TIKTOK: HOW CONGRESS CAN SAFEGUARD AMERICAN DATA PRIVACY AND PROTECT CHILDREN FROM ONLINE HARMS

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 23, 2023

Serial No. 118–13

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

U.S. GOVERNMENT PUBLISHING OFFICE
53–839 PDF WASHINGTON : 2023

COMMITTEE ON ENERGY AND COMMERCE

CATHY MCMORRIS RODGERS, Washington
Chair

MICHAEL C. BURGESS, Texas
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
LARRY BUCSHON, Indiana
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida
JOHN R. CURTIS, Utah
DEBBBIE LESKO, Arizona
GREG PENCE, Indiana
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania
KELLY ARMSTRONG, North Dakota, *Vice Chair*
RANDY K. WEBER, SR., TEXAS
RICK W. ALLEN, Georgia
TROY BALDERSON, Ohio
RUSS FULCHER, Idaho
AUGUST PFLUGER, Texas
DIANA HARSHBARGER, Tennessee
MARIANNETTE MILLER–MEEKS, Iowa
KAT CAMMACK, Florida
JAY OBERNOLTE, California

FRANK PALLONE, JR., New Jersey
Ranking Member
ANNA G. ESHOO, California
DIANA DEGETTE, Colorado
JAN SCHAKOWSKY, Illinois
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
PAUL TONKO, New York
YVETTE D. CLARKE, New York
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
ANGIE CRAIG, Minnesota
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas

PROFESSIONAL STAFF

NATE HODSON, *Staff Director*
SARAH BURKE, *Deputy Staff Director*
TIFFANY GUARASCIO, *Minority Staff Director*

C O N T E N T S

WITNESSES

SUBMITTED MATERIAL

[1] Mr. Chew's responses have been retained in committee files and are available at https://docs.house.gov/meetings/IF/IF00/20230323/115519/HHRG-118-IF00-Wstate-ChewS-20230323-SD030.pdf.

[2] The information has been retained in committee files and is included in the Documents for the Record at https://docs.house.gov/meetings/IF/IF00/20230323/115519/HHRG-118-IF00-20230323-SD030.pdf.

---

[2] The information has been retained in committee files and is included in the Documents for the Record at https://docs.house.gov/meetings/IF/IF00/20230323/115519/HHRG-118-IF00-20230323-SD030.pdf.

TIKTOK: HOW CONGRESS CAN SAFEGUARD AMERICAN DATA PRIVACY AND PROTECT CHILDREN FROM ONLINE HARMS

THURSDAY, MARCH 23, 2023

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
WASHINGTON, DC.

The committee met, pursuant to call, at 10:01 a.m. in the John D. Dingell Room 2123, Rayburn House Office Building, Hon. Cathy McMorris Rodgers (chair of the committee) presiding.

Members present: Representatives Rodgers, Burgess, Latta, Guthrie, Griffith, Bilirakis, Johnson, Hudson, Walberg, Carter, Duncan, Palmer, Dunn, Curtis, Lesko, Pence, Crenshaw, Joyce, Armstrong, Weber, Allen, Balderson, Fulcher, Pfluger, Harshbarger, Miller-Meeks, Cammack, Obernolte, Pallone (committee ranking member), Eshoo, DeGette, Schakowsky, Matsui, Castor, Sarbanes, Tonko, Clarke, Cárdenas, Ruiz, Peters, Dingell, Veasey, Kuster, Barragán, Blunt Rochester, Soto, Craig, Schrier, Trahan, and Fletcher.

