts from the public sphere. But over a decade of social media has revealed that this approach is not sufficient.⁴¹ *Instead, we recommend working toward community-based content curation, implemented as a proactive course of action that can be complemented by moderation.*

Content moderation is the reactive process of reviewing and deciding whether content created by a user is objectionable to the online community or in violation of a specific website's terms of service.⁴² Its origins go back to the online forums of the 1970s, when most moderation was done by volunteers to ensure the discussions followed certain rules and to prevent inappropriate topics, discussions, and content from being shared within the community.⁴³ Issues such as the liability of content moderators emerged during the 1990s,⁴⁴ and many companies have delegated the responsibilities regarding content moderation to third parties. Currently in many countries, underpaid workers are tasked with viewing this harmful content and deciding what to delete.⁴⁵ In addition to being emotionally and mentally taxing on the moderators, it also doesn't work consistently.

Firstly, moderation is limited to reacting post hoc to content that has already been shared. This renders it ineffective at preventing many instances of mis- and disinformation from being seen and shared widely as moderation is often slow, inconsistent, incremental, or merely ineffective.⁴⁶ Many technology companies in the United States, for example, recently added new content moderation policies,⁴⁷ such as labeling misleading content,

⁴⁰ CHUNG SHENG-LI ET AL., NEW FRONTIERS IN COGNITIVE CONTENT CURATION AND MODERATION 3, (Cambridge University Press ed. July 23, 2018), available at <https://www.cambridge.org/core/journals/apsipa-transactions-on-signal-and-information-processing/article/new-frontiers-in-cognitive-content-curation-and-moderation/DF4AAE1F2052DF784E52B7882208AF15>.

⁴¹ SARAH T. ROBERTS, BEHIND THE SCREEN: CONTENT MODERATION IN THE SHADOWS OF SOCIAL MEDIA (Yale University Press ed. 2019).

⁴² *Id.* at 3.

⁴³ *Id.* at 2.

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

publishing transparency reports of “coordinated inauthentic behavior,”⁴⁸ or redirecting users to more credible and authoritative content.⁴⁹ However, like fact-checking and media literacy, the effectiveness of these measures is still up for debate and often happen long after the content has already been widely shared. Labeling misleading or false content, for example, may backfire as it may imply that anything without a label is true,⁵⁰ while banning users or removing content may simply shift those users and the content to other platforms.⁵¹ Furthermore, social media platforms are increasingly outsourcing content moderation to companies that are ill-equipped to understand regional contexts,⁵² but have the effect of releasing the company from liability for harassment, incitement, and hate.⁵³

In addition, moderation solutions implemented by technology companies are often at risk for increased censorship and surveillance. In China, for example, content policies are typically handed down by the Chinese Communist Party (CCP), but it is the private companies who are responsible for carrying out the content moderation. The result is undue censorship, as companies are incentivized to over-correct, so they do not violate the CCP’s directives.⁵⁴ And in countries where there is local legislation that criminalizes false information, content removal and arrests have been common. In Singapore, for example, the Protection from Online Falsehoods and Manipulation Act, has resulted in

⁴⁸ AMELIA ACKER & JOAN DONOVAN, *Data Craft: A Theory/Methods Package for Critical Internet Studies*, 22 INFO., COMM’N & SOCIETY 1590 (2019).

⁴⁹ CLEA SKOPELITI & BETHAN JOHN, *Coronavirus: How Are the Social Media Platforms Responding to the ‘Infodemic’?*, FIRST DRAFT (Mar. 19, 2020), <https://firstdraftnews.org:443/latest/how-social-media-platforms-are-responding-to-the-coronavirus-infodemic/>.

⁵⁰ GORDON PENNYCOOK ET AL., *The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Headlines Increases Perceived Accuracy of Headlines Without Warnings*, 66 MGMT. SCI. 4921 (Feb. 2020).

⁵¹ P. M. KRAFT & JOAN DONOVAN, *Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign*, 37 POLITICAL COMM’N 194 (2020).

⁵² MARGARET E. ROBERTS, CENSORED (Princeton University Press ed. 2020), <https://press.princeton.edu/books/hardcover/978069178868/censored>.

⁵³ JOAN DONOVAN & GABRIELLE LIM, DETECT, DOCUMENT, AND DEBUNK: STUDYING MEDIA MANIPULATION AND DISINFORMATION (Oxford Handbook).

⁵⁴ LOTUS RUAN ET AL., *The Intermingling of State and Private Companies: Analysing Censorship of the 19th National Communist Party Congress on WeChat*, THE CHINA QUARTERLY (July 2020).

Facebook labeling content the government deems to be false – an act that has been widely criticized by human rights groups and opposition politicians^{55,56}

Moreover, illiberal and authoritarian-leaning governments have used disinformation as a pretense to crack down on dissent.⁵⁷ In Egypt, for example, the government justifies arresting and intimidating regime critics and other forms of digital expression as safeguarding national security from “false information.”⁵⁸ Even within established democracies, the fear of “foreign speech” has similarly raised concerns over potential infringements on freedom of expression and the further balkanization of the internet.⁵⁹

Community-based content curation, on the other hand, is proactive. Curation is the act of collecting, sorting, and organizing community-generated content around a topic and actively promoting the most useful, timely, and accurate information. Content curation was first proposed as a solution to the challenge of organizing online content during the early 1990s, by the Digital Library Initiative⁶⁰ and again in the early 2000s by Tim Berners-Lee’s semantic web.^{61,62}

Curators choose to highlight the best content based on quality, not on popularity. Librarians, for example, are professionally trained to identify trustworthy sources and contents that should be available online.⁶³ In addition to ensuring compliance within a certain framework, curation also aims for accuracy and relevance. *While a moderator checks whether content is acceptable under a set of rules, a curator selects the most useful, timely, and accurate content in order to display relevant information for users. We*

⁵⁵ Rachel Au-Yong, *Parliament: Workers’ Party Opposes Proposed Law on Fake News, Says Pritam Singh*, THE STRAITS TIMES (May 7, 2019), <https://www.straitstimes.com/politics/parliament-workers-party-opposes-proposed-law-on-fake-news-pritam-singh>.

⁵⁶ RSF Explains Why Singapore’s Anti-Fake News Bill Is Terrible, REPORTERS WITHOUT BORDERS (Apr. 8, 2019), <https://rsf.org/en/news/rsf-explains-why-singapores-anti-fake-news-bill-terrible>.

⁵⁷ Elana Beiser, *Hundreds of Journalists Jailed Globally Becomes the New Normal, Committee to Protect Journalists* (Dec. 13, 2018), <https://cpj.org/reports/2018/12/journalists-jailed-imprisoned-turkey-china-egypt-saudi-arabia/>.

⁵⁸ *Id.*

⁵⁹ Gabrielle Lim, *The Risks of Exaggerating Foreign Influence Operations and Disinformation*, CENTRE FOR INT’L GOVERNANCE INNOVATION (Aug. 7, 2020), <https://www.cigionline.org/articles/risks-exaggerating-foreign-influence-operations-and-disinformation>.

⁶⁰ Edward A. Fox & Ohm Sornil, *Digital libraries*, ENCYCLOPEDIA OF COMPUTER SCIENCE 576 (2003).

⁶¹ Tim Berners-Lee et al., *The Semantic Web*, 284 SCI. AM. 28 (2001).

⁶² Sheng-Li, *supra* note 40.

⁶³ See Joan Donovan, *You Purged Racists From Your Website? Great, Now Get to Work.* (July 1, 2020), WIRED, <https://www.wired.com/story/you-purged-racists-from-your-website-great-now-get-to-work/>.

recommend complementing content moderation with active curation. Where curation fails, moderation can step in, but both methods must work together.

Curation has been growing in several practical perspectives. For example, in terms of business models, Facebook has implemented an initiative called News Tabs, a new section inside of the company's mobile application that will surface the most recent and relevant stories for readers.⁶⁴ Instead of relying on algorithms to filter information, the company hired journalists and reporters to filter the best content. In general, social media companies might step up to the challenge and build a content curation model for search, trends, and recommendation that does not rely so heavily on reactionary moderation.⁶⁵

To avoid some of the problems attendant to moderation, such as influence from political elites and censorship, we stress that curation should be *community-focused and grounded in community input and expertise and with the goal to protect and encourage civic participation.* This means having humans in the loop and not delegating all content curation to algorithmic systems. Furthermore, it requires community input and a bottom-up approach that puts safety, trust, and transparency at the forefront — not traffic or profit.

3. RECOMMENDATIONS

Recognizing the particular challenges posed by mis- and disinformation, the role of algorithmic content curation and propagation, and the potential for *community-based content curation* to address those challenges is an important first step in protecting freedom of expression. Once that step is taken, it will be incumbent on governments, content platforms, media outlets, and other stakeholders to follow through with concrete action. While a full analysis of the path from moderating misinformation to curating information is beyond the scope of this comment, there are several promising steps that would put us closer to a functioning community-based curation strategy. We must promote:

⁶⁴ Mike Isaac, *In New Facebook Effort, Humans Will Help Create Your News Stories*, N.Y. TIMES (Aug. 20, 2019), <https://www.nytimes.com/2019/08/20/technology/facebook-news-humans.html>.

⁶⁵ Joan Donovan, *Combating the Cacophony with Librarians*, GLOBAL INSIGHTS (Jan. 2021), <https://www.ned.org/wp-content/uploads/2021/01/Combating-Cacophony-Content-Librarians-Donovan.pdf>.

- *Transparency:* In order to implement effective content curation, it is important to first know who is currently in control of content and what practices they currently use to shape it. This transparency will not only help the public understand who to hold accountable, but also will help to identify where in the process improvements can be made. Governments should publish policies relevant to content regulation online, identifying any orders issued to social media platforms and other online content providers.⁶⁶ At a bare minimum, content providers should make their content restriction policies, decision making processes, and actions available online and in plain language.⁶⁷ Ideally, they should go a step further in creating transparency by publishing the algorithms they use for content moderation online, as app developers did when developing contact tracing apps during the COVID-19 pandemic.⁶⁸ Open access to algorithms' source fosters improvement through a participatory public process,⁶⁹ and additionally facilitates the replication of successful algorithms.⁷⁰ Lastly, all advertising should be clearly labelled and traceable back to the purchaser.
- *Durability:* Search and content recommendation algorithms allow content providers to react to individual users' activity – but this reactivity can be easily gamed. Search engines and social media platforms should build durability into their functionality to prevent keyword squatting and other attacks.⁷¹ This means making platforms less reactive to small changes and more responsive to long-term advantages of a stable information ecosystem, including trends that are identified by trained curators rather than algorithms.
- *Building in multi-stakeholder engagement into development:* Content moderation – the reactive removal of harmful content – arguably stretches the expertise of platform developers. *Community-based content curation* – proactive promotion of useful, contextual, truthful information – is likely beyond that expertise entirely.

⁶⁶ *Manila Principles on Intermediary Liability*, <https://www.manilaprinciples.org/> (last visited Feb. 8, 2021).

⁶⁷ *Id.*

⁶⁸ *Open Source Solutions*, DIGITAL RESPONSE TO COVID-19, <https://joinup.ec.europa.eu/collection/digital-response-covid-19/open-source-solutions> (last visited Feb. 8, 2021).

⁶⁹ *The Power of Open Source AI*, FORBES (May 22, 2019), <https://www.forbes.com/sites/insights-intelai/2019/05/22/the-power-of-open-source-ai/?sh=4b1031276300>.

⁷⁰ See Tom Bianchi, *Open Source Should Always Have Been the Way for COVID-19 Contact Tracing Apps*, CITY A. M. (Sept. 17, 2020), <https://www.cityam.com/open-source-should-always-have-been-the-way-for-the-covid-19-contact-tracing-app/>.

⁷¹ See *supra* note 2.

However, there are professionals, such as librarians, civil society organizations, journalists, and other stakeholders who have that expertise.⁷² Technology companies therefore need to understand the limits of their own capabilities and build in multi-stakeholder engagement into their development process and throughout the life of their product – in other words, hiring and working with individuals who are trained and qualified to curate content and systematically privilege credible and responsible voices over inflammatory, divisive, sensational content. Reddit is organized by communities known as subreddits and who foster a bottom-up approach to curation that is driven not by algorithms but by the members of each community.⁷³ However, all subreddits are subject to the rules of the platform. Alternatively, social media companies might step up to the challenge by hiring librarians to build a content curation model that does not rely so heavily on reactionary moderation.⁷⁴

- *Creating infrastructure that encourages democratic participation and accountability*
 - Curation and moderation policies and enforcement, while important, are not enough. How platforms organize information and groups also impacts whether mis- or disinformation is readily spread. New information technologies should therefore also consider how best to build network infrastructure that allows individuals and communities to engage in ways that promote democratic participation and prioritizes authenticity, legibility, and accuracy. While this area of research is still nascent, we encourage further research drawing from archival studies, infrastructure studies, library science, network science, and organizational sociology.^{75, 76, 77}

While there is no communication without the presence of some misinformation, this should not be the guiding principle for our global information commons. In fact, just as media manipulators depend on journalists to cover both sides of a story and took advantage of that ethic to garner unearned attention, disinformers depend on the

⁷² Donovan, *supra* note 63.

⁷³ Jennifer Forestal, *Beyond Gatekeeping: Propaganda, Democracy, and the Organization of Digital Publics*, 83 J. POL. (Jan. 2021).

⁷⁴ Donovan, *supra* note 65.

⁷⁵ Forestal, *supra* note 73.

⁷⁶ Joan Donovan, *Navigating the Tech Stack: When, Where and How Should We Moderate Content?*, CENTRE INT'L GOVERNANCE INNOVATION (Oct. 28, 2019), <https://www.cigionline.org/articles/navigating-tech-stack-when-where-and-how-should-we-moderate-content>.

⁷⁷ Susan Leigh Star, *The Ethnography of Infrastructure*, 43 AM. BEHAV. SCI. (Nov. 1999).

inaction of technology companies to ensure their campaigns go viral. Throughout the last five years, researchers have documented the same pattern: well-funded groups with large follower networks across platforms leveraged breaking news to control media agendas, especially on topics related to race, public health, politics, and gender. Much can be done to prevent misinformation from reaching millions. Like secondhand smoke, misinformation-at-scale damages the quality of public life and over time has a corrosive effect on our society. Therefore, we must make it more difficult to spread mis- and disinformation-at-scale and offer up a new vision for a public interest internet that takes community safety as its most valued feature.

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ

TAKE A SURVEY

We want to hear from you. Take part in this short survey to help shape The Wall Street Journal. [Take Survey](#)

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499>

TECH

Facebook Executives Shut Down Efforts to Make the Site Less Divisive

The social-media giant internally studied how it polarizes users, then largely shelved the research

By [Jeff Horwitz](#) and [Deepa Seetharaman](#)

May 26, 2020 11:38 am ET

A [Facebook](#) Inc. [FB 1.02% ▲](#) team had a blunt message for senior executives. The company's algorithms weren't bringing people together. They were driving people apart.

"Our algorithms exploit the human brain's attraction to divisiveness," read a slide from a 2018 presentation. "If left unchecked," it warned, Facebook would feed users "more and more divisive content in an effort to gain user attention & increase time on the platform."

That presentation went to the heart of a question dogging Facebook almost since its founding: [Does its platform aggravate polarization and tribal behavior?](#)

The answer it found, in some cases, was yes.

Facebook had kicked off an internal effort to understand how its platform shaped user behavior and how the company might address [potential harms](#). Chief Executive [Mark Zuckerberg](#) had in public and private expressed concern about "sensationalism and polarization."

But in the end, Facebook's interest was fleeting. Mr. Zuckerberg and other senior executives largely shelved the basic research, according to previously unreported internal documents and people familiar with the effort, and weakened or blocked efforts to apply its conclusions to Facebook products.

[Facebook policy chief Joel Kaplan, who played a central role in vetting proposed changes](#) argued at the time that efforts to make conversations on the platform more civil were

<https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499>

1/11

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ

“paternalistic,” said people familiar with his comments.



Facebook CEO Mark Zuckerberg, right, with Facebook policy chief Joel Kaplan in 2018.

PHOTO: CHRISTOPHE MORIN/BLOOMBERG NEWS

Another concern, they and others said, was that some proposed changes would have disproportionately affected conservative users and publishers, at a time when the company faced accusations from the right of political bias.

Facebook revealed few details about the effort and has divulged little about what became of it. In 2020, the questions the effort sought to address are even more acute, as a charged presidential election looms and Facebook has been a conduit for conspiracy theories and partisan sparring about the coronavirus pandemic.

In essence, Facebook is under fire for making the world more divided. Many of its own experts appeared to agree—and to believe Facebook could mitigate many of the problems. The company chose not to.

Mr. Kaplan in a recent interview said he and other executives had approved certain changes meant to improve civic discussion. In other cases where proposals were blocked, he said, he was trying to “instill some discipline, rigor and responsibility into the process” as he vetted the effectiveness and potential unintended consequences of changes to how the platform operated.

Internally, the vetting process earned a nickname: “Eat Your Veggies.”

Americans were drifting apart on fundamental societal issues well before the creation of social media, decades of Pew Research Center surveys have shown. But 60% of Americans

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ

think the country's biggest tech companies are helping further divide the country, while only 11% believe they are uniting it, according to a Gallup-Knight survey in March.

At Facebook, "There was this soul-searching period after 2016 that seemed to me this period of really sincere, 'Oh man, what if we really did mess up the world?'" said Eli Pariser, co-director of Civic Signals, a project that aims to build healthier digital spaces, and who has spoken to Facebook officials about polarization.

Mr. Pariser said that started to change after March 2018, when Facebook got in hot water after disclosing that Cambridge Analytica, the political-analytics startup, improperly obtained Facebook data about tens of millions of people. The shift has gained momentum since, he said: "The internal pendulum swung really hard to 'the media hates us no matter what we do, so let's just batten down the hatches.'"

In a sign of how far the company has moved, Mr. Zuckerberg in January said he would stand up "against those who say that new types of communities forming on social media are dividing us." People who have heard him speak privately said he argues social media bears little responsibility for polarization.

He argues the platform is in fact a guardian of free speech, even when the content is objectionable—a position that drove Facebook's decision not to fact-check political advertising ahead of the 2020 election.

'Integrity Teams'

Facebook launched its research on divisive content and behavior at a moment when it was grappling with whether its mission to "connect the world" was good for society.

Fixing the polarization problem would be difficult, requiring Facebook to rethink some of its core products. Most notably, the project forced Facebook to consider how it prioritized "user engagement"—a metric involving time spent, likes, shares and comments that for years had been the lodestar of its system.

Championed by Chris Cox, Facebook's chief product officer at the time and a top deputy to Mr. Zuckerberg, the work was carried out over much of 2017 and 2018 by engineers and researchers assigned to a cross-jurisdictional task force dubbed "Common Ground" and employees in newly created "Integrity Teams" embedded around the company.

3/25/2021 Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ



Displays showing social-media posts during a House Intelligence Committee hearing in 2017.

PHOTO: ANDREW HARRER/BLOOMBERG NEWS

Even before the teams' 2017 creation, Facebook researchers had found signs of trouble. A 2016 presentation that names as author a Facebook researcher and sociologist, Monica Lee, found extremist content thriving in more than one-third of large German political groups on the platform. Swamped with racist, conspiracy-minded and pro-Russian content, the groups were disproportionately influenced by a subset of hyperactive users, the presentation notes. Most of them were private or secret.

The high number of extremist groups was concerning, the presentation says. Worse was Facebook's realization that its algorithms were responsible for their growth. The 2016 presentation states that "64% of all extremist group joins are due to our recommendation tools" and that most of the activity came from the platform's "Groups You Should Join" and "Discover" algorithms: "Our recommendation systems grow the problem."

Ms. Lee, who remains at Facebook, didn't respond to inquiries. Facebook declined to respond to questions about how it addressed the problem in the presentation, which other employees said weren't unique to Germany or the Groups product. In a presentation at an international security conference in February, Mr. Zuckerberg said the company tries not to recommend groups that break its rules or are polarizing.

"We've learned a lot since 2016 and are not the same company today," a Facebook spokeswoman said. "We've built a robust integrity team, strengthened our policies and practices to limit harmful content, and used research to understand our platform's impact on society so we continue to improve." Facebook in February announced \$2 million in funding for independent research proposals on polarization.

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ

The Common Ground team sought to tackle the polarization problem directly, said people familiar with the team. Data scientists involved with the effort found some interest groups—often hobby-based groups with no explicit ideological alignment—brought people from different backgrounds together constructively. Other groups appeared to incubate impulses to fight, spread falsehoods or demonize a population of outsiders.

SHARE YOUR THOUGHTS

What should Facebook and other social-media giants be doing, if anything, to reduce polarization among their users? Join the conversation below.

In keeping with Facebook's commitment to neutrality, the teams decided Facebook shouldn't police people's opinions, stop conflict on the platform, or prevent people from forming communities. The vilification of one's opponents was the problem, according to one internal document from the team.

"We're explicitly not going to build products that attempt to change people's beliefs," one 2018 document states. "We're focused on products that increase empathy, understanding, and humanization of the 'other side.'"

Hot-button issues

One proposal sought to salvage conversations in groups derailed by hot-button issues, according to the people familiar with the team and internal documents. If two members of a Facebook group devoted to parenting fought about vaccinations, the moderators could establish a temporary subgroup to host the argument or limit the frequency of posting on the topic to avoid a public flame war.

Another idea, documents show, was to tweak recommendation algorithms to suggest a wider range of Facebook groups than people would ordinarily encounter.

Building these features and combating polarization might come at a cost of lower engagement, the Common Ground team warned in a mid-2018 document, describing some of its own proposals as "antigrowth" and requiring Facebook to "take a moral stance."

Taking action would require Facebook to form partnerships with academics and nonprofits to give credibility to changes affecting public conversation, the document says.

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ

This was becoming difficult as the company slogged through controversies after the 2016 presidential election.

“People don’t trust us,” said a presentation created in the summer of 2018.



Chris Cox, previously Facebook chief product officer, in 2018.

PHOTO:STEPHEN LAM/REUTERS

The engineers and data scientists on Facebook’s Integrity Teams—chief among them, scientists who worked on newsfeed, the stream of posts and photos that greet users when they visit Facebook—arrived at the polarization problem indirectly, according to people familiar with the teams. Asked to combat fake news, spam, clickbait and inauthentic users, the employees looked for ways to diminish the reach of such ills. One early discovery: Bad behavior came disproportionately from a small pool of hyperpartisan users.

A second finding in the U.S. saw a larger infrastructure of accounts and publishers on the far right than on the far left. Outside observers were documenting the same phenomenon. The gap meant even seemingly apolitical actions such as reducing the spread of clickbait headlines—along the lines of “You Won’t Believe What Happened Next”—affected conservative speech more than liberal content in aggregate.

That was a tough sell to Mr. Kaplan, said people who heard him discuss Common Ground and Integrity proposals. A former deputy chief of staff to George W. Bush, Mr. Kaplan became more involved in content-ranking decisions after 2016 allegations Facebook had suppressed trending news stories from conservative outlets. An internal review didn’t substantiate the claims of bias, Facebook’s then-general counsel Colin Stretch told Congress, but the damage to Facebook’s reputation among conservatives had been done.

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ



Mr. Zuckerberg on Capitol Hill for congressional hearings in 2018.

PHOTO: ERIN SCOTT/ZUMA PRESS

Every significant new integrity-ranking initiative had to seek the approval of not just engineering managers but also representatives of the public policy, legal, marketing and public-relations departments.

Lindsey Shepard, a former Facebook product-marketing director who helped set up the Eat Your Veggies process, said it arose from what she believed were reasonable concerns that overzealous engineers might let their politics influence the platform.

“Engineers that were used to having autonomy maybe over-rotated a bit” after the 2016 election to address Facebook’s perceived flaws, she said. The meetings helped keep that in check. “At the end of the day, if we didn’t reach consensus, we’d frame up the different points of view, and then they’d be raised up to Mark.”

Scuttled projects

Disapproval from Mr. Kaplan’s team or Facebook’s communications department could scuttle a project, said people familiar with the effort. Negative policy-team reviews killed efforts to build a classification system for hyperpolarized content. Likewise, the Eat Your Veggies process shut down efforts to suppress clickbait about politics more than on other topics.

Initiatives that survived were often weakened. Mr. Cox wooed Carlos Gomez Uribe, former head of Netflix Inc.’s recommendation system, to lead the newsfeed Integrity Team in January 2017. Within a few months, Mr. Uribe began pushing to reduce the outsize impact hyperactive users had.

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ

Under Facebook's engagement-based metrics, a user who likes, shares or comments on 1,500 pieces of content has more influence on the platform and its algorithms than one who interacts with just 15 posts, allowing "super-sharers" to drown out less-active users. Accounts with hyperactive engagement were far more partisan on average than normal Facebook users, and they were more likely to behave suspiciously, sometimes appearing on the platform as much as 20 hours a day and engaging in spam-like behavior. The behavior suggested some were either people working in shifts or bots.

One proposal Mr. Uribe's team championed, called "Sparing Sharing," would have reduced the spread of content disproportionately favored by hyperactive users, according to people familiar with it. Its effects would be heaviest on content favored by users on the far right and left. Middle-of-the-road users would gain influence.



Facebook COO Sheryl Sandberg at a Senate Intelligence Committee hearing, 2018.
PHOTO: JIM LO SCALZO/EPA/SHUTTERSTOCK

Mr. Uribe called it "the happy face," said some of the people. Facebook's data scientists believed it could bolster the platform's defenses against spam and coordinated manipulation efforts of the sort Russia undertook during the 2016 election.

Mr. Kaplan and other senior Facebook executives pushed back on the grounds it might harm a hypothetical Girl Scout troop, said people familiar with his comments. Suppose, Mr. Kaplan asked them, that the girls became Facebook super-sharers to promote cookies? Mitigating the reach of the platform's most dedicated users would unfairly thwart them, he said.

Mr. Kaplan in the recent interview said he didn't remember raising the Girl Scout example but was concerned about the effect on publishers who happened to have enthusiastic

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ

followings.

The debate got kicked up to Mr. Zuckerberg, who heard out both sides in a short meeting, said people briefed on it. His response: Do it, but cut the weighting by 80%. Mr. Zuckerberg also signaled he was losing interest in the effort to recalibrate the platform in the name of social good, they said, asking that they not bring him something like that again.

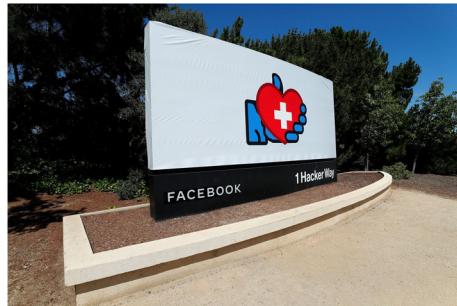
Mr. Uribe left Facebook and the tech industry within the year. He declined to discuss his work at Facebook in detail but confirmed his advocacy for the Sparring Sharing proposal. He said he left Facebook because of his frustration with company executives and their narrow focus on how integrity changes would affect American politics. While proposals like his did disproportionately affect conservatives in the U.S., he said, in other countries the opposite was true.

Other projects met Sparring Sharing's fate: weakened, not killed. Partial victories included efforts to promote news stories garnering engagement from a broad user base, not just partisans, and penalties for publishers that repeatedly shared false news or directed users to ad-choked pages.

The tug of war was resolved in part by the growing furor over the Cambridge Analytica scandal. In a September 2018 reorganization of Facebook's newsfeed team, managers told employees the company's priorities were shifting "away from societal good to individual value," said people present for the discussion. If users wanted to routinely view or post hostile content about groups they didn't like, Facebook wouldn't suppress it if the content didn't specifically violate the company's rules.

3/25/2021

Facebook Executives Shut Down Efforts to Make the Site Less Divisive - WSJ



Facebook headquarters in Menlo Park, Calif., this month.

PHOTO: JOHN G. MABANGLO/EPA/SHUTTERSTOCK

Mr. Cox left the company several months later after disagreements regarding Facebook's pivot toward private encrypted messaging. He hadn't won most fights he had engaged in on integrity ranking and Common Ground product changes, people involved in the effort said, and his departure left the remaining staffers working on such projects without a high-level advocate.

The Common Ground team disbanded. The Integrity Teams still exist, though many senior staffers left the company or headed to Facebook's Instagram platform.

Mr. Zuckerberg announced in 2019 that Facebook would take down content violating specific standards but where possible take a hands-off approach to policing material not clearly violating its standards.

"You can't impose tolerance top-down," he said in an October speech at Georgetown University. "It has to come from people opening up, sharing experiences, and developing a shared story for society that we all feel we're a part of. That's how we make progress together."

Write to Jeff Horwitz at Jeff.Horwitz@wsj.com and Deepa Seetharaman at Deepa.Seetharaman@wsj.com

Appeared in the May 27, 2020, print edition as '.'

Copyright © 2021 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499>

10/11

3/24/2021

FBI: Surge in Internet Crime Cost Americans \$4.2 Billion | Voice of America - English

USA

FBI: Surge in Internet Crime Cost Americans \$4.2 Billion

By Masood Farivar
March 17, 2021 08:13 PM



The FBI says it received a record number of complaints from the public last year about cybercrimes, including scams related to the COVID-19 pandemic, costing Americans a staggering \$4.2 billion in losses.

The FBI's Internet Crime Complaint Center received 791,790 complaints in 2020, an increase of 69% over 2019 and the largest number since the center was created two decades ago, the bureau said in a report released Wednesday.

By comparison, the total reported losses were \$3.5 billion in 2019 and \$1.5 billion five years ago, according to the report.

The type of online scam known as Business E-Email Compromise (BEC) remained the costliest category, the report said, resulting in losses of about \$1.8 billion. Once a fraudster gains access to a business's email account, he or she makes unauthorized fund transfers.

The COVID-19 outbreak gave scammers new opportunities to steal. The FBI internet crime center received more than 28,500 complaints related to people struggling to cope with the pandemic, the report said, without putting a dollar figure on the losses.

3/24/2021

FBI: Surge in Internet Crime Cost Americans \$4.2 Billion | Voice of America - English

Most vulnerable are targeted

“These criminals used phishing, spoofing, extortion, and various types of Internet-enabled fraud to target the most vulnerable in our society — medical workers searching for personal protective equipment, families looking for information about stimulus checks to help pay bills, and many others,” the report said.

The center received thousands of complaints related to COVID-linked unemployment benefit and small business loan programs Congress created last year.



The congressionally funded Paycheck Protection Program has proven a magnet for fraudsters. Congress created the program last March with an initial authorization of up to \$349 billion in forgivable loans to small businesses that keep workers on their payrolls. The Justice Department has charged numerous individuals with defrauding the program by setting up shell companies and other schemes.

In the latest case, tech executive Mukund Mohan pleaded guilty on Monday of wire fraud and money laundering in connection with his scheme to obtain over \$5.5 million in PPP loans and launder the proceeds.

The top three crimes reported to the FBI’s internet crime center last year were phishing or password theft scams, nonpayment/nondelivery scams and extortion, the report said.

In a nonpayment scheme, goods and services are shipped but payment is never made. A nondelivery scheme involves receiving payment without supplying

3/24/2021

FBI: Surge in Internet Crime Cost Americans \$4.2 Billion | Voice of America - English

goods and services.

Identity theft utilized

In several states, fraudsters filed illegal unemployment benefit claims using stolen identities, according to the report.

“Many victims of this identity theft scheme did not know they had been targeted until they attempted to file their own legitimate claim for unemployment insurance benefits,” the report said.

In recent months, a slew of new scams related to COVID vaccines has emerged: schemes asking people to pay out of pocket to receive a vaccine, put their names on a vaccine waiting list or obtain early access.

“Fraudulent advertisements for vaccines popped up on social media platforms, or came via email, telephone calls, online, or from unsolicited/unknown sources,” the report said.

The FBI’s Internet Crime Complaint Center was set up in 2000 as part of the bureau’s effort to combat cybercrime. It has received 5.8 million complaints, some of which have been referred to law enforcement agencies for investigation.

RELATED STORIES

COVID-19 Pandemic

UN Warns Cybercrime on Rise During Pandemic

Crisis has produced 600% increase in malicious emails

 By Associated Press
Sat, 05/23/2020 - 08:21 PM

COVID-19 Pandemic

3/24/2021

FBI: Surge in Internet Crime Cost Americans \$4.2 Billion | Voice of America - English

EU Commission Warns of Increased Cybercrime During Coronavirus Crisis

Authorities say more people working from home increases susceptibility to on-line scams



By VOA News

Tue, 03/24/2020 - 03:28 PM



By
Masood Farivar



Search
U.S.
World
Business
Tech & S
Culture
Newsge
Sports
Health
The Deb
Experts
Vantage



F



R
D PEARL

**OPINION**

Google Is Not Cracking Down on the Most Dangerous Drug in America | Opinion



Unlimited 30 Day Ad Free Trial

[SUBSCRIBE NOW >](#)You have **5** free articles remaining this month

Sign-up to our daily newsletter for more articles like this + access to 5 extra articles

[SUBSCRIBE >](#)

3/25/2021

Google Is Not Cracking Down on the Most Dangerous Drug in America | Opinion

[OPINION](#) [GOOGLE](#) [FENTANYL](#) [DRUGS](#) [DRUG OVERDOSE](#)

As the country grapples with the ongoing COVID-19 pandemic, more than two million Americans are still struggling with another life-threatening crisis: opioid abuse and addiction. While the opioid epidemic overall may be leveling off, health experts are sounding the alarm that the novel coronavirus may power the next wave of drug abuse. Their warnings may soon be realized if Google, one of the world's largest tech companies, fails to take action.

According to the Centers for Disease Control and Prevention, two thirds of the [Unlimited 30 Day Ad Free Trial](#)

[SUBSCRIBE NOW >](#)

You have 5 free articles remaining this month

Sign-up to our daily newsletter for more articles like this + access to 5 extra articles

[SUBSCRIBE >](#)

3/25/2021

Google Is Not Cracking Down on the Most Dangerous Drug in America | Opinion

the online purchase of pure fentanyl and fentanyl-laced drugs. Both can now be purchased with a simple search and a click of a mouse.

In 2009, Google acknowledged its role in distributing controlled substances when, before a landmark, half-billion-dollar settlement with the U.S. Department of Justice, it agreed to no longer accept paid advertisements for prescription drugs from pharmacies not authorized to sell those drugs in the United States.

Why, then, does Google continue to permit such ready access to fentanyl distribution sites in its search results?

[NEWSWEEK SUBSCRIPTION OFFERS >](#)



You have **5** free articles remaining this month
Sign-up to our daily newsletter for more articles like this + access to 5 extra articles

[SUBSCRIBE >](#)

3/25/2021

Google Is Not Cracking Down on the Most Dangerous Drug in America | Opinion



To study the ease with which one could locate fentanyl for sale online using Google's search engine, we constructed a set of 29 straightforward search terms, such as "buy fentanyl online no prescription" and "where to buy fentanyl online for sale."

Once a week, we ran Google searches with these terms and retrieved the top 100 results (to ensure that the search results were not distorted by previous searches, no cookies or personally identifying information were transmitted with these searches). We then compared the contents of the retrieved sites to a database of distinguishing markers—133 text snippets and 66 images drawn from websites previously identified by law enforcement as illegally selling fentanyl online. Finally, we manually reviewed matches to ensure that these sites were clearly purporting to sell fentanyl or a product containing fentanyl.

Unlimited 30 Day Ad Free Trial

[SUBSCRIBE NOW >](#)

You have **5** free articles remaining this month

Sign-up to our daily newsletter for more articles like this + access to 5 extra articles

[SUBSCRIBE >](#)

3/25/2021

Google Is Not Cracking Down on the Most Dangerous Drug in America | Opinion

a five-month period, we identified 70 unique sites with our Google searches. Google prominently displayed the fentanyl distributing websites.

The websites to which Google directed us had an average search rank of 11. This means that most of them were likely to appear either on the first or second page of search results. Many of these sites had blatantly obvious domain names, like [fentanylworld.com](#). While some of these sites were eventually unreachable, many of them remained active for the entire five-month period of our study.

[NEWSWEEK SUBSCRIPTION OFFERS >](#)

Google office in Berlin

Unlimited 30 Day Ad Free Trial

[SUBSCRIBE NOW >](#)

You have 5 free articles remaining this month

Sign-up to our daily newsletter for more articles like this + access to 5 extra articles

[SUBSCRIBE >](#)

3/25/2021

Google Is Not Cracking Down on the Most Dangerous Drug in America | Opinion

surfacing of websites that are blatantly purporting to sell fentanyl. In fact, by using distinct markers from websites previously identified as having sold fentanyl, Google can nearly eliminate the likelihood of inadvertently blocking an innocuous website.

In the past, tech industry giants such as Google have argued that it is pointless to block certain websites because they simply emerge under slightly modified names—thus leading to an endless whack-a-mole problem. This problem, however, can be addressed by tracking distinct markers in the underlying webpage code, text and imagery associated with specific sites. Similar approaches have proven effective in blocking everything from child sexual abuse to terrorism-related material.

We would freely share with Google and others our underlying methodology so that the company can build similar systems.

The fentanyl threat in America is too great to allow Google to continue to stand on the sidelines, denying its complicity in making fentanyl widely available through online sales. Making it harder to locate websites known to be selling fentanyl online will save lives, even if it cannot stop all online sales.

Unlimited 30 Day Ad Free Trial[SUBSCRIBE NOW >](#)

You have **5** free articles remaining this month

Sign-up to our daily newsletter for more articles like this + access to 5 extra articles

[SUBSCRIBE >](#)

3/25/2021

Google Is Not Cracking Down on the Most Dangerous Drug in America | Opinion

Dr. Hany Farid is a professor at the University of California, Berkeley, with a joint appointment in electrical engineering and computer sciences and the School of Information.

Mathea Falco is a leading expert in drug abuse prevention and treatment who served as the first U.S. assistant secretary of state for international narcotics and law enforcement affairs under President Jimmy Carter. Falco is the president of Drug Strategies, a non-profit research institute.

The views expressed in this article are the writers' own.

[REQUEST REPRINT & LICENSING, SUBMIT CORRECTION OR VIEW EDITORIAL GUIDELINES](#)

SPONSORED CONTENT



Unlimited 30 Day Ad Free Trial

mgid ▶

SUBSCRIBE NOW ▶

You have 5 free articles remaining this month

Sign-up to our daily newsletter for more articles like this + access to 5 extra articles

SUBSCRIBE ▶

3/23/2021

Bill Gates and Steve Jobs raised their kids tech-free — and it should've been a red flag | The Independent | The Independent

THE INDEPENDENT

[Contribute](#) [Subscribe](#) [LOGIN](#)

INDY/LIFE



Silicon Valley parents are strict about tech use

BILL GATES AND STEVE JOBS RAISED THEIR KIDS TECH-FREE — AND IT SHOULD'VE BEEN A RED FLAG

Chris Weller | Tuesday 24 October 2017 13:30 | comments

[Email](#) [Facebook](#) [Twitter](#) [WhatsApp](#) [SMS](#)

From news to politics, travel to sport, culture to climate – The Independent has a host of newsletters to suit your interests. Find the stories you want to read, and more, in your inbox. [Find out more](#).

- Interviews with Bill Gates, Steve Jobs, and other tech elites consistently reveal that Silicon Valley parents are strict about technology use.
- A new book suggests the signs may have been clear years ago that smartphone use should be regulated.

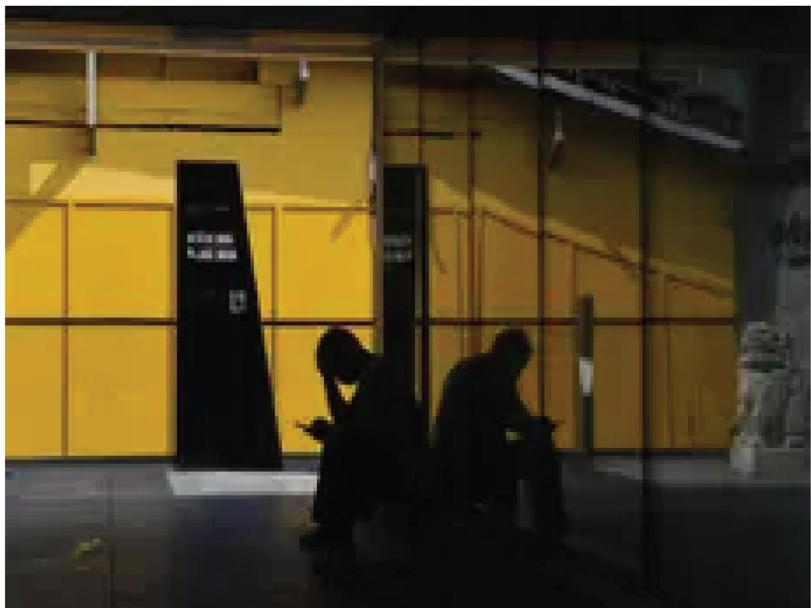
[Sign up to our free newsletters](#)

3/23/2021

Bill Gates and Steve Jobs raised their kids tech-free — and it should've been a red flag | The Independent | The Independent

THE INDEPENDENT[Contribute](#)[Subscribe](#)[LOGIN](#)

But the writing about smartphone risk may have been on the wall for roughly a decade, according to educators Joe Clement and Matt Miles, coauthors of the recent book ["Screen Schooled: Two Veteran Teachers Expose How Technology Overuse is Making Our Kids Dumber."](#)

[Read more](#)**How getting rid of my smartphone revolutionised my life**

It should be telling, Clement and Miles argue, that the two biggest tech figures in recent history — Bill Gates and Steve Jobs — seldom let their kids play with the very products they helped create.

"What is it these wealthy tech executives know about their own products that their consumers don't?" the authors wrote. The answer, according to a growing body of evidence, is the addictive power of digital technology.

'We limit how much technology our kids use at home'

In 2007, Gates, the former CEO of Microsoft, implemented a cap on screen time when his daughter started developing an unhealthy attachment to a video game. He also didn't let his kids get cell phones until they turned 14. (Today, the [average age](#) for a child getting their first phone is 10.)

INDY/LIFE Newsletter

X

3/23/2021

Bill Gates and Steve Jobs raised their kids tech-free — and it should've been a red flag | The Independent | The Independent

 INDEPENDENT[Contribute](#)[Subscribe](#)[LOGIN](#) I would like to be emailed about offers, events and updates from The Independent.
Read our [privacy notice](#)

Jobs, who was the CEO of Apple until his death in 2012, [revealed in a 2011 New York Times interview](#) that he prohibited his kids from using the newly-released iPad. "We limit how much technology our kids use at home," Jobs told reporter Nick Bilton.

 2

In "Screen Schooled," Clement and Miles make the case that wealthy Silicon Valley parents seem to grasp the addictive powers of smartphones, tablets, and computers more than the general public does — despite the fact that these parents often make a living by creating and investing in that technology.

Promoted stories

NFL Star Rob Gronkowski's Go To Shoes Off The Field

WOLF & SHEPHERD

Sponsored Links by Tab 

3/23/2021

Bill Gates and Steve Jobs raised their kids tech-free — and it should've been a red flag | The Independent | The Independent

 INDEPENDENT

≡

[Contribute](#)[Subscribe](#)[LOGIN](#)

technology, or "edtech." But Clement and Miles suggest that if Jobs' kids had attended the average US school today, they'd have used tech in the classroom far more than they did at home while growing up.

That's at the average school at least, according to the coauthors. A number of specialty Silicon Valley schools, such as the Waldorf School, are noticeably low-tech. They use chalkboards and No. 2 pencils. Instead of learning how to code, kids are taught the soft skills of cooperation and respect. At Brightworks School, [kids learn creativity](#) by building things and attending classes in treehouses.

Edtech won't be a 'cure all'

If there is any concession Gates has made on technology, it's in the benefits it offers students in certain educational settings. In the years since Gates implemented his household policy, the billionaire philanthropist has taken a keen interest in personalized education, an approach that uses electronic devices to help tailor lesson plans for each student.

In a recent [blog post](#), Gates celebrated Summit Sierra, a Seattle-based school that takes students' personal goals — like getting into a specific college — and devises a path to get there. Teachers in personalized learning settings take on more of a coaching role, helping to nudge students back on track when they get stuck or distracted.

Technology in these cases is being used as specifically as possible — and in ways Gates recognizes as useful for a student's development, not as entertainment.

"Personalized learning won't be a cure-all," he wrote. But Gates said he's "hopeful that this approach could help many more young people make the most of their talents."

Read more:

- [This chart is easy to interpret: It says we're screwed](#)
- [How Uber became the world's most valuable startup](#)
- [These 4 things could trigger the next crisis in Europe](#)

Read the original article on [Business Insider UK](#) © 2016 [Business Insider UK](#) all rights reserved

X

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

ANNALS OF TECHNOLOGY

INSIDE THE MAKING OF FACEBOOK'S SUPREME COURT

The company has created a board that can overrule even Mark Zuckerberg. Soon it will decide whether to allow Trump back on Facebook.

By Kate Klonick
February 12, 2021



Illustration by Dalbert B. Vilarino

On a morning in May, 2019, forty-three lawyers, academics, and media experts gathered in the windowless basement of the NoMad New York hotel for a private meeting. The room was laid out a bit like a technologist's wedding, with a nametag and an iPad at each seat, and large succulents as centerpieces. There were also party favors: Facebook-branded notebooks and pens. The company had convened the group to discuss the Oversight Board, a sort of private Supreme Court that it was creating to help

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

govern speech on its platforms. The participants had all signed nondisclosure agreements. I sneaked in late and settled near the front. "Clap if you can hear me," the moderator, a woman dressed in a black jumpsuit, said.

Since its founding, in 2004, Facebook had modelled itself as a haven of free expression on the Internet. But in the past few years, as conspiracy theories, hate speech, and disinformation have spread on the platform, critics have come to worry that the company poses a danger to democracy. Facebook promised to change that with the Oversight Board: it would assemble a council of sage advisers—the group eventually included humanitarian activists, a former Prime Minister, and a Nobel laureate—who would hear appeals over what kind of speech should be allowed on the site. Its decisions would be binding, overruling even those of Mark Zuckerberg, the company's founder. Zuckerberg said he had come to believe that a C.E.O. shouldn't have complete control over the limits of our political discourse. "Maybe there are some calls that just aren't good for the company to make by itself," he told me.

Listen

[Kate Klonick on the power of Facebook's Oversight Board](#), from *The New Yorker Radio Hour* and *Radiolab*.



In 2019, Facebook agreed to let me report on the process, and I spent eighteen months following its development. Last month, the board ruled on its first slate of cases, which dealt with, among other topics, the glorification of Nazis and misinformation about the coronavirus pandemic. In the next few months, it will decide an even larger question: whether [Donald Trump](#) should be cut off indefinitely from his millions of followers for his role in inciting the insurrection at the Capitol, on January 6th. Nathaniel Persily, a law professor at Stanford, told me, "How the board considers the issues and acts in that case will have dramatic implications for the future of the board, and perhaps for online speech in general."

In the beginning, Facebook had no idea how the board would work. To come up with ideas, the company held workshops with experts in Singapore, New Delhi, Nairobi, Mexico City, Berlin, and New York. "My job was to go all over the world and get as much feedback as possible," Zoe Darmé, who oversaw the consultation process, told me. At the workshop in New York, in the hotel basement, participants sat at tables of eight or nine and ran simulations of cases. I sat between Jeff Jarvis, a journalism professor, and Ben Ginsberg, a Republican lawyer who represented George W. Bush in *Bush v. Gore*.

For our first case, the moderator projected a picture of a smiling girl in a yearbook photo, with a cartoon thought bubble that read "Kill All Men." Facebook had removed the post for violating its hate-speech rules, which ban attacks based on "sex, gender identity." To many, this seemed simplistic. "It's a joke," one woman said. "There has to be an exception for humor." Facebook's rules did include a humor exception, for instances in which the user's intent was clear, but it was difficult to discern this person's motivation, and attendees worried that a broad carve-out for jokes could easily provide cover for hate speech. Carmen Scurato, who works at Free Press, an Internet-advocacy organization, pointed out the historical disadvantage of women, and argued that hate-speech policies ought to take power dynamics into account. In the end, the group voted to restore the photo, though no one knew exactly how to write that into a rule.

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

This kind of muddy uncertainty seemed inevitable. The board has jurisdiction over every Facebook user in the world, but intuitions about freedom of speech vary dramatically across political and cultural divides. In Hong Kong, where the pro-democracy movement has used social media to organize protests, activists rely on Facebook's free-expression principles for protection against the state. In Myanmar, where hate speech has contributed to a genocide against the Rohingya, advocates have begged for stricter enforcement. Facebook had hoped, through the workshops, to crowdsource beliefs about speech, but the results were more contradictory than anticipated. In New York, for example, sixty per cent of people voted to reinstate the "Kill All Men" post, but only forty per cent did so in Nairobi. Amid other theories, Darmé speculated, "Where countries are perhaps more concerned about safety, because they live in an area with less rule of law—and therefore there's a chance of a group actually maybe trying to kill all men—there's less concern about free speech." The full explanation is likely more complex; regardless, the divergent results underscored the difficulty of creating a global court for the Internet.

Some of the workshops devolved into disarray. In Singapore, Nairobi, and New Delhi, a few participants refused to sign the nondisclosure agreements, protesting Facebook's lack of transparency; in Germany, someone commandeered the microphone and berated the company for killing democracy. "We had to learn to put on our body armor," Darmé said. In New York, the session remained civil, but just barely. Some participants thought that the board would be ineffectual. "The whole thing seemed destined for failure," Sarah T. Roberts, a professor of information studies at U.C.L.A., told me. "Skeptics will think it's captured by the corporate interest of Facebook. Others will think it doesn't do enough, it's a pseudo-institution." Some predicted the board would come to have grand ambitions. Tim Wu, a law professor at Columbia, said, "If the board is anything like the people invited to New York, I wouldn't be surprised if it got out of control and became its own little beast that tried to change the world one Facebook decision at a time."