Staff present: Kate Arey, Digital Director; Sean Brebbia, Chief Counsel, Oversight and Investigations; Jolie Brochin, Clerk, Health; Deep Buddharaju, Senior Counsel, Oversight and Investigations; Sarah Burke, Deputy Staff Director; Michael Cameron, Professional Staff Member, Innovation, Data, and Commerce; Lauren Eriksen, Clerk, Oversight and Investigations; Sydney Greene, Director of Operations; Jack Heretik, Press Secretary; Slate Herman, Counsel, Communications and Technology; Jessica Herron, Clerk, Innovation, Data, and Commerce; Nate Hodson, Staff Director; Tara Hupman, Chief Counsel; Noah Jackson, Clerk, Communications and Technology; Sean Kelly, Press Secretary; Peter Kielty, General Counsel; Emily King, Member Services Director; Chris Krepich, Press Secretary; Tim Kurth, Chief Counsel, Innovations, Data, and Commerce; Giulia Leganski, Professional Staff Member, Communications and Technology; Kate O'Connor, Chief Counsel, Communications and Technology; Kaitlyn Peterson, Clerk, Energy and Environment; Brannon Rains, Professional Staff Member, Innovation, Data, and Commerce; Olivia Shields, Communications Director; Lacey Strahm, Fellow, Innovation, Data, and Commerce; Michael Taggart, Policy Director; Teddy Tanzer, Senior Counsel, Innovation, Data, and Commerce; Dray Thorne, Director of Information Technology; Hannah Anton, Minority Staff Assistant; Ian Barlow, Minority FTC Detailee; Jennifer Epperson, Minority Chief Counsel, Communications and Technology; Austin Flack, Minority Junior Professional Staff Member; Waverly Gordon, Mi-

nority Deputy Staff Director and General Counsel; Daniel Greene, Minority Professional Staff Member; Tiffany Guarascio, Minority Staff Director; Perry Hamilton, Minority Member Services and Outreach Manager; Lisa Hone, Minority Chief Counsel, Innovation, Data, and Commerce; Liz Johns, Minority GAO Detailee; Mackenzie Kuhl, Minority Digital Manager; Una Lee, Minority Chief Health Counsel; Will McAuliffe, Minority Chief Counsel, Oversight and Investigations; Dan Miller, Minority Professional Staff Member; Joe Orlando, Minority Senior Policy Analyst; Christina Parisi, Minority Professional Staff Member; Caroline Rinker, Minority Press Assistant; Harry Samuels, Minority Oversight Counsel; Michael Scurato, Minority FCC Detailee; Andrew Souvall, Minority Director of Communications, Outreach, and Member Services; Johanna Thomas, Minority Counsel; Caroline Wood, Minority Research Analyst; and C.J. Young, Minority Deputy Communications Director.

Mrs. RODGERS. The committee will come to order. Before I begin, I would like to take a moment to address the guests in the audience.

First of all, thank you for coming. We think engaged citizens are welcome and a valuable part of the political process. I do want to remind the guests in the audience that the Chair is obliged under the House rules and the rules of the committee to maintain order and preserve decorum in the committee room. I know that we have deep feelings on these issues and that we all may not agree on everything, but I ask that we abide by these rules and be respectful of our audience members, our viewers, and our witnesses. The Chair appreciates the audience cooperation in maintaining order as we have a full discussion on these important issues.

The Chair recognizes herself for 5 minutes for an opening statement.

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

Mr. Chew, you are here because the American people need the truth about the threat TikTok poses to our national and personal security. TikTok collects nearly every data point imaginable, from people's location to what they type and copy, who they talk to, biometric data, and more. Even if they have never been on TikTok, your trackers are embedded in sites across the Web. TikTok surveils us all, and the Chinese Communist Party is able to use this as a tool to manipulate America as a whole.

We do not trust TikTok will ever embrace American values, values for freedom, human rights, and innovation. TikTok has repeatedly chosen the path for more control, more surveillance, and more manipulation. Your platform should be banned.

I expect today you will say anything to avoid this outcome, like you are 100 percent responsible for what TikTok does, that you suddenly endorse a national data privacy standard, that Project Texas is more than a marketing scheme, that TikTok doesn't harm our innocent children, or that your ties to the Chinese Communist Party through ByteDance is just a myth. We aren't buying it.

In fact, when you celebrate the 150 million American users on TikTok, it emphasizes the urgency for Congress to act. That is 150 million Americans that CCP can collect sensitive information on, and control what we ultimately see, hear, and believe.

TikTok has repeatedly been caught in the lie that it does not answer to the CCP through ByteDance. Today the CCP's laws require Chinese companies like ByteDance to spy on their behalf. That means any Chinese company must grant the CCP access and manipulation capabilities as a design feature. Right now ByteDance is under investigation by the DoJ for surveilling American journalists, both digital activity and physical movements, through TikTok.