Participants had been instructed to use an app called Slido to submit questions for group discussion, which could be voted up or down on the agenda. The results were projected on a screen at the front of the room. The app had worked well abroad, but in New York it became a meta-commentary on content moderation. Sophisticated questions about "automatic tools for takedowns" and the "equity principle with diverse communities" were soon overtaken by a joke about "Game of Thrones." Posts were initially anonymous, but users quickly found a way around the system; "Harold" wrote, "I figured out how to identify self," which provoked laughter. The moderator shouted to regain control of the room. In the midst of the chaos, someone posted, "Can we abandon Slido and talk?," which quickly accumulated likes.

The idea that Facebook, like a fledgling republic, would need to institute democratic reforms might have seemed silly a decade ago. In 2009, shortly after the company was criticized for quietly changing its terms of service to allow it to keep users' data even after they deleted their accounts, it released a video of Zuckerberg, clad in an uncharacteristic button-up shirt and a tie, announcing a "new approach to site governance." People would be able to vote on Facebook's policies; the company called it "a bold step toward transparency." In the first referendum, on whether to change the terms of service, only 0.32 per cent of users voted. "In its own eyes, Facebook has become more than merely a recreational website where users share photos and wish each other a happy birthday," a columnist for the *Los Angeles Times* wrote. "It is now a global body of citizens that should be united and protected under a popularly ratified constitution. But it's hard to have a democracy, a constitution or a government if nobody shows up." In 2012, the project was quietly shuttered, and, as with Crystal Pepsi, Google Wave, and the Microsoft Zune, no one remembers that it existed.

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

This was still a hazily optimistic time for Facebook. The company promised to “give people the power to share and make the world more open and connected.” As more users joined tech platforms, companies instituted rules to sanitize content and keep the experience pleasant. Airbnb removed housing ads that displayed Nazi flags; Kickstarter disallowed crowdfunding for “energy food and drinks”; Etsy told users to be “helpful, constructive, and encouraging” when expressing criticism. Facebook hired content moderators to filter out pornography and terrorist propaganda, among other things. But, because it saw itself as a “neutral platform,” it tended not to censor political speech. The dangers of this approach soon became apparent. Facebook now has some three billion users—more than a third of humanity—many of whom get their news from the site. In 2016, Russian agents used the platform in an attempt to sway the U.S. Presidential election. Three years later, a white supremacist in New Zealand live-streamed a mass shooting. Millions of people joined groups and followed pages related to QAnon, a conspiracy theory holding that the world is controlled by a cabal of Satan-worshipping, pedophilic Democrats. The First Amendment has made it difficult for the U.S. government to stop toxic ideas from spreading online. Germany passed a law attempting to curb the dissemination of hate speech, but it is enforceable only within the country’s borders. As a result, Facebook has been left to make difficult decisions about speech largely on its own.

Over time, the company has developed a set of rules and practices in the ad-hoc manner of common law, and scholars have long argued that the system needed more transparency, accountability, and due process. The idea for the Oversight Board came from Noah Feldman, a fifty-year-old professor at Harvard Law School, who has written a biography of James Madison and helped draft the interim Iraqi constitution. In 2018, Feldman was staying with his college friend Sheryl Sandberg, the chief operating officer of Facebook, at her home in Menlo Park, California. One day, Feldman was riding a bike in the neighboring hills when, he said, “it suddenly hit me: Facebook needs a Supreme Court.” He raced home and wrote up the idea, arguing that social-media companies should create “quasi-legal systems” to weigh difficult questions around freedom of speech. “They could cite judicial opinions from different countries,” he wrote. “It’s easy to imagine that if they do their job right, real courts would eventually cite Facebook and Google opinions in return.” Such a corporate tribunal had no modern equivalent, but Feldman noted that people need not worry: “It’s worth recalling that national legal systems themselves evolved from more private courts administered by notables or religious authorities.” He gave the memo to Sandberg, who showed it to Zuckerberg. For a few years, Zuckerberg had been thinking about establishing a “legislative model” of content moderation in which users might elect representatives to Facebook, like members of Congress. A court seemed like a better first step.

In November, 2018, Feldman gave a short presentation to Facebook’s corporate board, at Zuckerberg’s invitation. “I didn’t feel like I was convincing my audience,” he told me. Feldman recalled that some members felt such a body wouldn’t sufficiently improve the company’s legitimacy; others worried that it could make decisions that would contradict Facebook’s business interests. A few minutes in, Zuckerberg defended the proposal. He noted that a huge proportion of his time was devoted to deliberating on whether individual, high-profile posts should be taken down; wouldn’t experts be better at making those decisions? The idea remained controversial, but Facebook’s corporate structure allows Zuckerberg to make unilateral decisions. Soon after, he ordered the project to begin. “I was kind of stunned,” Feldman told me. “Like, holy shit, this is actually going to happen.”

One day in June, 2019, an Uber dropped me off at Facebook’s campus, in a parking lot full of Teslas. For the past couple of years, while working as a law professor, I had been researching how tech companies govern speech. That morning, I headed into MPK 21, a five-hundred-thousand-square-foot building designed by Frank Gehry, with a rooftop garden inhabited by wild foxes. (Signs discourage interaction with them.) Walls are plastered with giant posters bearing motivational phrases like

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

"Nothing at Facebook Is Somebody Else's Problem" and "The Best Way to Complain Is to Make Things." When you visit, you register at a touch-screen kiosk and sign a nondisclosure agreement pledging that you won't divulge anything you see. The company knew that I was coming as a reporter, but the woman at the desk didn't know how to print a pass without a signed agreement; eventually, another employee handed me a lanyard marked "N.D.A." and said, "We'll just know that you're not under one."

I began by shadowing Facebook's Governance and Strategic Initiatives Team, which was tasked with creating the board. The core group was made up of a dozen employees, mostly in their thirties, who had come from the United Nations, the Obama White House, and the Justice Department, among other places. It was led by Brent Harris, a former consultant to nonprofits who frequently arrived at our meetings eating a granola bar. The employees spent much of their time drafting the board's charter, which some called its "constitution," and its bylaws, which some called its "rules of the court." During one meeting, they used pens, topped with a feather, to evoke the quills used by the Founding Fathers.

The group was young and highly qualified, but it was surrounded by tech executives who sometimes became actively involved. Early drafts of the charter included a lot of dry, careful legal language, but in later versions some of it had been stripped out. "Feedback is coming from people high in the company, who are not lawyers," Harris told me, during one meeting. I noted that someone had changed all references to "users" in the charter to "people," which seemed to imply that the board governed not only Facebook's customers but everyone in the world. Harris exchanged glances with another employee. "Feedback is coming from people *very* high in the company," he said. I later learned from the team that Zuckerberg had been editing the charter to make it "more approachable."

Employees on the governance team sometimes referred to themselves as "true believers" in the board. Kristen Murdock, who was an intelligence officer in the Navy before coming to Facebook, told me, "This is going to change the face of social justice on the Internet." But some executives did not hold it in the same regard. Elliot Schrage, then the head of global policy and communications, told people involved that he was skeptical of the project and did not think it could be improved. (Schrage claimed, through a spokesperson, that he was "fully supportive of efforts to improve governance" but that he "did have concerns about how to build a credible program.") Nick Clegg, a former Deputy Prime Minister of the U.K. who was supervising the governance team, told me, in 2019, that he was reluctant to let the board weigh in on sensitive topics, at least early on. "I would love to think that we'd have a relatively uncontroversial period of time," he said. At one point, a director of policy joked about ways to make the board seem independent, asking, "How many decisions do we have to let the Oversight Board win to make it legit?"

In time, the workings of the court came together. The board originally included twenty members, who were paid six-figure salaries for putting in about fifteen hours a week; it is managed by an independent trust, which Facebook gave a hundred and thirty million dollars. ("That's real money," a tech reporter texted me. "Is this thing actually for real?") According to Facebook, as many as two hundred thousand posts become eligible for appeal every day. "We are preparing for a fire hose," Milancy Harris, who came to the governance team from the National Counterterrorism Center, said. The board chooses the most "representative" cases and hears each in a panel of five members, who remain anonymous to the public. Unlike in the Supreme Court, there are no oral arguments. The user submits a written brief arguing her case; a representative for the company—"Facebook's solicitor general," one employee joked—files a brief explaining the company's rationale. The panel's decision, if ratified by the rest of the members, is binding for Facebook.

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

The “most controversial issue by far,” Darmé told me, was how powerful the board should be. “People outside the company wanted the board to have as much authority as possible, to tie Facebook’s hands,” she said. Some wanted it to write all of the company’s policies. (“We actually tested that in simulation,” Darmé said. “People never *actually* wrote a policy.”) On the other hand, many employees wondered whether the board would make a decision that killed Facebook. I sometimes heard them ask one another, in nervous tones, “What if they get rid of the newsfeed?”

As a result, the board’s powers were limited. Currently, users can appeal cases in which Facebook has removed a post, called “take-downs,” but not those in which it has left one up, or “keep-ups.” The problem is that many of Facebook’s most pressing issues—conspiracy theories, disinformation, hate speech—involve keep-ups. As it stands, the board could become a forum for trolls and extremists who are angry about being censored. But if a user believes that the company should crack down on certain kinds of speech, she has no recourse. “This is a big change from what you promised,” Evelyn Douek, a Harvard graduate student who consulted with the team, fumed, during one meeting. “This is the opposite of what was promised.” Users also currently can’t appeal cases on such issues as political advertising, the company’s algorithms, or the deplatforming of users or group pages. The board can take cases on these matters, including keep-ups, only if they are referred by Facebook, a system that, Douek told me, “stacks the deck” in Facebook’s favor. (Facebook claims that it will be ready to allow user appeals of keep-ups by mid-2021, and hopes eventually to allow appeals on profiles, groups, and advertising as well.)

Perhaps most important, the board’s rulings do not become Facebook policy in the way that a Supreme Court precedent becomes the law of the land. If the board decides that the company should remove a piece of content, Facebook is obligated to take down only that post; similar posts are taken down at Facebook’s discretion. (The company states that it will remove “identical posts with parallel context” based on its “technical and operational capacity.”) Policy recommendations are only advisory. This significantly narrows the board’s influence. Some hope that the recommendations will at least exert public pressure on the company. “Facebook undermines its goals and its own experiment if it restricts the impact of the board’s decisions or just ignores them,” Douek told me. Others felt let down. “It’s not what people told us they wanted,” Darmé said. “They wanted the board to have real power over the company.”

In August, 2019, the governance team met with advisers, over snacks and seltzer, and discussed who should sit on the board. A security guard stood outside, making sure that no one explored the offices unattended. (He stopped me on my way out and told me that I couldn’t leave without an escort.) The people selected for the board would determine its legitimacy, and how it ruled, but the experts had trouble agreeing on who could be trusted with this responsibility. One attendee suggested letting the first board members choose the rest, to preserve their independence from the company. Lauren Rivera, a professor at Northwestern’s business school, cautioned against this approach: “It’s empirically proven that when you have a group self-select, in the absence of any kind of guidance, they just pick more people that look like them.” The experts then began giving their own ideas. Journalists said that the board should be mostly journalists. International human-rights lawyers said that it should be all international human-rights lawyers. Information scientists said that it should be “anyone but lawyers.” A white man at a think tank said that it should be populated with “regular people.”

Ultimately, to select its would-be judges, Facebook opened a public portal, which received thousands of nominations. It got suggestions of candidates from political groups and civil-rights organizations. It also used its initial workshops to scout potential candidates and observe their behavior. “The thing about the global consultancy process is that it was also maybe Facebook’s first

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

true global recruiting process," Brent Harris told me later. Jarvis, the journalism professor at the New York workshop, said, "It's so Facebook of them." He added, "They never called me. I wonder what I said."

The number of people that Facebook planned to have on the board kept changing. I imagined the team sweating over a "Law & Order"-style corkboard of photographs. At one point, Kara Swisher, a tech journalist who has been critical of Facebook, nominated herself. "I would like to formally apply to be judge and jury over Mark Zuckerberg," she wrote in the *Times*. Facebook didn't take her up on it. A reporter sent me an encrypted text saying he had two sources telling him that Barack Obama would be on the board. When I asked Fariba Yassaee, who oversaw the search for members, about high-profile candidates, she smiled. "The people we're looking at are incredibly impressive, but they also are able to do the hard work that being on the board will entail," she said. "They need to be team players." In May, the first board members were announced. They included Helle Thorning-Schmidt, a former Prime Minister of Denmark; Catalina Botero Marino, a former special rapporteur for freedom of expression to the Inter-American Commission on Human Rights; Alan Rusbridger, the former editor of the *Guardian*; and Tawakkol Karman, an activist who won the Nobel Peace Prize, in 2011, for her role in Yemen's Arab Spring protests.

The slate was immediately controversial. Some employees were angry about the appointment of Michael McConnell, a retired federal judge appointed by George W. Bush. In 2000, McConnell argued before the Supreme Court that the Boy Scouts should be allowed to exclude gay people. (This year, during a Zoom class at Stanford Law School, he recited a quote that included the N-word. He defended this as a "pedagogical choice," but pledged not to use the word again.) "We all knew what people outside and inside the company were expecting: board members who respect all people and all cultures, including respect for L.G.B.T.Q. rights," Darmé, who had since left Facebook, told me. "Can you really have someone on the board who's argued something like this all the way to the highest court in the land?" Others believed that, considering that half of the country is Republican, disregarding such views would be undemocratic. "It is not a thing you can really say right now, but the vast majority of the world is much more ideologically conservative than Menlo Park," Harris said. "How do you reflect that on the board? Or do you decide, No, we're just not going to have that?"

People familiar with the process told me that some Republicans were upset about what they perceived to be the board's liberal slant. In the months leading up to the appointments, conservative groups pushed the company to make the board more sympathetic to Trump. They suggested their own lists of candidates, which sometimes included members of the President's family, most notably Ivanka and the President's sons. "The idea was, either fill this board with Trump-supporting conservatives or kill it," one person familiar with the process said. In early May, shortly after the board members were announced, Trump personally called Zuckerberg to say that he was unhappy with the makeup of the board. He was especially angry about the selection of Pamela Karlan, a Stanford Law professor who had testified against him during his first impeachment. "He used Pam as an example of how the board was this deeply offensive thing to him," the person familiar with the process said. Zuckerberg listened, and then told Trump that the members had been chosen based on their qualifications. Despite the pressure from Trump, Facebook did not change the composition of the board. (Trump declined to comment.)

Several candidates declined to be considered. Jameel Jaffer, the director of the Knight First Amendment Institute, told me, "I was worried, and still am, that Facebook will use membership on the board as a way of co-opting advocates and academics who would otherwise be more critical of the company." But others saw it as a way to push Facebook in the right direction. Julie Owono, a board member and the head of Internet Sans Frontières, told me, "I had expressed interest in joining the board because I feel, and still do, that Facebook is doing a terrible job on hate speech in environments that are already very tense." Thorning-Schmidt, the

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

former Prime Minister of Denmark, told me, "I needed to know this would be independent from Facebook and that Facebook would commit to following our decisions." She met with Zuckerberg and asked that he give his word: "I had to hear it from Mark Zuckerberg myself. And he said yes."

Critics of the board believe that it will prove to be little more than a distraction. "I think it's a gigantic waste of time and money," Julie Cohen, a law professor at Georgetown, said. She believes that its star-studded panel and lavish funding will prevent regulation while allowing the company to outsource controversial decisions. And, since it can currently rule only on individual posts, the board can't address Facebook's most fundamental problems. In mid-May, for example, a video called "Plandemic," which claimed that vaccine companies had created COVID-19 in order to profit from the pandemic, went viral on the platform. It was taken down within a few days, but by that time it had already been seen by 1.8 million people. Ellen P. Goodman, a law professor at Rutgers, believes that Facebook needs to add more friction to the circulation of content; anything catching fire, she said, should be subject to a "virality disruptor" that stops further spread until the content has been reviewed. Zephyr Teachout, a law professor at Fordham, says that the company should do away with targeted advertising, which incentivizes the promotion of incendiary, attention-grabbing posts. "If the core of our communications infrastructure is driven by targeted ads, we will have a toxic, conflict-driven communications sphere," she said. She also argues that the company is too big and needs to be broken up through antitrust litigation.

This summer, I spoke with Zuckerberg over Zoom. He wore a Patagonia fleece and sat in a wood-panelled room in front of a large marble fireplace. He had been heavily involved in the board's creation: editing documents, reading memos, reviewing possible members. "I don't see any path for the company ever getting out of the business of having to make these judgments," he told me. "But I do think that we can have additional oversight and additional institutions involved." He hoped, he said, that the board would "hold us accountable for making sure that we actually get the decisions right and have a mechanism for overturning them when we don't."

He looked tired. He seemed more at ease talking about "product" or "building tools" than he did discussing ethics or politics. It struck me that he was essentially a coder who had found himself managing the world's marketplace of ideas. "The core job of what we do is building products that help people connect and communicate," he said. "It's actually quite different from the work of governing a community." He hoped to separate these jobs: there would be groups of people who built apps and products, and others—including Facebook's policy team and now the board—who deliberated the thorny questions that came along with them. I brought up a speech he gave at Georgetown, in 2019, in which he noted that the board was personally important to him, because it helped him feel that, when he eventually left, he would be leaving the company in safe hands. "One day, I'm not going to be running the company," he told me. "I would like to not be in the position, long term, of choosing between someone who either is more aligned with my moral view and values, or actually is more aligned with being able to build high-quality products."

I asked what kinds of cases he hopes the board will take. "If I was them, I'd be wary of choosing something that was so charged right off the bat that it was immediately going to polarize the whole board, and people's perception of the board, and society," he told me. He knew that critics wished the board had more power: "This is certainly a big experiment. It's certainly not as broad as everyone would like it to be, upfront, but I think there's a path for getting there." But he rejected the notion that it was a fig leaf. "I'm not setting this up to take pressure off me or the company in the near term," he said. "The reason that I'm doing this is that I think, over the long term, if we build up a structure that people can trust, then that can help create legitimacy and create real oversight. But I think there is a real risk, if it gets too polarized too quickly, that it will never be able to blossom into that."

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

In April, 2020, the board members met for the first time, over Zoom. Facebook employees cried and took a screenshot. "It was such a profound experience to see this thing take on a life of its own," Heather Moore, who came to Facebook from a U.S. Attorney's office, said. After that, board members attended training sessions, which included icebreakers and trust exercises; in one, they brought pictures that represented pivotal moments in their lives. "Whether we can get along well enough to disagree and stay on mission is crucial and quite unknown," John Samples, a member who works at the Cato Institute, a libertarian think tank, told me. The group quickly came under intense public pressure to stand up to the company. In June, a nonprofit called Accountable Tech began targeting the board on Facebook with ads that included their photos and addressed them by name: "Pam Karlan: speak up or step down"; "Tell Michael McConnell: don't be complicit." Members often felt the need to assert their independence. The company assigned readings, some of which were, according to a board member, "just P.R. crap from Facebook," and employees sat in on early meetings and mock deliberations. "We're out of our mind if we're in an oversight position and the people who are teaching us about what we're overseeing are the people we're meant to oversee," the board member said. After complaints, Facebook employees stopped being invited to the meetings.

In October, Facebook began allowing appeals from a random five per cent of users, like a new Instagram feature, and the board's jurisdiction was rolled out over the next month. Its docket included a post from an American user about Joseph Goebbels, the Nazi minister of propaganda, and one from a user in Myanmar claiming that there is "something wrong with Muslims psychologically." Owono told me, "I never imagined I'd have to ask myself these kinds of hard questions so rapidly." They reviewed the company's Community Standards, a ten-thousand-word document that codifies Facebook's speech policies, and consulted precedents in international human-rights law. One debate that has arisen among board members mirrors the division on the Supreme Court between "textualist" and "living" interpretations of the Constitution. Some believe that their job is to hew more closely to Facebook's policies. "Our job is to ask, 'What does the text mean?'" one member told me. "We don't have much legitimacy if we just start making stuff up." Others believe that they should use their power to push back against Facebook's policies when they are harmful. Nicolas Suzor, a law professor from Australia, and a board member, told me, "I was worried we'd end up with decisions that were limited to the facts, but people are brave."

In one of the board's first cases, a user had posted photos and described them as showing churches in Baku, Azerbaijan, that had been razed as part of the ongoing persecution of Armenians in the region. He complained about "Azerbaijani aggression" and "vandalism," and referred to Azerbaijanis using the word "*taziki*," which literally means "washbowls" but is a play on a Russian slur. Facebook had taken down the post as hate speech, but some board members felt that it was strange to apply this rule to a complaint against a dominant group. The panel asked for a report from UNESCO, received a comment from the U.N. special rapporteur on minority issues, and another from a think tank in Ukraine, who told them that persecuted groups often used offensive language in their struggle for equality. "We learned that, during a conflict, it's usually accepted that people would use harsh words, so there's this idea that, especially when minority rights are at risk, there's a custom to allow more harsh discourse," a board member told me. "I'd never heard of that before, and I found it compelling." In the end, they voted to take the post down, though not everyone agreed. The opinion suggested that a minority of the members "believed that Facebook's action did not meet international standards and was not proportionate," and that the company "should have considered other enforcement measures besides removal."

In another case, someone in France had posted a video and accompanying text complaining that the government had refused to authorize a combination of azithromycin and hydroxychloroquine, an anti-malarial drug, as a treatment for COVID-19. Many on the right, including Trump and the French professor Didier Raoult, have claimed that hydroxychloroquine cures the illness,

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

though the claim has been debunked, and scientists have warned that the medication can cause dangerous side effects. The user claimed that "Raoult's cure" was being used elsewhere to save lives and posted the video in a public group with five hundred thousand members. Facebook worried that it might cause people to self-medicate, and removed it. According to one person on the board, members of the panel "who have lived in places that have had a lot of disinformation in terms of COVID-19" agreed with this decision, believing that, "in the midst of this huge pandemic affecting the entire world population, decisive measures may be adopted." But others noted that the post was pressing for a policy change, and worried about censoring political discussions. "No matter how controversial it would seem to us, those questions and challenges are what helps scientific knowledge advance," the board member said. They found that Facebook's standard for censoring such speech, interpreted under international human-rights law, involved determining whether it was likely to incite direct harm. Because the combination of medicines was not available over the counter in France, they decided that the risk of causing people to self-administer was low. They voted to restore the post but encouraged the company to append a link to more reliable scientific information.

When the board was just three weeks old, Black Lives Matter protests were sweeping the country, and Trump posted on both Facebook and Twitter threatening to send in the military to subdue them, writing, "When the looting starts, the shooting starts." His language echoed that of the segregationist George Wallace, who threatened civil-rights protesters in similar terms. Twitter flagged the tweet as violating its rules against "glorifying violence," but Facebook left it unmarked. Zuckerberg released a statement saying, "I disagree strongly with how the President spoke about this, but I believe people should be able to see this for themselves." In an interview on Fox News, he noted that he didn't think the company should be the "arbiter of truth" on political issues. Angry employees staged a virtual walkout and raised the idea, in a leaked Q&A., of letting the board hear the case. A few days after the incident, Suzor, the Australian law professor, suggested a full-board meeting. Users couldn't appeal Facebook's decision to the board—it hadn't yet started taking cases, and the post was a keep-up—but it debated the issue nonetheless.

Several members were shocked by Trump's threats and initially wanted to meet with Zuckerberg or release a statement condemning the platform's decision. "I was furious about Zuck's 'arbiter of truth' double-down," one board member told me. Others felt that taking a partisan stand would alienate half the country and lose the board legitimacy. "Seventy-five million people voted for Trump," Samples said. "What are you going to do about it?" The group discussed whether it should weigh in on matters outside its remit that are nevertheless of public importance. Jamal Greene, one of the co-chairs, told me, "The general sentiment was 'no' for right now, and maybe 'no' ever, but certainly not before we're even doing the thing that we're supposed to be doing." After two hours of discussion, the members decided to stay mum. "Moralistic ranting is not going to make a difference," Samples said. "Building up an institution that can slowly answer the hard questions? That might."

They didn't have much time for institution-building. On January 6th, a group of Trump supporters who disputed the results of the Presidential election stormed the Capitol, taking selfies, making threats, and attempting to disrupt the peaceful transition of power. Trump had urged on the mob by repeatedly claiming, on Facebook and elsewhere, that the election had been stolen from him. Hundreds of thousands of people had used the site to spread the claim, and to organize the rally at the Capitol. Afterward, Trump released a video tepidly disavowing violence and reiterating his claims of a fraudulent election. He tweeted, "These are the things and events that happen when a sacred landslide election victory is so unceremoniously & viciously stripped away from great patriots who have been badly & unfairly treated for so long." Facebook removed two of Trump's posts. The next morning, in a statement from his own Facebook, Zuckerberg announced an indefinite suspension of Trump's account. "In this moment, the risk

3/24/2021

Inside the Making of Facebook's Supreme Court | The New Yorker

to our democracy was too big," Sheryl Sandberg said, in an interview. "We felt we had to take the unprecedented step of what is an indefinite ban, and I'm glad we did." The next day, Twitter permanently banned him.

Many felt that the decision was an important step. "The platforms failed in regulating the accounts, of course, since he was inciting violence, and they banned him for that only *after* egregious violence resulted," Susan Benesch, the founding director of the Dangerous Speech Project, told me. "But banning him did lower his megaphone. It disrupted his ties with his large audience." Others expressed concern that Facebook had wielded its power to silence a democratically elected leader. "The fifth most valuable corporation in the U.S., worth over seven hundred billion dollars, a near monopoly in its market niche, has restricted a political figure's speech to his thirty million followers," Eugene Volokh, a law professor at U.C.L.A., said. "Maybe that's just fine. Maybe it's even a public service. But it's a remarkable power for any entity, public or private, to have." Angela Merkel, the Chancellor of Germany, described Trump's removal from Twitter as "problematic," and Alexey Navalny, the Russian opposition leader, tweeted, "I think that the ban of Donald Trump on Twitter is an unacceptable act of censorship."

In an interview, Sandberg noted that Trump could appeal the removal of his posts. But only Facebook had the power to refer his suspension to the board. In conversations with Facebook's leadership, members of the governance team and the board's trust argued that failing to bring the case before the board would undermine its legitimacy. Harris likened the board to Tinkerbell: "At the end of the day you can build all the things, but you just have to have enough people that believe in order to make it real." Members seemed eager to take it on. One texted me, "If not us, who? And if not now, when?" Even Clegg, who had initially favored a slower rollout of the board, wanted it to hear the case. "As far as I'm concerned, this was a no-brainer," Clegg told me. "Why wouldn't you send it to the Oversight Board? If you didn't, you'd be hobbling it right from the beginning." The day after Joe Biden's Inauguration, Facebook sent the case, asking the board to rule on whether Trump should remain indefinitely banned from the platform. Clegg added, when we spoke, that if the board can "answer also about political leaders in analogous situations, we'd be keen to hear."

Board members found out that they were getting the case only a half hour before the public did. Members eagerly watched the board's internal Web site to see if they had been selected for the panel. They will now have two more months to deliberate it. Civil-society groups like the Center for Democracy & Technology and R Street, a conservative think tank, are submitting comments on the case—the equivalent of filing *amicus* briefs—arguing for or against Trump's reinstatement. Trump has the opportunity to submit a brief arguing why he should be reinstated. "The board's Trump decision may affect the liberties and, yes, lives of hundreds of millions," Samples told me. "Few U.S. Supreme Court cases ever hold such potential for good or for ill." Ronaldo Lemos, a board member and law professor in Rio de Janeiro, told me that he believes the board has a lot of work ahead. "The Oversight Board is not going away anytime soon," he said. "We're not going anywhere."

READ MORE ABOUT THE ATTACK ON THE CAPITOL

- A reporter captures the siege on video.
- John Sullivan claims that he attended the insurrection as a journalist. Others believe he urged the mob on.
- Unmasking the Bullhorn Lady, a Pennsylvania mother of eight who became a fugitive from the F.B.I.



PROPOSAL FOR A SOCIAL MEDIA STANDARDS BOARD

Introduction

The Coalition for a Safer Web (www.coalitionsw.org) (CSW) was established in 2019 to develop innovative policy and technological solutions to accelerate the permanent de-platforming of hate and extremism content from social media platforms. CSW is a non-partisan, not-for-profit 501(c)(3) organization whose advisory board is chaired by Gov. Tom Ridge, first U.S. Secretary for Homeland Security. CSW's founding President is former U.S. Ambassador Marc Ginsberg.

Since its inception CSW has many undertaken ground-breaking initiatives, including:

- **TELEGRAM App:** Commencing a global policy initiative to curtail the role of the mobile app “TELEGRAM” as the principal conveyor of terrorist, anti-Semitic, and racist incitement instigated by transnational extremist groups.
- **RUSSIA & “THE BASE”:** Uncovered the role which the Russian Government is playing to support the operations from St. Petersburg of Rinaldo Navarro – the purported leader of the most violent neo-Nazi terrorist group known as “The Base.”
- **“THE VIRUS OF ANTI-SEMITISM FEEDS OFF THE “JEW FLU””:** CSW’s “Special Report” details how the Covid-19 pandemic has been leveraged by Russian-backed neo-Nazi groups by fabricating anti-Semitic conspiracies and tropes implying Jews are responsible for spreading the corona virus.
- **“NATIONAL STRATEGY TO COMBAT HATE & EXTREMISM”:** CSW issued a report proposing specific recommendations for Congress and presidential candidates to consider to expedite de-platforming extremist incitement from social media sites.
- **HOLDING TECH INFRASTRUCTURE COMPANIES ACCOUNTABLE:** In conjunction with the LawFare Project, CSW has developed an international strategy to hold accountable the tech support companies vital to enabling fringe extremist groups to operate on the web.

Executive Summary: Social Media Standards Board

CSW proposes a ground-breaking private sector, voluntary Social Media Standards Board (SMSB) which would serve as: 1) a private/public sector voluntary auditing organization to monitor compliance by social media companies of a new "code of conduct"; and 2) a forum to incubate and promote new technologies to accelerate identification and management of extremist/hate social media content to assist social media companies to fulfill their own customer obligations and public pledges to de-platform extremist content.



The SMSB is loosely modeled after the successful banking industry's Financial Accounting Standards Board (FASB). The SMSB would represent a voluntary initiative among social media companies, the digital advertising industry, concerned citizens groups, and Congress which would oversee development and compliance with a new social media industry-wide code of conduct, the violation of which result in financial penalties and the possible loss of content immunity under Section 230 of the Communications Decency Act of 1996 (Section 230).

Section 1: Why Create a Social Media Standards Board?

The American people are increasingly victimized by the unaccountability of social media platforms for the unsafe and extremist content uploaded daily on their platforms. Although Section 230 grants blanket legal immunity from content liability, major social media platforms are increasingly censoring the very content they profess they are under no legal duty to monitor. Their decisions to leave up or take down content are haphazard and subjective, without any industry-wide policy guard rails or consistent, accountable third-party monitoring. An entire industry of non-profit organizations has materialized in recent years to shine a light on social media deficiencies.

Despite deploying new technologies and recruiting thousands of content moderators, the terrain of social media content moderation resembles the Wild West. Silicon Valley is determined to preserve its immunity under Section 230, but acknowledges that it is being overwhelmed by adverse content and by an avalanche of demands to make their platforms safer and their content monitoring decisions more transparent.

Facebook recently unveiled a new quasi-independent global "Oversight Board" to adjudicate de-platorming decisions. Whatever may be its merits, Facebook executives reserve to themselves final decisions over content. Meanwhile, no other mainstream social media platform has created such an "oversight board." The interpretation of each company's terms of service and customer agreement is undertaken by nameless, faceless, private sector bureaucrats.

Meanwhile, in Europe, Australia and New Zealand, a new regime of laws has been enacted compelling social media companies to submit to government accountability or face major fines for their failures to cleanse their platforms of illicit content. In some new legal regimes social media executives may be subjected to criminal prosecution for failing to comply with these new laws.

The trans-Atlantic divide over social media accountability could not wider.



As Congress considers many legislative proposals to impose more social media accountability --- in the areas of data privacy, political censorship, illicit sale of products, or incitement to violence --- the public's safety is increasingly at risk.

There are no easy answers to the nation's social media challenges.

On July __, 2020, The Hill newspaper published a [CSW op ed](#) entitled “Facebook Ad Boycott is unlikely to solve the problem – a social media standards board would.” Public demand for reform and regulation of social media platforms has dramatically escalated, but there is little consensus in Congress or in the Executive Branch what form reform and regulation should take. Meanwhile, the #StopHateForProfit coalition ad boycott's recommendations to Facebook were rebuffed by Mark Zuckerberg, leaving the digital ad industry uncertain what their ad boycott will achieve.

Facebook's refusal to consider the coalition's reasonable recommendations coupled with Congress' inability to reach consensus how to hold social media companies accountable compelled CSW to undertake a review of existing private sector organizations which have succeeded in promoting voluntary, private sector solutions in industries where arbitrary and dysfunctional compliance with desirable harmonized standards was deficient.

Sometimes, government intervention compelled industries to bring order out of chaos; other times industries recognized the urgent need to voluntarily self-regulate because of public pressure and corporate interest.

Highly respected Silicon Valley entrepreneur turned social media critic Roger McNamee correctly observed that hate speech, conspiracy theories, misinformation, rabid political discourse, and illegal product sales have all served as “...the lubricant for their business” because it drives up customer usage, and thus, digital ad sales McNamee. No wonder when it comes to reducing dangerous content social media executives wind up taking down the bare minimum to keep their critics at bay.

Section 2: The Financial Accounting Standards Board as a SMSB Model

Established in 1973, the Financial Accounting Standards Board (FASB) is the independent, private-sector, not-for-profit organization based in Norwalk, Connecticut, which establishes financial accounting and reporting standards for public and private companies and not-for-profit organizations that follow Generally Accepted Accounting Principles (GAAP). The FASB is funded via annual grants from its banking industry stakeholders.

The FASB is recognized by the Securities and Exchange Commission as the designated accounting standard setter for public financial companies. FASB standards are recognized



as authoritative by many other organizations, including state Boards of Accountancy and the American Institute of CPAs (AICPA). The FASB develops and issues financial accounting standards through a transparent and inclusive process intended to promote financial reporting that provides useful information to investors and others who use financial reports.

The FASB created a new collaborative initiative between the financial and banking industry and a non-governmental oversight organization which harmonized disparate industry accounting and reporting standards into a coherent, transparent system of standards.

The following is lifted from the FASB Website:

FASB MISSION

The collective mission of the FASB, the Governmental Accounting Standards Board (GASB) and the Financial Accounting Foundation (FAF) is to establish and improve financial accounting and reporting standards to provide useful information to investors and other users of financial reports and educate stakeholders on how to most effectively understand and implement those standards.

The FASB, the GASB, the FAF Trustees, and the FAF management contribute to the collective mission according to each one's specific role:

- The FASB and the GASB are charged with setting the highest-quality standards through a process that is robust, comprehensive, and inclusive.
- The FAF management is responsible for providing strategic counsel and services that support the work of the standard-setting Boards.
- The FAF Trustees are responsible for providing oversight and promoting an independent and effective standard-setting process. Transforming the FASB Model to Promote Private Sector Social Media Customer Standards Harmonization

Section 3: The Digital Advertising's Global Alliance for Responsible Media

CSW proposes forming a SMSB working group to develop a plan of action to kickstart the launch of the SMSB among social media companies, and representatives of the Global Alliance for Responsible Media (GARM) — an initiative of digital corporate advertisers, major U.S. corporations, and public advocacy organizations.

GARM is a new digital advertising concept to voluntarily compel social media companies to better protect corporate brands from migrating onto illicit and extremist content. The symbiotic relationship between social media companies and digital advertisers results in



billions of dollars of ad revenue generated for social media companies. In recent years, many digital consumer advertisers, notably AT&T, Nestle, and others have withheld digital advertising purchases due to the proliferation of purchased advertising appearing on illicit and extremist content. The 2020 Facebook ad boycott is the latest iteration of public pressure being exerted on digital advertisers to withhold ad buys from major social media platforms.

GARM is a welcome corporate ad industry initiative, but it would greatly benefit from a durable structure to adequately fulfill its mission. GARM's creators envision a new code of conduct to establish new "rules of road" by which social media companies would prevent corporate brand contamination from appearing on extremist and illegal content.

Most importantly, GARM's concept behind a new code is to establish industry-wide standards governing technological goals to accelerate extremist content de-platforming and compel more transparency in the metrics social media companies could and should adopt to assuage consumers, impacted private companies, and the U.S. government of the progress (or lack thereof) they are achieving to meet their own extremist content de-platforming customer terms of service and public pledges.

Section 4: The SMSB Represents a Private Sector Remedy to a Public Safety Challenge

CSW is fully cognizant that social media companies have no legal or regulatory obligation to cooperate to create a SMSB. Indeed, their track record to date is to avoid any third-party, independent oversight of their content and zig-zagging moderation policies. Convincing them to test pilot a SMSB for an initial 2-3 years will require leveraging the threat of potential loss of Section 230 immunity, Congressional and state regulation, the digital advertising ecosystem's financial influence over social media companies, and concerned stakeholders, including corporate shareholders.

Digital corporate advertisers either directly via the GARM or independently — have not endorsed a SMSB. However, the GARM's advertising liaisons have requested CSW to submit the SMSB proposal to it for its consideration.

Moreover, the proposed SMSB is NOT a Congressionally mandated public regulatory institution. However, Congress' role as a recipient of SMSB recommendations and reports is vital. Without the leverage of Congressional support and impetus social media companies may refuse to expose themselves to oversight even to a watchdog organization they themselves must help create.



Section 5: The Role of Section 230 in a SMSB Sanctions Regime

Congress' leverage to bring social media companies to the SMSB table exists via Section 230 enforcement and the SMSB's effectiveness depends, in part, on Congress' review of SMSB audit reports.

The SMSB proposal envisions passage by Congress of an amendment to Section 230 delegating to the SMSB the power to suspend Section 230 immunity until a violating social media company restores its compliance with new industry code of conduct. The loss of Section 230 immunity would represent the ultimate penalty imposed on code violators for sustained violations. Lesser sanctions against social media companies imposed by the SMSB code could conceivably include: 1) de-certification from code compliance; 2) forfeiture of digital ad revenue; and 3) a referral by the SMSB for administrative action to the Federal Trade Commission.

Section 6: Overview of Proposed SMSB Mission & Administrative Structure

The SMSB is to serve as a "mission control" to undertake the following public policy goals and objectives:

1. Establish a third party, independent content moderation board to oversee social media company compliance with a new industry-wide code of conduct to be drafted by SMSB stakeholders (social media companies, the digital advertising industry, and concerned citizens groups).
2. Provide the SMSB content moderation board the authority to propose harmonizing the respective terms of service and customer agreements of social media companies with the new industry-wide code of conduct.
3. Determine whether social media companies are maintaining compliance with a code of conduct (i.e., via a certification of compliance issued by the SMSB).
4. Develop a SMSB management architecture, to include:
 - Executive management and content moderation staff oversight structure
 - Schedule for submitting to the public and Congress regular reports detailing code compliance and code violations committed by social media companies and actions taken by the SMSB against violations.
 - Initial annual budget
 - SMSB mission statement
 - Code of conduct sanctions and remedies to provide enforcement authority for the code of conduct (including revoking Section 230 immunity).



Participating social media companies (as defined) would enjoy a presumption of compliance if they are "certified" by the SMSB, but presumption would be overcome by showing of willful and knowing or grossly negligent compliance of a code of conduct.

Section 7: Model SMSB Structure

SMSB Compliance Board Qualifications

- No board member shall have any financial interest in a regulated entity, or have served as an employee, consultant, agent, or adviser for two years prior to service. • Nine (9) Members:
 - a. 2 extremist/incitement content experts.
 - b. 2 technology innovation experts.
 - c. 2 representatives from regulated entities to be designated by a social media advisory committee made up of social media companies and web infrastructure management companies.
 - d. 2 representatives from the digital corporate advertising ecosystem (to be designated by the GARM (Global Alliance for Responsible Media) industry group.
 - e. One representative from a citizen advocacy organization knowledgeable in Section 230 issues and extremist and hate speech/incitement.

SMSB Staff

- The Compliance Board shall appoint such staff as may be required to undertake the auditing and prepare compliance reports under the direction of a SMSB Executive Director (ED) who shall report to the Compliance Board. The qualifications and requirements of the ED shall be approved by a Compliance Board.

Web Content Voluntarily Subject to Independent Analysis

- A SMSB Compliance Board shall establish web content parameters to be subject to code regulation and audit focused exclusively on content deemed in support of extremism, incitement, hate and instruction content in support thereof.



SMSB Budget

- An annual budget shall be derived from contributions from social media corporate members and the GARM pursuant to a budget proposed by the Board. Failure to timely meet required donations shall result in loss of certification.

Operational Parameters

- Certification/Compliance/Monitoring/Enforcement

Certification issued bi-annually

- + Annual compliance reviews/audits
- + Interim special code compliance reviews triggered by majority vote of Compliance Board.
- + Annual audit reports
- + Determination and issuance of fines and revocation of "certification."
- + Code standard compliance monitored regularly by staff reporting to Compliance Board.
- +Certification (suspension or revocation) to be published by the SMSB AND prominently displayed by regulated entities.

####

3/25/2021

Tech Companies Detect a Surge in Online Videos of Child Sexual Abuse - The New York Times

The New York Times**Tech Companies Detect a Surge in Online Videos of Child Sexual Abuse**

In a first, videos outnumbered photos in reports to the authorities last year. Facebook found the most imagery, the bulk of it on its Messenger app.



By Gabriel J.X. Dance and Michael H. Keller

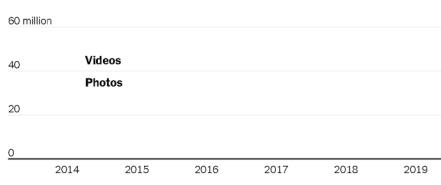
Published Feb. 7, 2020 Updated Feb. 20, 2020

The number of reported photos, videos and other materials related to online child sexual abuse grew by more than 50 percent last year, an indication that many of the world's biggest technology platforms remain infested with the illegal content.

Nearly 70 million images and videos were reported to the National Center for Missing and Exploited Children, a federally designated clearinghouse for the imagery that works with law enforcement agencies.

The record number was driven by a surge in illegal videos, which have always been popular among sexual predators but are now more readily detected by some companies. Over 41 million videos were reported; the number five years ago was under 350,000. The companies flagged many of the same images and videos multiple times as they were shared among users.

In 2019, there were more videos of abuse reported than photos



Source: National Center for Missing and Exploited Children • By Rich Harris

The center identified to The New York Times the companies that had detected the imagery, the first time detailed company information had been released.

Facebook reported nearly 60 million photos and videos, more than 85 percent of the total. The number reflects both its immense user base and its aggressive approach to routing out the material, but shows that offenders continue to exploit the platform. About half of the content was not necessarily illegal, according to the company, and was reported to help law enforcement with investigations. Instagram, owned by Facebook, was responsible for an additional 1.7 million photos and videos.

In a statement, Antigone Davis, Facebook's global head of safety, said "the size and expertise of our team, together with our sophisticated technology, have made us industry leaders in detecting, removing and reporting these images, and thwarting people from sharing them."

"We will continue to develop the best solutions to keep more children safe," she added.

Snapchat, Twitter and other social media companies also submitted reports of imagery. So did companies whose services include search engines and cloud storage, including Google and Microsoft. Apple, Dropbox and the chat platform Discord also detected the illegal content.

In all, 164 companies submitted reports.

"These numbers show that any service provider that allows individuals to host images and videos are susceptible to child sexual exploitation material being posted," said John Shehan, a vice president at the national center.

He confirmed the numbers released on Friday reflected all content reported to the center, including material that "may not meet the legal definition of child pornography."

Still, the numbers do not paint a complete picture of the problem: The industry has been plagued by uneven and inconsistent detection practices, as The Times reported last year. Some cloud storage services, including those owned by Amazon and Microsoft, do not scan for any of the illegal content at all, while other companies, like Snap, scans for photos but not videos.

3/25/2021

Tech Companies Detect a Surge in Online Videos of Child Sexual Abuse - The New York Times

The data shows broad disparities in the tech industry. Google reported more than 3.5 million combined images and videos; Yahoo more than two million; and Imgur, a photo-sharing site, more than 260,000. Dropbox, Microsoft, Snap and Twitter are the only other companies that reported more than 100,000 images and videos last year.

Apple reported dramatically fewer images than most other tech giants, just over 3,000 in total, and zero videos. These figures reflect the company's inability to scan material sent through its messaging app, which is encrypted, as well as the fact that it does not scan its file storage service, iCloud. Amazon, whose cloud services handle millions of uploads and downloads every second, sent no images or videos to the national center.

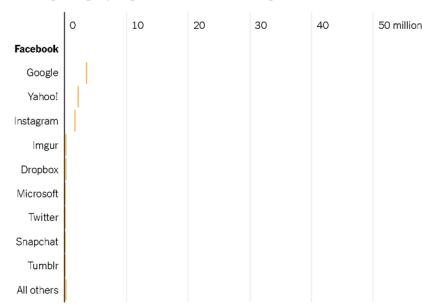
Senator Richard Blumenthal of Connecticut, who has sponsored child protection legislation and was recently part of a bipartisan group of lawmakers who asked 36 tech companies to detail their efforts in this area, called the numbers "appalling and astonishing."

"The disparate data reported here shows that we clearly cannot rely on tech companies to self-police," he said.

Alex Stamos, who served as chief of information security at both Facebook and Yahoo, said the numbers were a reflection of companies that have put more effort into finding and removing the material from their platforms.

"I hope these numbers encourage people to do more, not less," Mr. Stamos said.

Among imagery reported from tech companies, Facebook dominates



Source: National Center for Missing and Exploited Children • By Rich Harris

Last year, there was actually a decrease in the total number of reports filed with the national center, falling to 16.9 million from 18.4 million in 2018. That was at least in part because tech companies improved their reporting process by bundling photos and videos instead of flagging them individually.

A single report usually includes multiple photos and videos — for example, when the material is found in someone's email account — so the overall growth in reported imagery may signal "those that are sharing it are sharing in larger volumes," said Mr. Shehan of the national center.

Some companies that made a small number of reports ended up finding a large volume of imagery. Dropbox, for instance, made roughly 5,000 reports last year but found over 250,000 photos and videos. For victims of child sexual abuse, the recirculating imagery can cause lasting trauma. Online offenders are known to seek out children in the photos and videos, even into adulthood. Victims, or the parents of abused minors, also receive legal notices when their images are found during investigations, serving as constant reminders of their pain.

"To know that these images are online and that other people are enjoying your degradation for sexual gratification in some ways means you are forever being abused," said Alicia Kozakiewicz, a survivor of child sexual abuse who has been a longtime internet safety educator.

The growth in reported imagery, however, does not offer insights into whether more of the illegal content is being newly produced and posted online. Most imagery is detected by tech companies through automated scans that only recognize previously flagged material. And detecting videos, which last year for the first time surpassed the number of photos, is particularly difficult because the industry lacks a common standard for identifying them.

The number of reported videos spiked in 2018 when Facebook ramped up its detection efforts. The company was responsible for more than 90 percent of reports that year, according to law enforcement officials.

3/25/2021

Tech Companies Detect a Surge in Online Videos of Child Sexual Abuse - The New York Times

The continued growth in reported images from Facebook is sure to increase pressure on the company, which has been generally lauded for finding and reporting the content, but announced last year that it intended to encrypt its Messenger app. In 2019, Messenger was responsible for over 80 percent of all reports made by Facebook. Encryption would make it much more difficult to detect the illegal imagery on Messenger, which was also the largest source of reported material in 2018.

In September, The Times reported that the number of reports to the national center had grown exponentially, and that the federal response was lacking despite a 2008 law meant to address what was then called an “epidemic.” Throughout the country, law enforcement groups charged with investigating the crimes have been overwhelmed.

Legislation introduced in December would extend the length of time companies are required to retain information about illegal imagery in order to give law enforcement more opportunity to investigate. A bipartisan group of lawmakers said the bill was in response to a Times investigation revealing that cases often went cold after companies deleted the data. A draft of other proposed legislation is aimed at making companies follow a set of best practices to police imagery on their platforms or risk greater legal liability.

Even as the number of reported images and videos continues to grow, it remains difficult to assess the scope of the problem. While more companies are making efforts to detect the content, encrypted technologies and the dark web allow predators to continue trading imagery in secret.

“If all of the companies involved were looking as aggressively as Facebook, that number of reports could be 50 million or 100 million,” Mr. Stamos said.

293

3/25/2021

Thank you for posting: Smoking's lessons for regulating social media | MIT Technology Review

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

Accept Cookies

[Subscribe](#)

MIT Technology Review



Opinion

Thank you for posting: Smoking's lessons for regulating social media

Former Facebook executives admit they used the tobacco industry's playbook for addictive products. Perhaps it can also be used to undo the damage.

by **Joan Donovan**

October 5, 2020



MIT Technology Review



2 free stories remaining

[Sign in](#)

[Subscribe](#)

3/25/2021

Thank you for posting: Smoking's lessons for regulating social media | MIT Technology Review

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

 Accept Cookies

A few weeks ago, meanwhile, I was included in a discussion organized by the Computer History Museum, called [Decoding the Election](#). A fellow panelist, Hillary Clinton's former campaign manager Robby Mook, described how Facebook worked closely with the Trump campaign. Mook refused to have Facebook staff embedded inside Clinton's campaign because it did not seem ethical, while Trump's team welcomed the opportunity to have an insider turn the knobs on the social network's targeted advertising.

Taken together, these two pieces of information are damning for the future of American democracy; Trump's team openly marked 3.5 million Black Americans for deterrence in their data set, while Facebook's own staff aided voter suppression efforts. As Siva Vaidhyanathan, the author of [Anti-Social Media](#), has said for years: "The problem with Facebook is Facebook."