We also know that many of your employees still report directly to Beijing. Internal recordings reveal there is a back door for China to access user data across the platform. Your employees said, "Everything is seen in China."

A gateway to spy is not the only way TikTok and ByteDance can do the bidding of the CCP. TikTok has helped erase events and people China wants the world to forget. It has even censored an American teenager who exposed CCP's genocide and torture of Uyghur Muslims. The facts show that ByteDance is beholden to the CCP, and ByteDance and TikTok are one and the same.

TikTok also targets our children. The For You algorithm is a tool for TikTok to own their attention and prey on their innocence. Within minutes of creating an account, your algorithm can promote suicide, self-harm, and eating disorders to children. It encourages challenges for them to put their lives in danger and allows adults to prey on our beautiful, beloved daughters.

It is also a portal for drug dealers to sell illicit fentanyl that China has banned, yet is helping Mexican cartels produce, send across our border, and poison our children. In China the CCP proactively prohibits this type of TikTok content that promotes death and despair to kids.

From the data it collects to the content it controls, TikTok is a grave threat of foreign influence in American life. It has been said it is like allowing the Soviet Union the power to produce Saturday morning cartoons during the Cold War, but much more powerful and much more dangerous.

Banning your platform will address the immediate threats. Make no mistake, this committee is also looking to the future. America needs to be prepared to stop the next technological tool or weapon China will use for its own strategic gain. We must prevent any app, website, and platform like TikTok from ever spying on Americans again, and we must provide the strongest protections possible for our children.

That is why this committee is leading on a national privacy and data security standard. It restricts sensitive American data from reaching our adversaries to begin with, and what Big Tech and data brokers collect, process, store, and sell. It makes it illegal for any platform to track and target children under 17.

Mr. Chew, the committee has requested that TikTok appear before us for a long time. For those we serve, we are glad the day has finally come. Today the world is watching. ByteDance is watching. The Chinese Communist Party is watching. But the answers you owe are to the American people, a free people who cherish

their God-given unalienable, rights to life, liberty, and the pursuit of happiness for all. They deserve the truth.

Complete honesty is the standard and the law you are being held to before this committee as we seek to get answers and a full understanding of what happens at TikTok under your watch. Thank you.

[The prepared statement of Mrs. Rodgers follows:]

Opening Statement of Chair Cathy McMorris Rodgers
As Prepared for Delivery
Committee on Energy and Commerce
Hearing entitled "TikTok: How Congress Can Safeguard American Data Privacy And Protect Children From Online Harms"
March 23, 2023

Mr. Chew, you are here because the American people need the truth about the threat TikTok poses to our national and personal security.

TikTok collects nearly every data point imaginable, from people's location, to what they type and copy, who they talk to, biometric data, and more.

Even if they've never been on TikTok, your trackers are embedded in sites across the web.

TikTok surveils us all and the Chinese Communist Party (CCP) is able to use this as a tool to manipulate America as a whole."

We do not trust TikTok will ever embrace American values—values for freedom, human rights, and innovation.

TikTok has repeatedly chosen the path for more control, more surveillance, and more manipulation.

Your platform should be banned.

I expect today you'll say anything to avoid this outcome.

Like that you are 100 percent responsible for what TikTok does, that you suddenly endorse a national data privacy standard, that Project Texas is more than just a marketing scheme, that TikTok doesn't harm our innocent children, or that your ties to the Chinese Communist Party through ByteDance is just a myth.

We aren't buying it.

In fact, when you celebrate the 150 million American users on TikTok it emphasizes the urgency for Congress to act.

That is 150 million Americans that CCP can collect sensitive information on and control what we ultimately see, hear, and believe."

TikTok has repeatedly been caught in the lie that it does not answer to the CCP through ByteDance.

Today, the CCP's laws require Chinese companies like ByteDance to spy on their behalf.

That means any Chinese company must grant the CCP access and manipulation capabilities as a design feature.

Right now, ByteDance is under investigation by the DOJ for surveilling American journalists—both digital activity and physical movements through TikTok.

We also know that many of your employees still report directly to Beijing.

Internal recordings reveal there is a backdoor for China to access user data across the platform.

Your employees said quote, 'everything is seen in China.'

A gateway to spy is not the only way TikTok and ByteDance can do the bidding of the CCP.