While research and reports from academics, civil society, and the media have long made these claims, regulation has not yet come to pass. But at the end of September, Facebook's former director of monetization, Tim Kendall, gave [testimony](#) before Congress that suggested a new way to look at the site's deleterious effects on democracy. He outlined Facebook's twin objectives: making itself profitable and trying to control a growing mess of misinformation and conspiracy. Kendall compared social media to the tobacco industry. Both have focused on increasing the capacity for addiction. "Allowing for misinformation, conspiracy theories, and fake news to flourish were like Big Tobacco's bronchodilators, which allowed the cigarette smoke to cover more surface area of the lungs," he said.

The comparison is more than metaphorical. It's a framework for thinking about how public opinion needs to shift so that the true costs of misinformation can be measured and policy can be changed.

Personal choices, public dangers

It might seem inevitable today, but regulating the tobacco industry was not an obvious choice to policymakers in the 1980s and 1990s, when they struggled with the notion that it was an individual's choice to smoke. Instead, a broad public campaign to address the dangers of *secondhand smoke* is what finally broke the industry's heavy reliance on the myth of smoking as a



MIT Technology Review



2 free stories remaining

Sign in

Subscribe

3/25/2021

Thank you for posting: Smoking's lessons for regulating social media | MIT Technology Review

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

 Accept Cookies

programs, supplementary insurance, and even hard infrastructure expenses such as ventilation and alarm systems. If these externalities hadn't been acknowledged, perhaps we'd still be coughing in smoke-filled workplaces, planes, and restaurants.

And, like secondhand smoke, misinformation damages the quality of public life. Every conspiracy theory, every propaganda or disinformation campaign, affects people—and the expense of not responding can grow exponentially over time. Since the 2016 US election, newsrooms, technology companies, civil society organizations, politicians, educators, and researchers have been working to quarantine the viral spread of misinformation. The true costs have been passed on to them, and to the everyday folks who rely on social media to get news and information.



MIT Technology Review



2 free stories remaining[Sign in](#)[Subscribe](#)

3/25/2021

Thank you for posting: Smoking's lessons for regulating social media | MIT Technology Review

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

 Accept Cookies

Response have confirmed that the fires along the West Coast are caused by dozens of arsonists.

These fires are allegedly linked to Antifa and the Riots.

FALSE CLAIM

Read this warning 



Molalla Police Department

3h · 

...

To those of you still in and around town, please report any suspicious activity (strange people walking around/looking into cars and houses/ vehicles driving through neighborhoods that don't belong there) to 911 immediately. Don't waste time posting it on FB, calling a friend or calling the non-emergency line. Call 911 immediately. The sooner we can get to the area the better chance of identifying the issue we have. A lot of rumors and posts are going around about looters. Please use caution and get us there ASAP. CALL 911.

10:24 PM · Sep 9, 2020 from Seattle, WA · Twitter for iPhone

3.1K Retweets 500 Quote Tweets 3.6K Likes



MIT Technology Review



2 free stories remaining

Sign in

Subscribe

3/25/2021

Thank you for posting: Smoking's lessons for regulating social media | MIT Technology Review

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

Accept Cookies

The costs are very real. In Oregon, fears about “antifa” are emboldening militia groups and others to set up identity checkpoints, and some of these vigilantes are using Facebook and Twitter as infrastructure to track those who they deem suspicious.

Online deception is now a multimillion-dollar global industry, and the emerging economy of misinformation is growing quickly. Silicon Valley corporations are largely profiting from it, while key political and social institutions are struggling to win back the public's trust. If we aren't prepared to confront the direct costs to democracy, understanding who pays what price for unchecked misinformation is one way to increase accountability.

Combating smoking required a focus on how it diminished the quality of life for nonsmokers, and a decision to tax the tobacco industry to raise the cost of doing business.

Now, I am not suggesting placing a tax on misinformation, which would have the otherwise unintended effect of sanctioning its proliferation. Taxing tobacco has stopped some from taking up the habit, but it has not prevented the public health risk. Only limiting the places people can smoke in public did that. Instead, technology companies must address the negative externalities of unchecked conspiracy theories and misinformation and redesign their products so that this content reaches fewer people. That is in their power, and choosing not to do so is a personal choice that their leaders make. 

Share



Link



Tagged

disinformation, Facebook, misinformation, Opinion

Author

 [Joan Donovan](#)



MIT Technology Review



2 free stories remaining

[Sign in](#)

[Subscribe](#)

[Support Imprimis](#)

Imprimis

Who Is in Control? The Need to Rein in Big Tech

January 2021 • Volume 50, Number 1 • Allum Bokhari

Allum Bokhari

Breitbart News



Allum Bokhari is the senior technology correspondent at Breitbart News. He is a graduate of the University of Oxford and was a 2020 Lincoln Fellow at the Claremont Institute for the Study of Statesmanship and Political Philosophy. In 2018, he obtained and published "The Google Tape," a recording of Google's top executives reacting to the 2016 Trump election and declaring their intention to make the American populist movement a "blip" in history. He is the author of *#Deleted: Big Tech's Battle to Erase the Trump Movement and Steal the Election*.

[Facebook](#) [Twitter](#) [LinkedIn](#) [Print](#) [Email](#) [Download Issue](#)

3/25/2021

Who Is in Control? The Need to Rein in Big Tech - Imprimis

The following is adapted from a speech delivered at Hillsdale College on November 8, 2020, during a Center for Constructive Alternatives conference on Big Tech.

In January, when every major Silicon Valley tech company permanently banned the President of the United States from its platform, there was a backlash around the world. One after another, government and party leaders—many of them ideologically opposed to the policies of President Trump—raised their voices against the power and arrogance of the American tech giants. These included the President of Mexico, the Chancellor of Germany, the government of Poland, ministers in the French and Australian governments, the neoliberal center-right bloc in the European Parliament, the national populist bloc in the European Parliament, the leader of the Russian opposition (who recently survived an assassination attempt), and the Russian government (which may well have been behind that attempt).

Common threats create strange bedfellows. Socialists, conservatives, nationalists, neoliberals, autocrats, and anti-autocrats may not agree on much, but they all recognize that the tech giants have accumulated far too much power. None like the idea that a pack of American hipsters in Silicon Valley can, at any moment, cut off their digital lines of communication.

I published a book on this topic prior to the November election, and many who called me alarmist then are not so sure of that now. I built the book on interviews with Silicon Valley insiders and five years of reporting as a Breitbart News tech correspondent. Breitbart created a dedicated tech reporting team in 2015—a time when few recognized the danger that the rising tide of left-wing hostility to free speech would pose to the vision of the World Wide Web as a free and open platform for all viewpoints.

This inversion of that early libertarian ideal—the movement from the freedom of information to the control of information on the Web—has been the story of the past five years.

When the Web was created in the 1990s, the goal was that everyone who wanted a voice could have one. All a person had to do to access the global marketplace of ideas was to go online and set up a website. Once created, the website belonged to that person. Especially if the person owned his own server, no one could deplatform him. That was by design, because the Web,

3/25/2021

Who Is in Control? The Need to Rein in Big Tech - Imprimis

when it was invented, was competing with other types of online services that were not so free and open.

It is important to remember that the Web, as we know it today—a network of websites accessed through browsers—was not the first online service ever created. In the 1990s, Sir Timothy Berners-Lee invented the technology that underpins websites and web browsers, creating the Web as we know it today. But there were other online services, some of which predated Berners-Lee's invention. Corporations like CompuServe and Prodigy ran their own online networks in the 1990s—networks that were separate from the Web and had access points that were different from web browsers. These privately-owned networks were open to the public, but CompuServe and Prodigy owned every bit of information on them and could kick people off their networks for any reason.

In these ways the Web was different. No one owned it, owned the information on it, or could kick anyone off. That was the idea, at least, before the Web was captured by a handful of corporations.

We all know their names: Google, Facebook, Twitter, YouTube, Amazon. Like Prodigy and CompuServe back in the '90s, they own everything on their platforms, and they have the police power over what can be said and who can participate. But it matters a lot more today than it did in the '90s. Back then, very few people used online services. Today everyone uses them—it is practically impossible not to use them. Businesses depend on them. News publishers depend on them. Politicians and political activists depend on them. And crucially, citizens depend on them for information.

Today, Big Tech doesn't just mean control over online information. It means control over news. It means control over commerce. It means control over politics. And how are the corporate tech giants using their control? Judging by the three biggest moves they have made since I wrote my book—the censoring of the *New York Post* in October when it published its blockbuster stories on Biden family corruption, the censorship and eventual banning from the Web of President Trump, and the coordinated takedown of the upstart social media site Parler—it is obvious that Big Tech's priority today is to support the political Left and the Washington establishment.

Big Tech has become the most powerful election-influencing machine in American history. It is not an exaggeration to say that if the technologies of Silicon Valley are allowed to develop to

3/25/2021

Who Is in Control? The Need to Rein in Big Tech - Imprimis

their fullest extent, without any oversight or checks and balances, then we will never have another free and fair election. But the power of Big Tech goes beyond the manipulation of political behavior. As one of my Facebook sources told me in an interview for my book: "We have thousands of people on the platform who have gone from far right to center in the past year, so we can build a model from those people and try to make everyone else on the right follow the same path." Let that sink in. They don't just want to control information or even voting behavior—they want to manipulate people's worldview.

Is it too much to say that Big Tech has prioritized this kind of manipulation? Consider that Twitter is currently facing a lawsuit from a victim of child sexual abuse who says that the company repeatedly failed to take down a video depicting his assault, and that it eventually agreed to do so only after the intervention of an agent from the Department of Homeland Security. So Twitter will take it upon itself to ban the President of the United States, but is alleged to have taken down child pornography *only after* being prodded by federal law enforcement.

How does Big Tech go about manipulating our thoughts and behavior? It begins with the fact that these tech companies strive to know everything about us—our likes and dislikes, the issues we're interested in, the websites we visit, the videos we watch, who we voted for, and our party affiliation. If you search for a Hannukah recipe, they'll know you're likely Jewish. If you're running down the Yankees, they'll figure out if you're a Red Sox fan. Even if your smart phone is turned off, they'll track your location. They know who you work for, who your friends are, when you're walking your dog, whether you go to church, when you're standing in line to vote, and on and on.

As I already mentioned, Big Tech also monitors how our beliefs and behaviors change over time. They identify the types of content that can change our beliefs and behavior, and they put that knowledge to use. They've done this openly for a long time to manipulate consumer behavior—to get us to click on certain ads or buy certain products. Anyone who has used these platforms for an extended period of time has no doubt encountered the creepy phenomenon where you're searching for information about a product or a service—say, a microwave—and then minutes later advertisements for microwaves start appearing on your screen. These same techniques can be used to manipulate political opinions.

3/25/2021

Who Is in Control? The Need to Rein in Big Tech - Imprimis

I mentioned that Big Tech has recently demonstrated ideological bias. But it is equally true that these companies have huge economic interests at stake in politics. The party that holds power will determine whether they are going to get government contracts, whether they're going to get tax breaks, and whether and how their industry will be regulated. Clearly, they have a commercial interest in political control—and currently no one is preventing them from exerting it.

To understand how effective Big Tech's manipulation could become, consider the feedback loop.

As Big Tech constantly collects data about us, they run tests to see what information has an impact on us. Let's say they put a negative news story about someone or something in front of us, and we don't click on it or read it. They keep at it until they find content that has the desired effect. The feedback loop constantly improves, and it does so in a way that's undetectable.

What determines what appears at the top of a person's Facebook feed, Twitter feed, or Google search results? Does it appear there because it's popular or because it's gone viral? Is it there because it's what you're interested in? Or is there another reason Big Tech wants it to be there? Is it there because Big Tech has gathered data that suggests it's likely to nudge your thinking or your behavior in a certain direction? How can we know?

What we *do* know is that Big Tech openly manipulates the content people see. We know, for example, that Google reduced the visibility of Breitbart News links in search results by 99 percent in 2020 compared to the same period in 2016. We know that after Google introduced an update last summer, clicks on Breitbart News stories from Google searches for "Joe Biden" went to zero and stayed at zero through the election. This didn't happen gradually, but in one fell swoop—as if Google flipped a switch. And this was discoverable through the use of Google's own traffic analysis tools, so it isn't as if Google cared that we knew about it.

Speaking of flipping switches, I have noted that President Trump was collectively banned by Twitter, Facebook, Twitch, YouTube, TikTok, Snapchat, and every other social media platform you can think of. But even before that, there was manipulation going on. Twitter, for instance, reduced engagement on the President's tweets by over eighty percent. Facebook deleted posts by the President for spreading so-called disinformation.

3/25/2021

Who Is in Control? The Need to Rein in Big Tech - Imprimis

But even more troubling, I think, are the invisible things these companies do. Consider “quality ratings.” Every Big Tech platform has some version of this, though some of them use different names. The quality rating is what determines what appears at the top of your search results, or your Twitter or Facebook feed, etc. It’s a numerical value based on what Big Tech’s algorithms determine in terms of “quality.” In the past, this score was determined by criteria that were somewhat objective: if a website or post contained viruses, malware, spam, or copyrighted material, that would negatively impact its quality score. If a video or post was gaining in popularity, the quality score would increase. Fair enough.

Over the past several years, however—and one can trace the beginning of the change to Donald Trump’s victory in 2016—Big Tech has introduced all sorts of new criteria into the mix that determines quality scores. Today, the algorithms on Google and Facebook have been trained to detect “hate speech,” “misinformation,” and “authoritative” (as opposed to “non-authoritative”) sources. Algorithms analyze a user’s network, so that whatever users follow on social media—e.g., “non-authoritative” news outlets—affects the user’s quality score. Algorithms also detect the use of language frowned on by Big Tech—e.g., “illegal immigrant” (bad) in place of “undocumented immigrant” (good)—and adjust quality scores accordingly. And so on.

This is not to say that you are informed of this or that you can look up your quality score. All of this happens invisibly. It is Silicon Valley’s version of the social credit system overseen by the Chinese Communist Party. As in China, if you defy the values of the ruling elite or challenge narratives that the elite labels “authoritative,” your score will be reduced and your voice suppressed. And it will happen silently, without your knowledge.

This technology is even scarier when combined with Big Tech’s ability to detect and monitor entire networks of people. A field of computer science called “network analysis” is dedicated to identifying groups of people with shared interests, who read similar websites, who talk about similar things, who have similar habits, who follow similar people on social media, and who share similar political viewpoints. Big Tech companies are able to detect when particular information is flowing through a particular network—if there’s a news story or a post or a video, for instance, that’s going viral among conservatives or among voters as a whole. This gives them the ability to shut down a story they don’t like before it gets out of hand. And these systems are growing more sophisticated all the time.

3/25/2021

Who Is in Control? The Need to Rein in Big Tech - Imprimis

If Big Tech's capabilities are allowed to develop unchecked and unregulated, these companies will eventually have the power not only to suppress existing political movements, but to anticipate and prevent the emergence of new ones. This would mean the end of democracy as we know it, because it would place us forever under the thumb of an unaccountable oligarchy.

The good news is, there is a way to rein in the tyrannical tech giants. And the way is simple: take away their power to filter information and filter data on our behalf.

All of Big Tech's power comes from their content filters—the filters on "hate speech," the filters on "misinformation," the filters that distinguish "authoritative" from "non-authoritative" sources, etc. Right now these filters are switched on by default. We as individuals can't turn them off. But it doesn't have to be that way.

The most important demand we can make of lawmakers and regulators is that Big Tech be forbidden from activating these filters without our knowledge and consent. They should be prohibited from doing this—and even from nudging us to turn on a filter—under penalty of losing their Section 230 immunity as publishers of third party content. This policy should be strictly enforced, and it should extend even to seemingly non-political filters like relevance and popularity. Anything less opens the door to manipulation.

Our ultimate goal should be a marketplace in which third party companies would be free to design filters that could be plugged into services like Twitter, Facebook, Google, and YouTube. In other words, we would have two separate categories of companies: those that host content and those that create filters to sort through that content. In a marketplace like that, users would have the maximum level of choice in determining their online experiences. At the same time, Big Tech would lose its power to manipulate our thoughts and behavior and to ban legal content—which is just a more extreme form of filtering—from the Web.

This should be the standard we demand, and it should be industry-wide. The alternative is a kind of digital serfdom. We don't allow old-fashioned serfdom anymore—individuals and businesses have due process and can't be evicted because their landlord doesn't like their politics. Why shouldn't we also have these rights if our business or livelihood depends on a Facebook page or a Twitter or YouTube account?

3/25/2021

Who Is in Control? The Need to Rein in Big Tech - Imprimis

This is an issue that goes beyond partisanship. What the tech giants are doing is so transparently unjust that all Americans should start caring about it—because under the current arrangement, we are all at their mercy. The World Wide Web was meant to liberate us. It is now doing the opposite. Big Tech is increasingly in control. The most pressing question today is: how are we going to take control back?

[!\[\]\(3ecd90fece18462627d0164b6f5a0422_img.jpg\) Facebook](#) [!\[\]\(89aa7095ff7f9a0328f6960fccee3958_img.jpg\) Twitter](#) [!\[\]\(7f15c3f9dc13d22360b42b2f0505953a_img.jpg\) LinkedIn](#) [!\[\]\(a16589889e62146fd87d3b0fb656a7ab_img.jpg\) Print](#) [!\[\]\(c00d40d8f921be9c7b7e769860dff432_img.jpg\) Email](#) [!\[\]\(1f9fcb67863a72e935291f73d060a47d_img.jpg\) Download Issue](#)

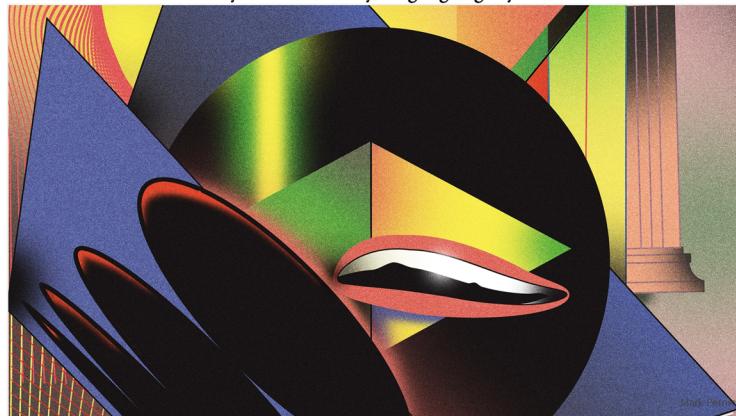


Copyright © 2021 Hillsdale College. All rights reserved.



The Dark Psychology of Social Networks

Why it feels like everything is going haywire



Story by Jonathan Haidt and Tobias Rose-Stockwell

DECEMBER 2019 ISSUE | TECHNOLOGY

SUPPOSE THAT THE biblical story of Creation were true: God created the universe in six days, including all the laws of physics and all the physical constants that apply throughout the universe. Now imagine that one day, in the early 21st century, God became bored and, just for fun, doubled the gravitational constant. What would it be like to live through such a change? We'd all be pulled toward the floor; many buildings would collapse; birds would fall from the sky; the Earth would move closer to the sun, reestablishing orbit in a far hotter zone.

3/19/2021

Social Media Is Warping Democracy - The Atlantic

 TheAtlantic - Why It Feels Like Everything Is Going Haywire - The Atlantic - ...

To hear more feature stories, see our full list or get the Audm iPhone app.

Let's rerun this thought experiment in the social and political world, rather than the physical one. The U.S. Constitution was an exercise in intelligent design. The Founding Fathers knew that most previous democracies had been unstable and short-lived. But they were excellent psychologists, and they strove to create institutions and procedures that would work with human nature to resist the forces that had torn apart so many other attempts at self-governance.

For example, in ["Federalist No. 10,"](#) James Madison wrote about his fear of the power of "faction," by which he meant strong partisanship or group interest that "inflamed [men] with mutual animosity" and made them forget about the common good. He thought that the vastness of the United States might offer some protection from the ravages of factionalism, because it would be hard for anyone to spread outrage over such a large distance. Madison presumed that factious or divisive leaders "may kindle a flame within their particular States, but will be unable to spread a general conflagration through the other States." The Constitution included mechanisms to slow things down, let passions cool, and encourage reflection and deliberation.

Madison's design has proved durable. But what would happen to American democracy if, one day in the early 21st century, a technology appeared that—over the course of a decade—changed several fundamental parameters of social and political life? What if this technology greatly increased the amount of "mutual animosity" and the speed at which outrage spread? Might we witness the political equivalent of buildings collapsing, birds falling from the sky, and the Earth moving closer to the sun?

America may be going through such a time right now.

What Social Media Changed

Facebook's early mission was "to make the world more open and connected"—and in the first days of social media, many people assumed that a huge global increase in connectivity would be good for democracy. As social media has aged,

3/19/2021

Social Media Is Warping Democracy - The Atlantic

however, optimism has faded and the list of known or suspected harms has grown: Online political discussions (often among anonymous strangers) are experienced as angrier and less civil than those in real life; networks of partisans co-create worldviews that can become more and more extreme; disinformation campaigns flourish; violent ideologies lure recruits.

The problem may not be connectivity itself but rather the way social media turns so much communication into a public performance. We often think of communication as a two-way street. Intimacy builds as partners take turns, laugh at each other's jokes, and make reciprocal disclosures. What happens, though, when grandstands are erected along both sides of that street and then filled with friends, acquaintances, rivals, and strangers, all passing judgment and offering commentary?

The social psychologist Mark Leary coined the term *sociometer* to describe the inner mental gauge that tells us, moment by moment, how we're doing in the eyes of others. We don't really need self-esteem, Leary argued; rather, the evolutionary imperative is to get *others* to see us as desirable partners for various kinds of relationships. Social media, with its displays of likes, friends, followers, and retweets, has pulled our sociometers out of our private thoughts and posted them for all to see.

Human beings evolved to gossip, preen, manipulate, and ostracize. We are easily lured into this new gladiatorial circus.

If you constantly express anger in your private conversations, your friends will likely find you tiresome, but when there's an audience, the payoffs are different—outrage can boost your status. A 2017 study by William J. Brady and other researchers at NYU measured the reach of half a million tweets and found that each moral or emotional word used in a tweet increased its virality by 20 percent, on average. Another 2017 study, by the Pew Research Center, showed that posts exhibiting “indignant disagreement” received nearly twice as much engagement—including likes and shares—as other types of content on Facebook.

3/19/2021

Social Media Is Warping Democracy - The Atlantic

The philosophers Justin Tosi and Brandon Warmke have proposed the useful phrase *moral grandstanding* to describe what happens when people use moral talk to enhance their prestige in a public forum. Like a succession of orators speaking to a skeptical audience, each person strives to outdo previous speakers, leading to some common patterns. Grandstanders tend to “trump up moral charges, pile on in cases of public shaming, announce that anyone who disagrees with them is *obviously* wrong, or exaggerate emotional displays.” Nuance and truth are casualties in this competition to gain the approval of the audience. Grandstanders scrutinize every word spoken by their opponents—and sometimes even their friends—for the potential to evoke public outrage. Context collapses. The speaker’s intent is ignored.

Human beings evolved to gossip, preen, manipulate, and ostracize. We are easily lured into this new gladiatorial circus, even when we know that it can make us cruel and shallow. As the Yale psychologist Molly Crockett has argued, the normal forces that might stop us from joining an outrage mob—such as time to reflect and cool off, or feelings of empathy for a person being humiliated—are attenuated when we can’t see the person’s face, and when we are asked, many times a day, to take a side by publicly “liking” the condemnation.

[From October 2018: America is living James Madison’s nightmare]

In other words, social media turns many of our most politically engaged citizens into Madison’s nightmare: arsonists who compete to create the most inflammatory posts and images, which they can distribute across the country in an instant while their public sociometer displays how far their creations have traveled.

Upgrading the Outrage Machine

At its inception, social media felt very different than it does today. Friendster, Myspace, and Facebook all appeared between 2002 and 2004, offering tools that helped users connect with friends. The sites encouraged people to post highly curated versions of their lives, but they offered no way to spark contagious outrage. This changed with a series of small steps, designed to improve user experience, that collectively altered the way news and anger spread through

3/19/2021

Social Media Is Warping Democracy - The Atlantic

American society. In order to fix social media—and reduce its harm to democracy—we must try to understand this evolution.

When Twitter arrived in 2006, its primary innovation was the timeline: a constant stream of 140-character updates that users could view on their phone. The timeline was a new way of consuming information—an unending stream of content that, to many, felt like drinking from a fire hose.

Later that year, Facebook launched its own version, called the News Feed. In 2009, it added the “Like” button, for the first time creating a public metric for the popularity of content. Then it added another transformative innovation: an algorithm that determined which posts a user would see, based on predicted “engagement”—the likelihood of an individual interacting with a given post, figuring in the user’s previous likes. This innovation tamed the fire hose, turning it into a curated stream.

Mark Pernice

The News Feed's algorithmic ordering of content flattened the hierarchy of credibility. Any post by any producer could stick to the top of our feeds as long as it generated engagement. "Fake news" would later flourish in this environment, as a personal blog post was given the same look and feel as a story from *The New York Times*.^[P]

Twitter also made a key change in 2009, adding the "Retweet" button. Until then, users had to copy and paste older tweets into their status updates, a small obstacle that required a few seconds of thought and attention. The Retweet

3/19/2021

Social Media Is Warping Democracy - The Atlantic

button essentially enabled the frictionless spread of content. A single click could pass someone else's tweet on to all of your followers—and let you share in the credit for contagious content. In 2012, Facebook offered its own version of the retweet, the "Share" button, to its fastest-growing audience: smartphone users.

Chris Wetherell was one of the engineers who created the Retweet button for Twitter. He admitted to BuzzFeed earlier this year that he now regrets it. As Wetherell watched the first Twitter mobs use his new tool, he thought to himself: "We might have just handed a 4-year-old a loaded weapon."

The coup de grâce came in 2012 and 2013, when Upworthy and other sites began to capitalize on this new feature set, pioneering the art of testing headlines across dozens of variations to find the version that generated the highest click-through rate. This was the beginning of "You won't believe ..." articles and their ilk, paired with images tested and selected to make us click impulsively. These articles were not usually intended to cause outrage (the founders of Upworthy were more interested in uplift). But the strategy's success ensured the spread of headline testing, and with it emotional story-packaging, through new and old media alike; outrageous, morally freighted headlines proliferated in the following years. In *Esquire*, Luke O'Neil reflected on the changes wrought on mainstream media and declared 2013 to be "The Year We Broke the Internet." The next year, Russia's Internet Research Agency began mobilizing its network of fake accounts, across every major social-media platform—exploiting the new outrage machine in order to inflame partisan divisions and advance Russian goals.

The internet, of course, does not bear sole responsibility for the pitch of political anger today. The media have been fomenting division since Madison's time, and political scientists have traced a portion of today's outrage culture to the rise of cable television and talk radio in the 1980s and '90s. A multiplicity of forces are pushing America toward greater polarization. But social media in the years since 2013 has become a powerful accelerant for anyone who wants to start a fire.

The Decline of Wisdom

Even if social media could be cured of its outrage-enhancing effects, it would still raise problems for the stability of democracy. One such problem is the degree to which the ideas and conflicts of the present moment dominate and displace older

3/19/2021

Social Media Is Warping Democracy - The Atlantic

ideas and the lessons of the past. As children grow up in America, rivers of information flow continually into their eyes and ears—a mix of ideas, narratives, songs, images, and more. Suppose we could capture and quantify three streams in particular: information that is new (created within the past month), middle-aged (created 10 to 50 years ago, by the generations that include the child's parents and grandparents), and old (created more than 100 years ago).

Citizens are now more connected to one another, on platforms that have been designed to make outrage contagious.

Whatever the balance of these categories was in the 18th century, the balance in the 20th century surely shifted toward the new as radios and television sets became common in American homes. And that shift almost certainly became still more pronounced, and quickly so, in the 21st century. When the majority of Americans began using social media regularly, around 2012, they hyper-connected themselves to one another in a way that massively increased their consumption of new information—entertainment such as cat videos and celebrity gossip, yes, but also daily or hourly political outrages and hot takes on current events—while reducing the share of older information. What might the effect of that shift be?

In 1790, the Anglo-Irish philosopher and statesman Edmund Burke wrote, “We are afraid to put men to live and trade each on his own private stock of reason; because we suspect that this stock in each man is small, and that the individuals would do better to avail themselves of the general bank and capital of nations and of ages.” Thanks to social media, we are embarking on a global experiment that will test whether Burke’s fear is valid. Social media pushes people of all ages toward a focus on the scandal, joke, or conflict of the day, but the effect may be particularly profound for younger generations, who have had less opportunity to acquire older ideas and information before plugging themselves into the social-media stream.

Our cultural ancestors were probably no wiser than us, on average, but the ideas we inherit from them have undergone a filtration process. We mostly learn of

3/19/2021

Social Media Is Warping Democracy - The Atlantic

ideas that a succession of generations thought were worth passing on. That doesn't mean these ideas are always right, but it does mean that they are more likely to be valuable, in the long run, than most content generated within the past month. Even though they have unprecedented access to all that has ever been written and digitized, members of Gen Z (those born after 1995 or so) may find themselves less familiar with the accumulated wisdom of humanity than any recent generation, and therefore more prone to embrace ideas that bring social prestige within their immediate network yet are ultimately misguided.

For example, a few right-wing social-media platforms have enabled the most reviled ideology of the 20th century to draw in young men hungry for a sense of meaning and belonging and willing to give Nazism a second chance. Left-leaning young adults, in contrast, seem to be embracing socialism and even, in some cases, communism with an enthusiasm that at times seems detached from the history of the 20th century. And polling suggests that young people across the political spectrum are losing faith in democracy.

Is There Any Way Back?

Social media has changed the lives of millions of Americans with a suddenness and force that few expected. The question is whether those changes might invalidate assumptions made by Madison and the other Founders as they designed a system of self-governance. Compared with Americans in the 18th century—and even the late 20th century—citizens are now more connected to one another, in ways that increase public performance and foster moral grandstanding, on platforms that have been designed to make outrage contagious, all while focusing people's minds on immediate conflicts and untested ideas, untethered from traditions, knowledge, and values that previously exerted a stabilizing effect. This, we believe, is why many Americans—and citizens of many other countries, too—experience democracy as a place where everything is going haywire.

[There was a time in American public life when atonement was seen as a form of strength—a way not only to own up to one's missteps but also to control the narrative. That time is over, Megan Garber writes.]

3/19/2021

Social Media Is Warping Democracy - The Atlantic

It doesn't have to be this way. Social media is not intrinsically bad, and has the power to do good—as when it brings to light previously hidden harms and gives voice to previously powerless communities. Every new communication technology brings a range of constructive and destructive effects, and over time, ways are found to improve the balance. Many researchers, legislators, charitable foundations, and tech-industry insiders are now working together in search of such improvements. We suggest three types of reform that might help:

(1) Reduce the frequency and intensity of public performance. If social media creates incentives for moral grandstanding rather than authentic communication, then we should look for ways to reduce those incentives. One such approach already being evaluated by some platforms is “demetrication,” the process of obscuring like and share counts so that individual pieces of content can be evaluated on their own merit, and so that social-media users are not subject to continual, public popularity contests.

(2) Reduce the reach of unverified accounts. Bad actors—trolls, foreign agents, and domestic provocateurs—benefit the most from the current system, where anyone can create hundreds of fake accounts and use them to manipulate millions of people. Social media would immediately become far less toxic, and democracies less hackable, if the major platforms required basic identity verification before anyone could open an account—or at least an account type that allowed the owner to reach large audiences. (Posting itself could remain anonymous, and registration would need to be done in a way that protected the information of users who live in countries where the government might punish dissent. For example, verification could be done in collaboration with an independent nonprofit organization.)

(3) Reduce the contagiousness of low-quality information. Social media has become more toxic as friction has been removed. Adding some friction back in has been shown to improve the quality of content. For example, just after a user submits a comment, AI can identify text that's similar to comments previously flagged as toxic and ask, “Are you sure you want to post this?” This extra step has been shown to help Instagram users rethink hurtful messages. The quality of information that is spread by recommendation algorithms could likewise be

3/19/2021

Social Media Is Warping Democracy - The Atlantic

improved by giving groups of experts the ability to audit the algorithms for harms and biases.

MANY AMERICANS MAY THINK that the chaos of our time has been caused by the current occupant of the White House, and that things will return to normal whenever he leaves. But if our analysis is correct, this will not happen. Too many fundamental parameters of social life have changed. The effects of these changes were apparent by 2014, and these changes themselves facilitated the election of Donald Trump.

If we want our democracy to succeed—indeed, if we want the *idea* of democracy to regain respect in an age when dissatisfaction with democracies is rising—we'll need to understand the many ways in which today's social-media platforms create conditions that may be hostile to democracy's success. And then we'll have to take decisive action to improve social media.

This article appears in the December 2019 print edition with the headline “Why It Feels Like Everything Is Going Haywire.”

3/25/2021

Square, Jack Dorsey's Pay Service, Is Withholding Money Merchants Say They Need - The New York Times

The New York Times

Square, Jack Dorsey's Pay Service, Is Withholding Money Merchants Say They Need

Small businesses say the Twitter chief's other company is holding on to 30 percent of their customers' payments during the pandemic.



By Nathaniel Popper

June 23, 2020

OAKLAND, Calif. — Jack Dorsey has won plaudits for his corporate activism during the coronavirus crisis, taking on President Trump in his role as Twitter's chief executive and donating nearly a third of his total wealth to pandemic relief.

But at Mr. Dorsey's other company, Square, a payments business where he is also chief executive, he is facing a growing chorus of unhappy customers.

Thousands of small enterprises that use Square to process their credit card transactions — including plumbers, legal consultants and construction firms — have complained that the company recently began holding back 20 to 30 percent of the money they collected from customers. The withholdings came with little warning, they said, and Square asserted the right to hang on to the money for the next four months.

Square told them that it was doing this to protect against risky transactions or customers who demanded their money back. But several affected businesses provided documents to The New York Times showing they had not had any returns or risk flags.

Square was unfairly keeping money from them at an economically vulnerable time to protect its own bottom line, they said. That had thrown their small businesses into financial difficulties, they added, forcing them to lay off employees, cut expansion plans, take out loans and miss mortgage payments.

"It may not be the coronavirus that puts us out of business but actually the greed of Square that breaks the camel's back," said Jesse Larsen, the owner of PennyWise Contracting, a construction company in Olympia, Wash.

YOUR CORONAVIRUS TRACKER: We'll send you the latest data for places you care about each day.

[Sign Up](#)

He said Square had begun holding on to 30 percent of each transaction in early May, which totaled thousands of dollars for him. Without those funds, he said, he had to put a hold on hiring and sell a boat and other personal property to keep his company operating.

Over the last month, around 1,300 business owners have signed an online petition asking Square to end the withholding. On Facebook, Twitter and consumer complaint sites, an array of small businesses have groused about the tough situation Square has put them in.

On Tuesday Square published a blog post to explain its new "rolling reserve" policy, the one that some merchants have experienced. In the post, which Square shared with The Times ahead of publication, the company said it had begun holding back money late last year and expanded the practice after the virus-related lockdowns as a way to protect consumers against losses. It said it had put reserves in place on only 0.3 percent of its millions of merchants.

"We apply reserves on more 'risky' sellers, such as those that take prepayment for goods or services delivered at a future date, sell goods or services more prone to disputes, or operate in an industry that historically receives higher chargeback rates than others," Square said in the post.

The San Francisco company, which is known for mobile payments and the square credit card reader that can turn smartphones and tablets into payment devices, has long made most of its money by deducting between 2 and 4 percent in fees every time a merchant uses Square to process a credit card or debit card transaction.

Keeping back parts of a transaction is legal. All payment companies have policies that allow them to hold back some portion of money from businesses if there are indications of trouble.

3/25/2021

Square, Jack Dorsey's Pay Service, Is Withholding Money Merchants Say They Need - The New York Times



Square said it had started holding back money late last year and expanded the practice to protect consumers against losses during the pandemic. Tom Jamieson for The New York Times

But Square did not withhold money before. And it appears to be the only payment company that is systematically applying the practice beyond the industries that the lockdowns hit particularly hard, such as travel companies, according to industry consultants and competitors.

The Coronavirus Outbreak >

Latest Updates >

Updated 48 minutes ago

- Denmark extends its suspension of the AstraZeneca vaccine.
- President Biden is expected to discuss the pandemic today at his first news conference.
- Free with your Covid shot: beer, arcade tokens and Krispy Kreme doughnuts.

Is this helpful?  

"Most companies are doing the opposite and trying to help small businesses," said Richard Meldner, the publisher of eSellerCafe, an industry publication that wrote about Square's withholding in May. "In all of this, Square is doing what the other companies did not."

Square has been hit harder by the pandemic-induced recession than other technology-focused payment companies. More than rivals like PayPal or Stripe, Square focuses on merchants with physical stores, many of which had to close during shelter-in-place orders.

Last month, when Square disclosed its financial results, it said it had swung to a \$106 million loss for the quarter and reported that it was increasing the cash it had on hand by 290 percent to hedge against future losses.

But many businesses whose money has been withheld said it was unfair for them to contribute to Square's financial cushion when they had shown no signs of being an increased risk.

Sean Weber, the owner of Legal Knock, a company near Los Angeles that builds websites for law firms, provided documents showing that he had used Square for two years and never had a customer ask for money back. Yet Square began withholding money from him in May, totaling around \$4,000, he said.

Mr. Weber said the only warning he had gotten was an email right before the first deductions, with little explanation. When he called Square to ask what he had done wrong, he initially had trouble getting through. The company later told him that it was a general policy imposed as a result of the risks caused by the pandemic.

"I told him: 'That's not my problem. Why do I have to bear the burden of that?'" Mr. Weber said he had responded. He was told there was no appeals process or method for getting the money released, he added.

3/25/2021

Square, Jack Dorsey's Pay Service, Is Withholding Money Merchants Say They Need - The New York Times

Mr. Weber said he had since had to miss the \$3,000 monthly mortgage payment on his home while looking for a new payment processor. When he complained about Square's policy on Twitter, the company blocked him, something it has also done to other customers who have publicly brought up the issue.

Nikol de Riso, the owner of EGA Solutions in Palmetto, Fla., said she could not get a response from Square for two weeks about the money it had held from her business, which provides various legal and practical services for small businesses. When she finally got someone on the phone, she said, she was told that the withholding was a general policy and not a result of any risks in her business.

Square said it planned to announce on Tuesday that it was providing merchants with more notice and more information about why they were facing reserves.

Without the money that was being withheld, Ms. Riso said, she had to furlough seven of her 53 employees while she switched over to a different processor, Redde Payments. Redde imposes no reserves and is charging her less for each transaction — around 2 percent instead of the 3.5 percent she paid Square — and she said she had an account representative who picked up the phone when she had problems.

Square told Ms. Riso that even after she switched, it would hold on to her money — about \$6,000 — for the next 120 days.

"My company is not going through a hard time, so why punish my people?" she said she had asked Square. "You are stealing other people's money."



March 24, 2021

Twitter, Inc.
1355 Market St. #900
San Francisco, CA 94103

Dear Ranking Member Rodgers:

Thank you for your March 11, 2021, letter inquiring about our content moderation policies and practices.

As Jack Dorsey, our CEO, will discuss in his testimony tomorrow, we recognize there is a trust deficit that has been building over the last several years affecting our service, not only for technology companies but also for the broader information ecosystem and institutions.

We strive to implement policies impartially and at scale. We built our policies primarily around the promotion and protection of three fundamental human rights — freedom of expression, safety, and privacy. As we develop, implement, and enforce our policies, we seek to balance these rights that can sometimes come into conflict with one another. Additionally, our policies must be adaptable to changes in behavior and evolving circumstances.

In an effort to do our part to address the trust deficit, Twitter is focusing on solutions aimed at enhancing transparency, embracing procedural fairness, increasing user choice, and protecting privacy.

Please see the answers to your specific questions below. Our team is available to answer any follow-up questions you might have or discuss these issues in greater detail. Thank you for your ongoing dialogue, and we look forward to continued conversations about solutions that earn your trust and advance the principles we've proposed.

1. As it relates to Twitter's content policies, please answer the following:

- a. What process does Twitter undertake to determine whether content on its platform violates its policies and is any outside person or third party involved in that process? If so, please identify such outside person or third party and how they are involved.**
- b. What process does Twitter undertake to determine whether a user should be suspended or deplatformed and is any outside person or third party involved in that process? If so, please identify such outside person or third party and how they are involved.**

c. When content is flagged or reported by users, what process does Twitter undertake to determine whether such content violates its policies? Please explain.

d. Does Twitter have an appeal process to challenge content decisions or decisions to suspend or deplatform users? If yes, please describe such process.

Policy Development

Consistent with its First Amendment rights, Twitter has developed a series of policies—the [Twitter Rules](#)—to govern how Twitter can be used and to ensure safety, privacy, and authenticity across the platform. All individuals accessing or using Twitter’s services must adhere to the policies set forth in these rules and agree to do so as part of our Terms of Service.

In crafting our rules, we consult experts, including our Trust & Safety Council and ad-hoc groups for specific issues, and strive to seek input from the public as we evaluate policies, as evidenced by our current efforts seeking [feedback](#) on our World Leaders Policy.

Policy Enforcement

We use a combination of machine learning and human review to assess potential violations of the Twitter Rules. In determining whether to take enforcement action against specific behavior or accounts we consider a number of factors, including (but not limited to) whether:

- the behavior is directed at an individual, group, or protected category of people;
- the report of a potential rule violation has been filed by the target of the abuse or a bystander;
- the user behind the potentially violative content has a history of violating our policies;
- the severity of the violation;
- the content may be a topic of legitimate public interest.

In most cases and where legally appropriate, when we take action on a Tweet, we show the violator the offending Tweet, explain which Rule was broken, and require them to remove the content before they can Tweet again. If someone repeatedly violates our Rules, our enforcement actions become stronger. We may require violators to remove the Tweet and we may take additional actions such as verifying account ownership and/or temporarily limiting an individual’s ability to Tweet for a set period of time. If someone continues to violate Rules beyond that point, their account may be permanently suspended.

Twitter Rules are enforced exclusively by our internal teams. No “outside” individuals are involved in making content-related enforcement decisions.

Please note that we do receive legal requests related to content and will review and respond to these in accordance with our [law enforcement guidelines](#). We provide detail on these requests in our transparency reports.

Procedural Fairness

As part of our effort to ensure procedural fairness, we strive to give people an easy, clear way to appeal decisions we make that they think are not right. For example, individuals can appeal a suspension through the platform interface or by [filing a report](#) online.

Transparency

Our [Twitter Transparency Center](#) provides information and statistics regarding accounts against which we have taken enforcement actions across twelve categories of terms of service violations.

More information about our enforcement philosophy and practices is publicly available on our [Help Center](#).

2. Since January 2020, please list every Republican public official—federal, state, or local—Twitter has suspended or deplatformed.

Twitter does not use political viewpoints, ideology, or party affiliation to make decisions related to content moderation. As noted above, we look at various factors to determine whether accounts or Tweets are in violation of the Twitter Rules. We apply the Twitter Rules impartially, and our [Transparency Center](#) makes information regarding accounts against which we have taken enforcement action publicly available for all those interested.

Because we do not categorize or track the accounts against which we take enforcement action based on the politics or ideology of the account holder, we do not have the data requested.

3. Since January 2020, please list every Democrat public official—federal, state, or local—Twitter has suspended or deplatformed.

Please see the response to question (2), above.

4. Since January 2020, as it relates to heads of government and world leaders, please identify each account Twitter has suspended or deplatformed and identify the specific policy for such decisions.

We have made clear that no world leader is completely above the Twitter Rules, and we have taken enforcement action, including the removal of

content, on accounts related to numerous government officials and world leaders across the globe for violating our policies against the glorification of violence and platform manipulation, among others. These accounts have ranged from those belonging to heads of nations to those affiliated with local officials within countries.

We recognize that suspending an account has significant ramifications, especially when that account belongs to a world leader or head of state. Politicians and government officials are constantly evolving how they use our service, and we want our policies to remain relevant to the ever-changing nature of political discourse on Twitter and protect the health of the public conversation.

In recent months, there have been increased questions about how we should address rule violations by world leaders, and whether we are striking the right balance between mitigating harm and ensuring access to information that is in the public interest. As a result, we are re-examining our approach to world leaders and soliciting feedback from the public. Starting on March 19, 2021, we called for responses to a [public survey](#) that will help inform the development of our policy framework. The questionnaire will be available in multiple languages and will close on Monday, April 12, 2021, at 5 p.m. PT. We are simultaneously consulting with a range of human rights experts, civil society organizations, and academics worldwide whose feedback will be reflected in forthcoming revisions to the policy framework.

We want to serve the public conversation and allow the public to hear from and engage with leaders around the world. Ultimately, our aim is to have a policy that appropriately balances fundamental human rights and considers the global context in which we operate.

5. Without disclosing personally identifiable information, please disclose any content removed by Twitter related to Black Lives Matter riots and identify the number of accounts suspended or disabled for posting such content.

We do not have this data, as we do not categorize or track the content we remove or the accounts against which we take enforcement action based on the politics or ideology of the account holder. We remove content and suspend accounts—either temporarily or permanently—based on the factors set forth in response to question (1), above.

Please refer to our [Transparency Center](#) for additional metrics regarding accounts against which we have taken enforcement actions across twelve categories of terms of service violations.

6. On June 1, 2020, now-Vice President Kamala Harris posted “If you’re able to, chip in now to the Minnesota Freedom Fund to help post bail for those protesting on the ground in Minnesota” and linked to an ActBlue Fund. Please explain how this post does not violate Twitter’s policies.

Our enforcement teams reviewed this Tweet and determined it does not violate the Twitter Rules.

7. As it relates to news articles on Twitter, please answer the following:

- a. Since January 2020, how many news articles has Twitter temporarily or permanently blocked? Please identify each article and explain the specific policy such articles violated.
- b. What is the process Twitter undertakes to determine which articles should be temporarily or permanently blocked? Please identify the specific criteria for determining whether an article should be blocked.

We apply the Twitter Rules impartially to all entities that use our service. Because we do not track the content against which we have enforced based on whether it was in the form of an article, we do not have the data you are requesting. Our [policy](#) on blocking or limiting the spread of URL links on Twitter is publicly available.

8. Does Twitter have a process to communicate, consult, and coordinate with law enforcement to address illicit content? If so, please explain.

Information sharing and engagement can be critical to Twitter’s success in safeguarding the conversation occurring on Twitter in certain circumstances. We have well-established relationships with law enforcement agencies, including the Federal Bureau of Investigation and others. Consistent with applicable law, we look forward to continued cooperation with federal, state, and local government agencies on a variety of issues because in certain circumstances, only they have access to information critical to our joint efforts to stop bad-faith actors.

Twitter has detailed, [publicly available guidelines](#) for law enforcement authorities seeking assistance. These guidelines set forth how law enforcement authorities can request Twitter account information, content removal, data preservation, and emergency disclosures; our global teams respond to each of these types of requests on a daily basis.

9. Does Twitter have a process to preserve evidence of illegal content on its platform to assist law enforcement? If so, please explain.

Twitter retains different types of information for different lengths of time, and in accordance with our [Terms of Service](#) and [Privacy Policy](#). Given Twitter's real-time nature, some information may only be stored for a very brief period of time. Where legally appropriate, we accept requests from law enforcement to preserve records that constitute potentially relevant evidence in legal proceedings. We will preserve, but not disclose, a temporary snapshot of the relevant account records for 90 days pending service of valid legal process.

Some information we store is automatically collected, while other information is provided at the user's discretion. More information on Twitter's retention policies can be found in our Privacy Policy.

10. Does Twitter coordinate with Google and Facebook on any content decisions? If so, please identify the categories of such content decisions.

Twitter does not coordinate with other entities on individual content moderation decisions.

We do voluntarily collaborate with industry peers to share information to inform and support our efforts related to terrorism, child sexual exploitation, election security, state-backed information operations, and COVID-19 misinformation. For example:

- In June 2017, we launched the Global Internet Forum to Counter Terrorism (the "GIFCT"), a partnership among Twitter, YouTube, Facebook, and Microsoft. The GIFCT facilitates, among other things: information sharing; technical cooperation; and, research collaboration, including with academic institutions.
- We participate in the National Center for Missing and Exploited Children's hash sharing database for industry and non-governmental organizations which consists of image and video hashes of known child sexual abuse material.
- We are a member of the Technology Coalition. This industry-led nonprofit organization strives to eradicate child sexual exploitation by mentoring emerging or established companies, sharing trends and best-practices across the industry, and facilitating technological solutions across the ecosystem.
- Along with a number of technology companies, we have established a dedicated, formal communications channel to facilitate real-time information sharing regarding election integrity. We also share information with our industry peers when we identify accounts acting in coordination in state-backed information operation campaigns.

- In March 2020, we announced an informal industry effort to share information about COVID-19. This followed requests by White House officials for the technology industry to come together to combat misinformation about the virus.

11. Does Twitter coordinate with Google and Facebook on any decisions related to suspending or deplatforming users? If so, please explain.

Twitter does not coordinate with other entities on individual content moderation decisions. Please see response to question (10), above, for additional details on how we share information with industry peers and government partners.

12. As it relates to former-President Trump, please answer the following:

- a. Did Twitter coordinate with Google, Facebook, or any other tech company to make content decisions about his posts? If so, please explain.
- b. Did Twitter coordinate with Google, Facebook, or any other tech company to suspend or remove his account? If so, explain.

Twitter did not coordinate with other platforms on decisions related to President Trump's account, including decisions to suspend it or take action on certain content.

13. Did Twitter coordinate with Google, Facebook, or any other tech company to make content decisions related to Black Lives Matter riots? If so, please explain.

Twitter did not coordinate with other platforms on decisions related to Black Lives Matter, including decisions to suspend accounts or take action on certain content.

14. Did Twitter coordinate with Google, Facebook, or any other tech company to suppress the October 14, 2020, New York Post article titled "Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad"? If so, please explain.

Twitter did not coordinate with other platforms on decisions related to the October 14, 2020, New York Post article titled "Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad."

15. Does Twitter alter its algorithms to drive certain content or narratives based on the political leaning of such content? If so, please explain.

Twitter does not alter its algorithms to drive certain content or narratives based on the political leanings reflected in the content.

Furthermore, as noted above, we are committed to providing more choice to how the people who use our service view content. In December 2018, Twitter introduced a sparkle icon located at the top of individuals' timelines to more easily switch on and off reverse-chronological timeline. The algorithms we employ are designed to help people see the most relevant Tweets. The icon now allows individuals using Twitter to easily switch to chronological order ranking of the Tweets from only those accounts they follow. This improvement allows individuals on Twitter to see how algorithms affect what they see, and enables greater transparency into the technology we use to rank Tweets.

16. What specific criteria does Twitter have that determines what content "trends" and the title for such trends? Are any employees involved in deciding what content "trends" or is that decision fully automated?

A combination of algorithms and our teams determine if a Tweet represents a trend by evaluating if the Tweet is very reflective of the trend and popular. Our algorithms are designed to identify representative Tweets that aren't potentially abusive, spam, or posted by accounts trying to take advantage of our system. In some cases, we may add brief descriptions to help add context. Descriptions will provide straightforward, clearly sourced context around why something is trending. Descriptions are developed by our curation team and follow their guidelines.

17. Please explain any efforts Twitter has undertaken to support local news and traditional media.

Twitter is a window into what's happening in the world, which is why some of the most active Twitter accounts belong to journalists. News often breaks first on Twitter, and everyone from national media outlets to reporters on the ground often use our service to update the public on developing stories. By engaging on Twitter, journalists generate greater interest and trust in their work.

Because journalism is core to Twitter's service, we believe we have a responsibility to protect that work. A year ago, as journalists came under unique economic threats and direct attempts at censorship in the context of the global COVID pandemic, we recognized our role in that mission. Last March, we donated one million dollars evenly distributed between the Committee to Protect Journalists and the International Women's Media Foundation. These funds were used to help ensure that these

organizations could continue their work in the face of new economic strains and to directly support journalists. We are also longtime sponsors of nonprofit organizations that support journalists in the U.S. and abroad.

Thank you, again, for the opportunity to address your questions. We look forward to speaking with you and members of the Committee in greater detail this week and moving forward.

Sincerely,



Lauren Culbertson
Head of U.S. Public Policy
Twitter

CC:
Rep. Bob Latta
Rep. Gus M. Bilirakis
Rep. Fred Upton
Rep. Michael C. Burgess, M.D.
Rep. Steve Scalise
Rep. Brett Guthrie
Rep. David McKinley
Rep. H. Morgan Griffith
Rep. Bill Johnson
Rep. Billy Long
Rep. Larry Bucshon, M.D.
Rep. Markwayne Mullin
Rep. Richard Hudson
Rep. Tim Walberg
Rep. Earl L. "Buddy" Carter
Rep. Jeff Duncan
Rep. Gary Palmer
Rep. Neal Dunn
Rep. John Curtis
Rep. Debbie Lesko
Rep. Greg Pence
Rep. Dan Crenshaw
Rep. John Joyce
Rep. Kelly Armstrong



Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Google.com

March 24, 2021

The Honorable Cathy McMorris Rodgers
Ranking Member, House Committee on Energy & Commerce
1314 Longworth House Office Building
Washington, DC 20515

The Honorable Bob Latta Ranking Member, Subcommittee on Communications & Technology	The Honorable Gus Bilirakis Ranking Member, Subcommittee on Consumer Protections & Commerce
The Honorable Michael C. Burgess, M.D.	The Honorable Fred Upton
The Honorable Steve Scalise	The Honorable Brett Guthrie
The Honorable David McKinley	The Honorable H. Morgan Griffith
The Honorable Bill Johnson	The Honorable Billy Long
The Honorable Larry Bucshon, M.D.	The Honorable Markwayne Mullin
The Honorable Richard Hudson	The Honorable Tim Walberg
The Honorable Earl L. "Buddy" Carter	The Honorable Jeff Duncan
The Honorable Gary Palmer	The Honorable Neal Dunn
The Honorable John Curtis	The Honorable Debbie Lesko
The Honorable Greg Pence	The Honorable Dan Crenshaw
The Honorable John Joyce	The Honorable Kelly Armstrong

Dear Ranking Member McMorris Rodgers and esteemed Republican members of the House of Representatives Committee on Energy and Commerce:

Thank you for your letter dated March 11, 2021, regarding your Big Tech Accountability Platform. We welcome the opportunity to address Google's similar commitments to transparency, accountability, objectivity, and support for a competitive publishing industry.

Please find our responses to your questions below.

Big Tech Responsibility:

1. **As it relates to Google's content policies regarding advertising and sponsored content, please answer the following:**
 - a. **What process does Google undertake to determine whether content violates its policies and is any outside person or third party involved in that process? If so, please identify such outside person or third party and how they are involved.**
 - b. **When content is flagged or reported by users, what process does Google undertake to determine whether such content violates its policies? Please explain.**

We enforce our policies using both automated and manual detection and enforcement, and we incorporate third party feedback to assess and address potentially problematic content. In addition to important and useful flags by individual users reporting ads, our sophisticated automated technology helps us detect problematic content at scale. Our automated systems are carefully trained to quickly identify and take action against spam and violative content. This includes flagging potentially problematic content for human reviewers, whose judgment is needed for the many decisions that require a more nuanced determination. The context in which a piece of content is created or shared is an important factor in any assessment about its quality or its purpose. We are attentive to educational, scientific, artistic, or documentary contexts, including journalistic intent, where the content might otherwise violate our policies.

We offer users several pathways to allow outside parties to identify potentially problematic ads or content, for example through the "[report an ad](#)" form, which you can find here at: https://support.google.com/google-ads/contact/vio_other_aw_policy. When an ad or content is identified as potentially problematic, we review that ad or content to determine whether or not it violates our policies.

We work hard to ensure that we protect our users but also allow them to get the information they need, in consonance with our mission.

- c. **Does Google have an appeal process to challenge content decisions or decisions to suspend or ban organizations from advertising? If yes, please describe such process.**

We engage with our publishers, advertisers, and content creators to ensure that they are abiding by our policies and so they understand if and how they can come back to our platform after a policy-violation problem. We do that proactively and reactively. For example, on Play, we list all of our developer policies in the [Developer Policy Center](#) (which you can find here at: <https://play.google.com/about/developer-content-policy>) and engage with App developers through the developer console to ensure they understand our policy

requirements and are aware of potential improvements they can make to help them succeed on the platform. On YouTube, we have an appeals process where creators can request that we re-evaluate their adherence to our policies if they think we have gotten it wrong. We aim to make it easy for developers or creators who are willing to address our concerns in good faith and can reinstate their content or accounts when they do. The same is true for publishers who are able to appeal enforcement actions that we have taken where they feel that they have not breached our policies or where they have addressed the breach and would like to be re-evaluated.

Our advertising policies exist to protect users, advertisers, and publishers from bad actors and ensure that only high-quality ads are served across our platforms. Sometimes advertisers have concerns about enforcement decisions. To address these concerns, we make it clear to advertisers that we have taken action on their content and provide them the opportunity to appeal that decision and give us clarifications. The decision will then be evaluated by a different member of our Trust and Safety team. On the other hand, in cases of serious, repeated, or deceptive violations, we may take action that affects an entire advertiser account.

d. Since January 2020, please list every organization Google has suspended or banned for violating its content policies.

At Google, we have nearly 22,000 people dedicated to monitoring content on our platforms and spent \$1.2 billion last year to ensure the protection of our users. We recently published our [annual Ads Safety Report](#) which gives a sense of the scale of our enforcement efforts (you can find the report here at: <https://blog.google/products/ads-commerce/ads-safety-report-2020/>) . In 2020, we blocked or removed 3.1 billion bad ads, which equates to almost 5,900 ads per minute. We suspended more than 1.7 million advertiser accounts for egregious policy violations. And we blocked nearly 100 million COVID-related Google Ads from running on our platforms, including those engaging in price-gouging and promoting products such as fake cures or fake vaccine treatments. We also removed ads from over 1.3 billion publisher pages and 1.6 million publisher sites.

We cannot generally comment on individual sites, pages, or accounts, in the interest of fairness to the advertisers and publishers involved and to inhibit bad actors from attempting to game our systems. That said, we take compliance with our ads policies very seriously and take action in accordance with our policies where appropriate. And we are an industry leader in providing publicly accessible transparency reports on our content decisions. Examples of those reports can be found at: <https://transparencyreport.google.com/?hl=en> and <https://transparencyreport.google.com/youtube-policy/removals?hl=en>.

2. As it relates to news articles on Google search, please answer the following:

a. What criteria does Google use to determine what news articles appear on its first search page results?

We understand that connecting our users to high quality news content helps journalism and democracy flourish by bringing new audiences to publishers. We help newspapers earn revenue from digital ads and increase their readership via clicks from Google Search and we are working to help newspapers adapt to an increasingly competitive market. Our Google News Initiative is a \$300 million commitment to help journalism thrive in a digital age. In October 2020, we announced an initial \$1 billion investment in partnerships with news publishers. And last April, we launched a Journalism Emergency Relief Fund to help thousands of small, medium, and local news publishers.

The Google Search index represents more than 100 million gigabytes of data, mapping hundreds of billions of webpages. Whether for news or for other topics, we use algorithms to organize our Search results to give users the most useful and relevant results according to our best understanding of what information they are looking for — as expressed by their search queries.

Usually, multiple pieces of content are relevant to a user's intent, which is why we look to a variety of other factors to rank links to these pieces of content. Our ranking algorithms look for signals that indicate the expertise, authoritativeness, and trustworthiness of every piece of content so that the best results for the user at that time are at the top. In the context of news, they can also look at signals like recency, location, or prominence (whether a news story is covered by many news organizations). One early and well-known example of the type of algorithms we use for Search ranking is PageRank, which uses links on the web to assess the importance of a given website. For more information, please see our dedicated websites on [a.co/howsearchworks](https://www.google.com/search/howsearchworks) and <https://newsinitiative.withgoogle.com/hownewsworks>.

Reputable independent parties — including *The Economist* — have done in-depth studies of our search results and concluded that they are not politically biased. Just last month, consistent with *The Economist*, New York University reached the same conclusion. (See the New York University - Stern Business School Center for Business and Human Right report here: https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/60187b5f4576e708708c8e9/1612217185240/NYU+False+Accusation_2.pdf.)

b. Since January 2020, please identify any news article Google has prevented from showing up in search entirely and explain why.

At Google, we believe in open access to information, so we try hard to make information from the web available to everyone. We believe that society works best when it provides a space for all voices to be heard, and that people are best served when they have access to a breadth of diverse content from a variety of sources. While we do have a narrow set of policies related to search features like autocomplete, we do not remove links from search results except in very limited circumstances, including those based on our legal obligations, copyright, webmaster guidelines, spam, and sensitive personal information like government IDs. Please see our policies relating to [removals for legal obligations](https://support.google.com/websearch/answer/9673730) (which you can find here at: <https://support.google.com/websearch/answer/9673730>), [webmaster guidelines](https://support.google.com/webmasters/answer/2600224) (which you can find here at: <https://support.google.com/webmasters/answer/2600224>)

[guidelines/webmaster-guidelines](#)), [voluntary removal policies](#) (which you can find here at: <https://support.google.com/websearch/answer/3143948>) and those concerning [removals for copyright infringement](#) (which you can find here at: <https://support.google.com/transparencyreport/answer/7347743?hl=en>), and the section of our [Transparency Report](#) (which you can find here at: <https://transparencyreport.google.com/>) relating to content removals due to [copyright](#) (which you can find here at: <https://transparencyreport.google.com/copyright/overview>), [government requests](#) (which you can find here at: <https://transparencyreport.google.com/government-removals/overview>), and more.

3. Does Google have a process to communicate, consult, and coordinate with law enforcement to address illicit content? If so, please explain.

Protecting our users is always our first priority. While we generally apply our policies independently, we welcome information from our peers and law enforcement to help us ensure the integrity of our platform.

From counter terrorism, to our work to fight against child sexual abuse material (CSAM), to protecting our elections, as well as the work we have done to address the events at the nation's Capitol on January 6 of this year, we have a dedicated team that responds to law enforcement around the clock, every day of the year. We have referred cases to law enforcement when we identified illegal activity on our platform, and do so urgently when we become aware of an imminent threat to life, such as in missing persons cases or in suicide threats.

As our publicly available transparency report describes, we responded to over 100,000 law enforcement requests in the first half of 2020 alone. We proactively made over half a million reports to the National Center for Missing and Exploited Children (NCMEC), and we recently published a [transparency report](#) focused on our efforts to combat online CSAM (you can find our transparency report here at: <https://transparencyreport.google.com/child-sexual-abuse-material/reporting?hl=en>). Just recently, we were [thanked](#) by law enforcement for our work on identifying and combating coordinated influence operations, which you can find here at: <https://www.justice.gov/usao-ndca/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps>.

We are proud of the work we do with law enforcement to protect our democracy and our users, and we describe it in our publicly available Transparency Report. We welcome and value the ongoing discussions with the government and law enforcement on how we can help to protect the public against crime and terrorism.

4. Does Google have a process to preserve evidence of illegal activity on its platform to assist law enforcement? If so, please explain.

We have a robust law enforcement response process with analysts and lawyers dedicated to ensure that we not only appropriately respond to legal processes, including preservation requests, from law enforcement to protect our users, but also make referrals to law enforcement when we identify illegal activity on our platform.

5. How does Google determine what search results show up on the first page? Please identify the specific criteria.

Our company mission is to organize the world's information and make it universally accessible and useful. That's why Search makes it easy to discover a broad range of information from a wide variety of sources. Search ranks websites [based on hundreds of factors](#) (which you can find described here at: <https://www.google.com/search/howsearchworks/>), from relevance to authoritativeness to recency. Search algorithms look at many factors, including the words of your query, relevance and usability of pages, expertise of sources, and a user's location and settings.

There are billions of Search queries around the world every day, and 15% of the searches we see each day are searches that we have never seen before. As such, Search continues to change to meet the evolving needs and expectations of the people who use Google, and to adapt to new tactics of spam or fraud. For these changes, we rely on extensive testing and have a rigorous evaluation process to analyze metrics and decide whether to implement a proposed change. Changes to our ranking algorithms are also informed by feedback from Search raters all around the country and the world who assess updates to Search based on our publicly available [rater guidelines](#), which you can find here at: <https://static.googleusercontent.com/media/guidelines.raterhub.com/en/searchqualityevaluatorguidelines.pdf>. Their feedback helps us understand which changes make Search more useful.) Data from these evaluations and experiments go through a thorough review by experienced engineers and search analysts, as well as other legal and privacy experts, who then determine if the change is approved to launch.

As we [recently announced](#), since 2017 we have done more than a million search quality tests, and we now average more than 1,000 tests per day, which you can find here at: <https://www.blog.google/products/search/our-latest-investments-information-quality-search-and-news/>. And in 2020, we ran over 600,000 experiments that resulted in more than 4,500 improvements to Search quality.

You can learn about how Search works at our How Search Works website which you can find at: <https://www.google.com/search/howsearchworks/mission/>.

6. How often does Google make material changes to its algorithms? Please explain the process Google undertakes to make such changes and provide reasons for such changes.

See answer to question 5.

7. What criteria does Google use to tailor or adjust its algorithms to determine the content users see?

See answer to question 5.

Big Tech Power:**8. Does Google coordinate with Twitter and Facebook on any content decisions?
If so, please identify the categories of such content decisions.**

Our Trust and Safety teams make content decisions independently based on our transparent policies and according to the processes described in the answers to questions 1a and 1b, above.

We do, however, collaborate with industry in other ways, to protect our platform and the people who use our products:

- **Countering terrorism content:** To substantially disrupt terrorists' abilities to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence using our platforms, we have joined with others in the industry to establish the Global Internet Forum to Counter Terrorism (GIFCT). Among other important initiatives, GIFCT allows participating companies and organizations to submit digital fingerprints — “hashes” — of identified terrorist and violent extremist content to a shared database to enable participating platforms to swiftly identify it for removal.
- **Fighting child sexual abuse material:** To help eradicate the horrors of child sexual abuse material, in 2006 Google joined with other industry members in the Technology Coalition. We make cutting-edge technology available for free to qualifying industry and non-governmental organizations in order to help identify, remove, and report CSAM more quickly and at a greater scale. In the last decade-plus, member companies have made progress with the development and roll-out of innovative technology to combat CSAM, and, in 2020, the Coalition announced “Project Protect,” a renewed investment and strategic plan to enhance our collective work. Tools like CSAI Match and Content Safety API, which were developed by Google and YouTube engineers, help prioritize potentially illegal content for review while identifying both known and never-before-seen CSAM. In addition to being used on our platforms, these tools are also being used by companies like Adobe, Tumblr, and Reddit to aid in faster identification of potential victims of CSAM, while reducing the toll on content moderators.
- **Countering online influence operations:** When we find attempts to conduct coordinated influence operations on our platforms, we work to swiftly remove such content and terminate the responsible accounts. We take steps to prevent possible future attempts by the same actors, and routinely exchange information and share our findings with others in the industry. We also share updates about this kind of activity via our [Threat Analysis Group Bulletin](https://blog.google/threat-analysis-group/) (which you can find here at: <https://blog.google/threat-analysis-group/>).

Google also coordinates with our peers and law enforcement on specific or general threats when appropriate.

9. Does Google coordinate with Twitter and Facebook on any decisions related to suspending or banning users, particularly when it comes to advertising decisions? If so, please explain.

See answer to question 8.

10. Does Google coordinate with Twitter, Facebook, or any other tech company to determine which apps are available on the Google Play app store? If so, please explain.

See answer to question 8.

11. Does Google coordinate with Twitter, Facebook, or any other tech company to determine which apps, games, or extensions are available on the Chrome Web Store? If so, please explain.

See answer to question 8.

12. Did Google coordinate with Twitter, Facebook, or any other tech company to make content decisions related to Black Lives Matter riots? If so, please explain.

See answer to question 8.

13. Did Google do anything to reduce access to the October 14, 2020, New York Post article titled “Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad”? If so, please explain.

We enforce our policies consistently and without regard to the political leaning of the content that is on our services. In this case, we did not find a policy violation, and therefore took no enforcement action.

14. Does Google alter its algorithms to drive certain content or narratives based on the political leaning of such content? If so, please explain.

No. Google's ranking systems are not designed to assess or consider the political leanings of content as we make ranking decisions. Our business model is dependent on being a useful and trustworthy source of information for everyone, so we have a natural, long-term business incentive to prevent anyone from interfering with the integrity of our products.

We design Search and other products with extraordinary care to serve our mission without political bias and have robust systems to ensure that employees' personal biases do not impact our products and that our policies are enforced without regard to political viewpoint.

Our Search algorithm ranks pages to provide the most useful and relevant information by matching search terms against available web pages and looking at factors like the number of times the words appear and freshness of the page. Political viewpoint is not a factor in our algorithm.

We seek to ensure that our Search results are providing the most authoritative and responsive results by using external quality raters from across 49 U.S. states. Our [Search Quality Rater Guidelines](https://static.googleusercontent.com/media/guidelines.raterhub.com/en/searchqualityevaluatorguidelines.pdf), which you can find here at <https://static.googleusercontent.com/media/guidelines.raterhub.com/en/searchqualityevaluatorguidelines.pdf>, are a public document that provides transparency for ratings, users, and webmasters about how Search works. And they make clear that ratings should never be based on personal opinions, preferences, religious beliefs, or political views.

15. Please explain any efforts Google has undertaken to support local news and traditional media.

Google is committed to supporting open access to information. Our products give people choice and help them find more authoritative and relevant journalism — from international stories to community reporting — than ever before. Over the past 20 years, we have collaborated closely with the news industry and provided billions of dollars to support the creation of quality journalism in the digital age by sharing revenue with news publishers via our ad network, and by developing tools, training, and funding through programs like the Google News Initiative, and launching Google News Showcase. Through both our services and our direct funding of news organizations, Google is one of the world's biggest financial supporters of journalism.

Each month, people click through from Google Search and Google News results to publishers' websites more than 24 billion times. The traffic we send to news sites helps publishers increase their readership, build trust with readers, and earn money. We also pay to license content through initiatives like Google News Showcase, a new online experience that's powered by a \$1 billion investment in news organizations. We have agreements with more than 500 news publications in a dozen countries for Google News Showcase, with more to come. We have also consistently worked to find new ways to support the news industry including the Google News Initiative, through which we provide tools, training, and grant funding to help news organizations evolve in the digital age. The Google News Initiative includes a \$61 million commitment in funding to support more than two thousand news partners across the United States and Canada. In April 2020, we launched a [Journalism Emergency Relief Fund](https://newsinitiative.withgoogle.com/journalism-emergency-relief-fund/) to deliver urgent aid to thousands of small, medium, and local news publishers globally (which you can find described here at: <https://newsinitiative.withgoogle.com/journalism-emergency-relief-fund/>).

Our advertising technology helps news organizations make money by showing ads on their websites, apps, and videos. With respect to digital ad revenue, [publishers kept over 69%](#) of the revenues from digital ads when Google's tools are used, which you can find here at: <https://blog.google/products/admanager/display-buying-share-revenue-publishers/>. The UK Competition and Markets Authority concluded that our fees were in line with or lower than average ad tech fees in the industry. And, as shown in a [blog we published in June](#) 2020, which you can find here at: <https://www.blog.google/products/admanager/news-publishers-make-money-ad-manager/>, news publishers in particular typically handle many parts of their own ad placement and sales, and so typically keep 95% of overall digital ad

revenue generated when using Ad Manager. We help newspapers to earn revenue from digital ads and to increase their readership via clicks from Google Search and Google News.

We also regularly work closely with the news industry to develop products — and evolve existing products — to better address their needs. For example, Google partnered with news publishers to launch Subscribe with Google, a suite of products to help news publishers grow their reader revenue businesses. We also partnered with publishers to develop an open standard that eventually became the Accelerated Mobile Pages (AMP) framework; AMP was designed to help publishers to address changes in user behavior as the prominence of mobile applications and platforms was rising and new, proprietary formats risked creating an unsustainable amount of technical overhead. As one final example, we recently made ranking updates and published changes to our search rater guidelines to help us better recognize original reporting, show it more prominently in Search, and ensure it stays there longer; this was in partnership with, and in response to feedback from, publishers.

We provide meaningful support to the local news industry and will continue these efforts going forward.

Thank you again for your inquiry. We look forward to continuing this conversation in this month's House Energy and Commerce Committee hearing and beyond.

Sincerely,



Mark Isakowitz
Vice President
Government Affairs and Public Policy

March 24, 2021

The Honorable Cathy McMorris Rodgers
Ranking Member
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Committee Members:

Thank you for your letter of March 11th regarding Facebook's content moderation practices. Please find the answers to your questions below.

1. As it relates to Facebook's content policies, please answer the following:

a. **What process does Facebook undertake to determine whether content on its platform violates its policies and is any outside person or third party involved in that process? If so, please identify such outside person or third party and how they are involved.**

We apply our own policies and make independent decisions about how to moderate content based on our Community Standards, which are posted publicly and outline what is and is not allowed on Facebook. Our policies are based on principles of voice, safety, dignity, authenticity, and privacy.

We work with vendor partners to help us review content at scale, 24 hours a day. While full time employees are involved in content review, the majority of those who review content for Facebook work full time for our partners and work at sites managed by these partners.

In certain countries, we work with independent third-party fact-checkers who review and rate the accuracy of stories. These partners have been certified through a non-partisan International Fact-Checking Network, and we list them publicly. Today, we partner with over 80 partners fact-checking content in over 60 languages. For the full list, see <https://www.facebook.com/business/help/997484867366026?id=673052479947730>

Once a story is rated as false, altered, or partly false, we show it lower in News Feed. And on Instagram, we make it harder to find by filtering from Explore and hashtag pages and down-ranking it in Feed.

In addition, content across Facebook and Instagram that has been rated false or altered is prominently labeled so people can better decide for themselves what to read, trust, and share. These labels are shown on top of false and altered photos and videos, including on top of Stories content on Instagram and link out to the assessment from the

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK


fact-checker. For content rated partly false or missing context, we'll apply a lighter-weight warning label.

In developing and iterating on our policies, we consult with outside academics and experts from across the political spectrum and around the world, and we provide in-depth examples and explanations of what policy changes would entail. As a matter of practice, we do not share the names of the groups we consult with for a number of reasons, including safety and security concerns—which are especially acute in places around the world where the government may exercise censorship or control—and the fact that groups may not want to be named.

On top of the consultations we have when building and refining our policies, we also receive input from the Oversight Board about our policies and practices. Cases can be appealed to the Oversight Board by Facebook itself, and by people using both Facebook and Instagram. In addition to the binding decision on the case content, the Oversight Board publicly issues recommendations that help us refine our policies and practices.

b. What process does Facebook undertake to determine whether a user should be deplatformed and is any outside person or third party involved in that process? If so, please identify such outside person or third party and how they are involved.

Please see the response to your previous question. The consequences for violating our Community Standards vary depending on the severity of the violation and the person's history on the platform. For instance, we may warn someone for a first violation, but if they continue to violate our policies, we may restrict their ability to post on Facebook or disable their profile.

c. When content is flagged or reported by users, what process does Facebook undertake to determine whether such content violates its policies? Please explain.

Facebook encourages users to report to us content that may violate our policies. We use a combination of technology, reports from our community, and review by our teams to identify and review content against our standards. If we determine that content or an account violates our policies, we take action—removing the content, disabling the account, or covering content with a warning. Even if user-reported content does not violate our policies, however, users have control over what they see and who they interact with. A user can:

- Block someone, which prevents the other person from seeing things the user posts on his/her profile; starting conversations with the user; adding the user as a friend; tagging the user in posts, comments, or photos; and inviting the user to events or groups.
- Unfriend someone, which prevents the other person from posting on the user's timeline.

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK


- Block someone's messages, which means they will no longer be able to contact the user in Messenger or in Facebook chat. A user can also ignore a Messenger conversation, which automatically moves it out of the user's inbox.
- Unfollow someone, which means the person's post will not appear in News Feed. On Instagram, a user can prevent someone from commenting on the user's photos and videos and can also block someone from finding the user's profile, posts or story.

d. Does Facebook have an appeal process to challenge content decisions or decisions to suspend or deplatform users? If yes, please describe such process.

If someone believes that we have gotten a content moderation decision wrong, that person can generally appeal or is given the option to disagree with our decision. In some cases, we then re-review our decisions on those individual pieces of content.

In order to request re-review of a content decision we made, users are often given the option to "Request Review" or to provide feedback by stating they "Disagree with Decision." We try to make the opportunity to request this review or give this feedback clear, either via a notification or interstitial, but we are always working to improve.

Transparency in our appeals process is important, so we now include in our Community Standards Enforcement Report how much content people appealed and how much content was restored upon appeal. Gathering and publishing those statistics keeps us accountable to the broader community and enables us to continue improving our content moderation. For more information, see <https://transparency.facebook.com/community-standards-enforcement>.

We have also established an Oversight Board so people in the community can appeal our content decisions to a body that has independent judgment. The Oversight Board uses its independent judgment to decide some of our most significant and difficult cases, and the decisions it makes are binding.

2. Since January 2020, please list every Republican public official—federal, state, or local—Facebook has suspended or deplatformed.

We do not in the ordinary course of our operations track or maintain a list of the information you have requested. At Facebook, we are a platform for ideas across the political and ideological spectrum, and when we identify or learn of content that violates our policies, we remove that content regardless of who posted it. The political affiliation of the user generating the content has no bearing on that content assessment. Rather, decisions about whether to remove content are based on our Community Standards, which direct all reviewers when making decisions. We seek to write actionable policies that clearly distinguish between violating and non-violating content, and we seek to make the review process for reviewers as objective as possible.

3. Since January 2020, please list every Democrat public official—federal, state, or local—Facebook has suspended or deplatformed.

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK


Please see the response to your previous question.

4. Since January 2020, as it relates to heads of government and world leaders, please identify each account Facebook has suspended or deplatformed and identify the specific policy for such decisions.

Freedom of expression is a founding principle for Facebook, and we think it is important that people around the world hear from their elected officials and governmental leaders. All users, including world leaders, are subject to our policies, including our Community Standards, and we strive to enforce our policies consistently, without regard to political affiliation or the country from which a user hails.

When we identify or learn of content that violates our Community Standards, we remove that content, regardless of who posted it. Even if a politician or government official says it, if we determine that content may lead to violence or deprive people of their right to vote, we will take that content down. In 2018, we removed from our platform Senior General Min Aung Hlaing, the commander-in-chief of Myanmar's armed forces, and last month we removed the entire Myanmar military—the Tatmadaw. We have also removed content from government officials hailing from a number of countries including Brazil, India, Israel, Myanmar, the Philippines, and Turkey. This content was removed for violating our Community Standards, including our Violence and Incitement policy.

5. Without disclosing personally identifiable information, please disclose any content removed by Facebook related to Black Lives Matter riots and identify the number of accounts suspended or disabled for posting such content.

We remove content and track those removals based on which policies in our community standards they violate. We generally do not track content removals based on an incident that the content relates to, and therefore we are unable to identify the information requested in this question. For more information on our tracking of content removals, please see our Community Standards Enforcement Report at <https://transparency.facebook.com/community-standards-enforcement>.

6. On June 1, 2020, now-Vice President Kamala Harris posted "If you're able to, chip in now to the Minnesota Freedom Fund to help post bail for those protesting on the ground in Minnesota" and linked to an ActBlue Fund. Please explain how this post does not violate Facebook's policies.

We remove content that expresses substantive support—which includes fundraising—or praise for groups, leaders, or individuals involved in terrorist activity, organized hate, mass murder, human trafficking, and organized violence or criminal organizations.

Protesting is not considered organized violence under our policies, and the cited content does not violate our Community Standards.

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK



7. **As it relates to news articles on Facebook, please answer the following:**

- a. **Does Facebook reduce the distribution of every news article pending review by third-party fact checkers? If no, please explain Facebook's process for determining which news articles should have their distribution reduced.**
- b. **On October 14, 2020, Facebook decided to reduce distribution of a New York Post article titled "Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad" pending review of Facebook's third-party fact checkers. Please provide an update as to the third-party fact checkers determination.**

In 2019, we announced that, if we identify signals that a piece of content is false, we temporarily reduce its distribution in order to allow sufficient time for our independent, third-party fact-checkers to review and determine whether to apply a rating. Quick action is critical in keeping a false claim from going viral, and so we take this step to provide an extra level of protection against potential misinformation. These temporary demotions expire after seven days if the content has not been rated false by an independent fact-checker.

In the weeks leading up to the election, the Director of National Intelligence, the Head of the FBI, and the bipartisan leaders of the Senate Select Committee on Intelligence reminded Americans about the threat posed by foreign influence operations emanating from Russia and Iran. Along with their public warnings, and as part of the ongoing cooperation that tech companies established with government partners following the 2016 election, the FBI also privately warned tech companies to be on high alert for the potential of hack-and-leak operations carried out by foreign actors in the weeks leading up to November 3rd. We took these risks seriously.

In the case of the October 14 *New York Post* story, we were not able to verify whether the content was part of a foreign influence operation. Given the concerns raised by the FBI and others, we took steps consistent with our policies to slow the spread of suspicious content and provide fact-checkers the opportunity to assess it. However, at no point did we take any action to block or remove the content from the platform. People could—and did—read and share the Post's reporting while we had this temporary demotion in place. Consistent with our policy, after seven days, we lifted the temporary demotion on this content because it was not rated false by an independent fact-checker.

8. **Does Facebook have a process to communicate, consult, and coordinate with law enforcement to address illicit content? If so, please explain.**

We have a long history of working successfully with the Department of Justice, the FBI, state and local law enforcement, and other government agencies to address a wide variety of threats to our platform. We have been able to provide support to authorities around the world. We reach out to law enforcement when we see a credible threat of imminent harm. We contact federal, state, or local law enforcement depending on the specific circumstances of a threat. We also have robust processes in place to handle government requests we receive, and we disclose account records in accordance with

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK


our terms of service and applicable law. We have law enforcement response teams available around the clock to respond to emergency requests.

Leading up to the 2020 election, we met regularly with federal, state and local law enforcement officials and the intelligence community to allow us to better understand and respond to election-related concerns or threats. In connection with the events of January 6, we have also provided law enforcement with around-the-clock assistance, including real-time response during the Capitol attack and extensive support in identifying the insurrectionists so they can be brought to justice.

9. Does Facebook have a process to preserve evidence of illegal content on its platform to assist law enforcement? If so, please explain.

We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of formal legal process. Law enforcement may submit formal preservation requests through Facebook's Law Enforcement Online Request System (<https://www.facebook.com/records>) or by mail.

10. Does Facebook coordinate with Google and Twitter on any content decisions? If so, please identify the categories of such content decisions.

We make independent decisions on individual pieces of content or accounts according to our Community Standards.

Our Community Standards outline what is and is not allowed on Facebook. We base our policies on principles of voice, safety, dignity, authenticity, and privacy. We also publish our quarterly Community Standards Enforcement Report to give visibility into how we are doing at enforcing the Community Standards. Google and Twitter have their own content moderation policies and make content moderation decisions based on those policies.

As it relates to the events at the Capitol, we have been engaging with law enforcement and also discussing threats we are seeing on the platform with other industry participants to help keep our community safe. This is consistent with our practice of sharing terrorist threats and hashed content with Microsoft, Twitter, and YouTube through the Global Internet Forum to Counter Terrorism (GIFCT), which was designed to foster technical collaboration among member companies, advance relevant research, and share knowledge with smaller platforms. Since 2017, GIFCT's membership has expanded beyond the founding companies to include over a dozen diverse platforms committed to cross-industry efforts to counter the spread of terrorist and violent extremist content online. GIFCT is one way in which we manage communication with other companies about potential threats, including terrorism. Importantly, however, we do not coordinate on what actions to take. Each company makes those decisions for themselves.

11. Does Facebook coordinate with Google and Twitter on any decisions related to suspending or deplatforming users? If so, please explain.

Please see the response to your previous question.

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK


12. **As it relates to former-President Trump, please answer the following:**

- a. **Did Facebook coordinate with Google, Twitter, or any other tech company to make content decisions about his posts? If so, please explain.**
- b. **Did Facebook coordinate with Google, Twitter, or any other tech company to suspend or remove his account? If so, explain.**

Facebook did not coordinate with any other companies when deciding to place a feature block on former President Trump's page for 24 hours, when extending that action indefinitely.

We made the decision on our own, and consistent with our Community Standards, which inform how we moderate content. In this extraordinary case, we determined that former President Trump's posts, on balance, contributed to, rather than diminished, the risk of ongoing violence.

13. **Did Facebook coordinate with Google, Twitter, or any other tech company to make content decisions related to Black Lives Matter riots? If so, please explain.**

Please see the response to your Question 10.

14. **Did Facebook coordinate with Google, Twitter, or any other tech company to suppress the October 14, 2020 *New York Post* article titled "Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad"? If so, please explain.**

Please see the response to your Question 10.

15. **Does Facebook alter its algorithms to drive certain content or narratives based on the political leaning of such content? If so, please explain.**

At Facebook, we are a platform for ideas across the political and ideological spectrum, and we moderate content according to our published Community Standards to help keep users on the platform safe, reduce objectionable content, and ensure users participate on the platform responsibly. We are clear and transparent about what our standards are, and we seek to apply them to all of our users consistently.

We frequently make changes to the algorithms that drive News Feed ranking in an effort to improve people's experience on Facebook. For example, in 2018, we responded to feedback from our community that public content—posts from businesses, brands, and media—was crowding out the personal moments that lead us to connect more with each other. As a result, we moved from focusing only on helping users find relevant content to helping them have more meaningful social interactions. This meant that users began seeing more content from their friends, family, and Groups. We also reduce the distribution of some problematic types of content, including content that users may find

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK


spammy or low-quality, such as clickbait headlines and links to low-quality webpages like ad farms.

As we said last month, we're listening to users who have told us they are seeing too much political content and are looking at how to support user choice while improving the experience on Facebook.

16. Please explain any efforts Facebook has undertaken to support local news and traditional media.

We at Facebook care a great deal about making sure that a sustainable news and journalism ecosystem can thrive because it is important to the societies and communities we serve. We invest in products, programs and partnerships to connect people to diverse sources of news and information that educate and entertain them. These investments serve communities on and off Facebook.

We are proud that news publishers derive significant value from our site. We have a free platform and custom-built tools that derive unique value to publishers and journalists of all sizes, helping them build sustainable business models. This is why so many publishers voluntarily post their own content to Facebook with links to their news stories. That engagement links directly back to the publisher's site and generates revenue opportunities for those publishers. And in October 2019, we announced the U.S. launch of Facebook News—a dedicated news destination within the Facebook app. We invested millions of dollars to obtain access to new stories for this surface.

In addition to the value the site drives to publishers who choose to use it, we support local news and traditional media in other ways as well. During the COVID-19 pandemic, we announced a \$100 million investment (<https://www.facebook.com/journalismproject/coronavirus-update-news-industry-support>) to support the news industry—\$25 million in emergency grant funding for local news through the Facebook Journalism Project, and \$75 million in additional marketing spend to move money over to news organizations around the world.

We have a long record of investment in this space. In January 2017, we announced the Facebook Journalism Project, an initiative to establish stronger ties between Facebook and the news industry. Over the past three years, this project has invested more than \$425 million to help the journalism industry by developing news products; providing grants, training, and tools for journalists; and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Facebook Journalism Project, we have met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

This investment includes support for organizations like the Pulitzer Center, Report for America, the Knight-Lenfest Local News Transformation Fund, the Local Media Association and Local Media Consortium, the American Journalism Project, NewsMatch, and the Community News Project.

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK


Also through the Facebook Journalism Project, in February 2018, we launched our Local News Subscriptions Accelerator, a pilot program designed to help news publishers grow their digital subscription revenues with the help of professional training and grant funding to accelerate innovation. In August 2018, we introduced our Membership Accelerator, another program designed to help non-profit news organizations and local, independent publishers with membership models to build sustainable businesses by providing supporters access to exclusive content and experiences through memberships. These programs have generated millions of dollars in recurring, sustainable revenue for local publishers.

In January 2019, we increased our investment in these programs in the United States and expanded the Accelerator training model globally. Hundreds of publishers around the world are now leveraging these resources to transform their businesses.

* * *

Thank you for the opportunity to answer your questions.

Sincerely,

Facebook, Inc.

575 7TH STREET NW
STE 700
WASHINGTON, D.C.
20004

FACEBOOK


3/25/2021 Twitter says no to law enforcement protest policing tool | Engadget

Sections ▾ Login

Gear Gaming Entertainment Products Tomorrow Audio Video Deals Buyer's Guide

f t

Twitter says no to law enforcement protest policing tool

Media Sonar was used to track protestors by hashtag and keywords.



T. Seppala | 12.10.16
@timseppala

December 10th, 2016

✉ f t

In this article: aclu, api, blacklivesmatter, culture, cyberspying, geofeedia, internet, mediasonar, mikebrown, socialmediasurveillance, surveillance, twitter



Mike Blake / Reuters

Twitter has cut off access for a tool that law enforcement was using to monitor the social network for protest-specific keywords. Those included "Mikebrown," "Blacklivesmatter" and "imunarmed" according to documents obtained by *The Daily Dot*. Media Sonar has been selling [social media surveillance software](#) to police departments for thousands of dollars. Twitter, for its part, cut off the firm's API keys in October and has vowed to

Champions
of actually
having a
nice day

Learn more



3/25/2021 Twitter says no to law enforcement protest policing tool | Engadget

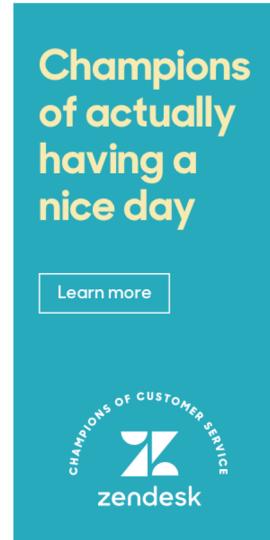
Sections ▾ Login 

Remember, using Twitter's data feed for spying and surveillance is a violation of the service's developer agreement. With the list of keywords, the Northern California chapter of the American Civil Liberties Union's evidence suggests that Media Sonar was selling itself as a way to monitor African Americans specifically. One column groups keywords together under a heading named "Mike Brown Related." Mike Brown was the unarmed black teenager shot by a white police officer in Ferguson, Missouri in 2014.

[Further documents](#) (PDF) show that the firm pitches itself as a way to "avoid the warrant process when identifying social media accounts for particular individuals."

What's more, the company apparently directed law enforcement officials to not mention the Media Sonar by name in court, instead using "proprietary search engine" or "internet tools" when pressed for information under oath. It's a far cry from issuing cyanide capsules to its customers, but still pretty telling of the company's intent to keep its secrets safe.

This isn't the first time Twitter has done this, and it likely won't be the last organization to [mine social media data](#) for policing. This fall, Facebook, Instagram and Twitter cut off access to tracking systems [from Geofeedia](#). We've reached out to Twitter for more information and will update this post should it arrive.



March 24, 2021

Hon. Frank Pallone
Chairman
Energy and Commerce Committee
U.S. House of Representatives
2107 Rayburn HOB
Washington, DC 20515

Hon. Cathy McMorris Rodgers
Ranking Member
Energy and Commerce Committee
U.S. House of Representatives
1035 Longworth HOB
Washington, DC 20515

Dear Chairman Pallone, Ranking Member McMorris Rodgers, and Members of the House Energy and Commerce Committee,

The undersigned organizations commend the Committee for holding today's hearing entitled "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation" and for giving our communities the chance to hear from tech CEOs on a national stage. Our organizations write today to reiterate the urgent need for action against Spanish-language disinformation on social media platforms. Disinformation is a tactic of white supremacy and oppression, and manifests into tangible harms, including voter suppression and hate crimes. It is beyond time for social media platforms to be held accountable for their role in the harassment endured and lives lost at the hands of disinformation, hate, and extremism.

In November 2020, many of the undersigned organizations [sent a letter](#) to Facebook founder and CEO Mark Zuckerberg, raising the issue of rampant Spanish-language disinformation on the platform. In particular, our groups highlighted consistent inaction by

Facebook to address election, voting, and pandemic-related misinformation, including content with calls to arms that fuel the fires of white supremacy and hate. In February 2021, we received a response from Kevin Martin, Facebook Vice President of Public Policy, in lieu of a response from Mr. Zuckerberg. Mr. Martin's response, while thorough on other Facebook-led initiatives, did not fully address the scope of our concerns, and did not prioritize the seriousness of the ongoing issue. For example, Mr. Martin referenced an account flagged by the undersigned groups merely to reiterate that the account *did not* violate Facebook's content policies, despite it being a repeat spreader of false information and hate. This, unfortunately, is one link in a long chain of Facebook's empty promises and rehearsed responses.

For the better part of the last year, our organizations have used our limited resources, during a global pandemic, to garner action from Facebook's leadership. It should be incumbent upon Facebook to take action to protect all of its users from white supremacy, instead of brushing off civil rights and social justice advocates who continue to spend our emotional, physical, and political capital to repeatedly inform Facebook that white supremacy and disinformation online are killing our communities.

After months of inaction and lackluster dialogue from Facebook, the National Hispanic Media Coalition, Free Press, and the Center for American Progress developed a [Spanish-language Disinformation Action Plan](#), making the following demands from Facebook:

1. Hire and publicly identify a C-suite position to oversee U.S. Spanish-language content moderation policy and enforcement.
2. Publicly explain the translation process of the content moderation algorithms, including how the algorithms are trained and audited to ensure proactive detection, reporting, and processing of Spanish-language content.
3. Clarify whether Facebook's content moderators evaluate content in-language, via translation, or both. Explain precisely how many US-based Spanish-language content

moderators the company employs, as well as the overall number of US-based content moderators. In each case, provide the breakdown of between direct employees and contractors involved in moderation.

4. Publicly share the materials that are used to train content moderators of U.S.-based Spanish-language content.

At the time of this letter's drafting, Facebook has not committed to any of our demands, nor have they provided any new information or detail (neither publicly nor privately) as to their internal progress to address Spanish-language disinformation.

We would like to thank Congressman Tony Cárdenas and Congressman Darren Soto for their support in the fight to close the Spanish-language misinformation gap on Facebook. We urge the Members of this Committee to support our Action Plan, and to consider actions in addition to this hearing to hold Facebook and all social media companies accountable for the real-life harm created by their business models. We thank the Committee for their commitment to the Spanish-speaking and Latinx communities, and ask that you join us in saying: Ya Basta, Facebook—*enough is enough*.

Sincerely,

Anti-Defamation League

Free Press Action

Fundamedios, Inc.

Global Project Against Hate and Extremism

MediaJustice

National Hispanic Media Coalition

National Latinx Psychological Association

353

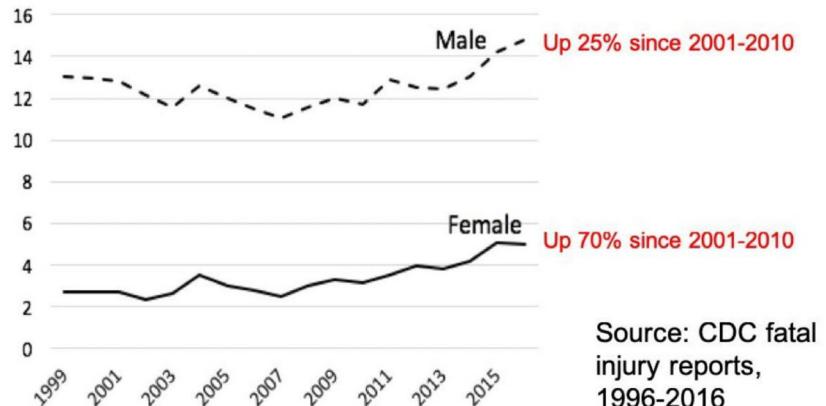
TransLatin@ Coalition

UnidosUS

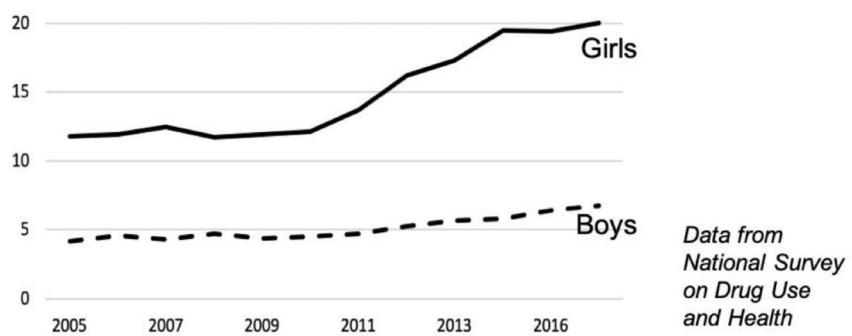
United Church of Christ, OC Inc.

United States Hispanic Leadership Institute

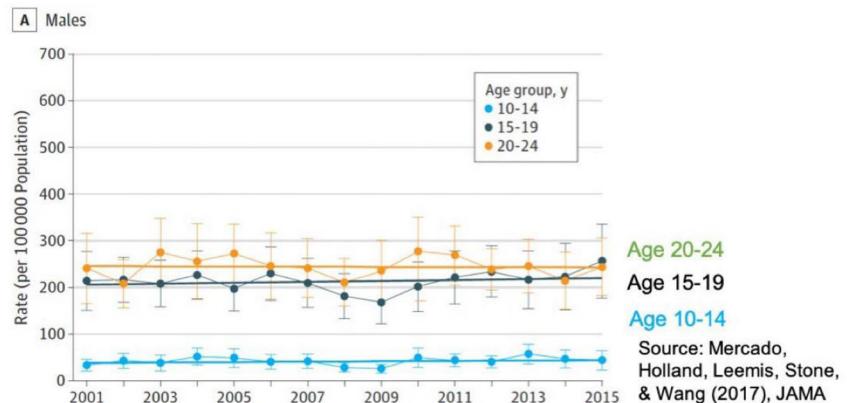
Suicide rate per 100,000, by sex, ages 15-19



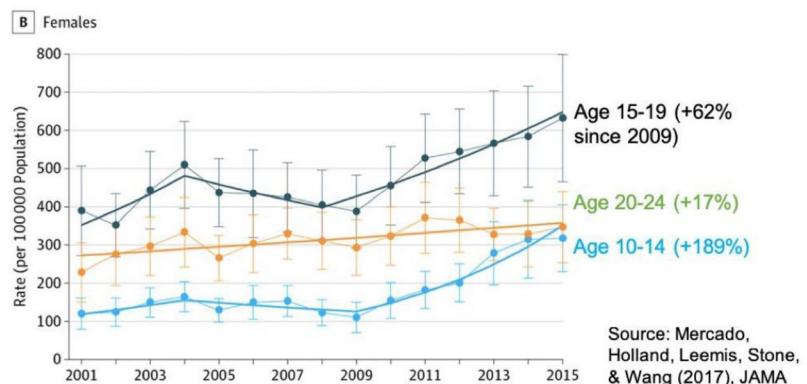
Persons Aged 12-17 Who Had At Least One Major Depressive Episode in the Past Year (%), By Gender



Hospital Admissions for non-fatal self-harm: Boys



Hospital Admissions for non-fatal self-harm: Girls



Source: Mercado,
Holland, Leemis, Stone,
& Wang (2017), JAMA

Figure 2. Suicide and homicide death rates among children and adolescents aged 10–14: United States, 2000–2017