TikTok has helped erase events and people China wants the world to forget.

It has even censored an American teenager, who exposed the CCP's genocide and torture of Uyghur Muslims.

The facts show that ByteDance is beholden to the CCP and ByteDance and TiKTok are one in the same."

TikTok also targets our children.

The 'For You' algorithm is a tool for TikTok to own their attention and prey on their innocence.

Within minutes of creating an account, your algorithm can promote suicide, self-harm, and eating disorders to children.

It encourages challenges for them to put their lives in danger and allows adults to prey on our beautiful, beloved daughters.

It's also a portal for drug dealers to sell illicit fentanyl that China has banned, yet, is helping Mexican cartels produce, send across our border, and poison our children.

In China, the CCP proactively prohibits this type of TikTok content that promotes death and despair to kids."

From the data it collects to the content it controls, TikTok is a grave threat of foreign influence in American life.

It's been said it is like allowing the Soviet Union the power to produce Saturday morning cartoons during the Cold War but much more powerful and much more dangerous.

Banning your platform will address the immediate threats.

Make no mistake, this Committee is also looking to the future too.

America needs to be prepared to stop the next technological tool or weapon China will use for its own strategic gain.

We must prevent any app, website, and platform like TikTok from ever spying on Americans again and we must provide the strongest protections possible for our children.

That is why this Committee is leading on a national privacy and data security standard.

It restricts sensitive American data from reaching our adversaries to begin with and what Big Tech and data brokers collect, process, store, and sell.

It makes it illegal for any platform to track and target children under 17."

Mr. Chew, the Committee has requested that TikTok appear before us for a long time.

For those we serve, we are glad this day has finally come.

Today, the world is watching.

ByteDance is watching.

The Chinese Communist Party is watching.

But the answers you owe are to the American people, a free people who cherish their God-given unalienable rights to life, liberty, and the pursuit of happiness for all.

They deserve the truth.

Complete honesty and the law is the standard you are being held to before this Committee as we seek to get answers and a full understanding of what happens at TikTok under your watch.

Mrs. RODGERS. The Chair now recognizes the ranking member, Mr. Pallone, for 5 minutes.

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

Mr. PALLONE. Thank you, Madam Chair, and let me say that I agree with much of what you just said, and I certainly appreciate your enthusiasm and your commenting on being a mother and concerned about children. And I am glad that we are having this hearing today.

Big Tech has transformed the information superhighway into a super spreader of harmful content, invasive surveillance practices, and addictive and damaging design features. Data is Big Tech's most valuable commodity, and by collecting far more user data than they need, Big Tech platforms can use, share, and sell information to generate billions of dollars in revenue.

Today the American people are powerless to stop this invasion of their privacy, and we can't wait any longer to pass comprehensive national privacy legislation that puts people back in control of their data. We must hold Big Tech accountable for its actions, and transparency is critical to that accountability.

In the past several Congresses, this committee has heard from senior executives of other social media platforms about troubling and repeated instances where they put profits over people. Now, today, we intend to bring more transparency to TikTok, which is controlled by its Beijing, communist-based parent company, ByteDance. And while TikTok videos provide a new, fun way for people to express their creativity and enjoy the videos of others, the platform also threatens the health, privacy, and security of the American people. And I am not convinced that the benefits outweigh the risks that it poses to Americans in its present form.

More than 130 million people in the United States use TikTok every month, including two-thirds of American teenagers. TikTok collects and compiles vast troves of valuable personal information to create an addictive algorithm that is able to predict with uncanny accuracy which videos will keep users scrolling, even if the content is harmful, inaccurate, or feeds destructive behavior or extremist beliefs.

Now, the combination of TikTok's Beijing, communist-based China ownership and its popularity exacerbates its danger to our country and to our privacy. The Chinese Communist government can compel companies based in Beijing like TikTok to share data with the communist government through existing Beijing law or coercion.

National security experts are sounding the alarm, warning that the Chinese Communist government could require TikTok to compromise device security, maliciously access American user data, promote pro-Communist propaganda, and undermine American interests. Disinformation campaigns could be launched by the Chinese Communist government through TikTok, which has already become rife with misinformation and disinformation, illegal activities, and hate speech. A recent report found that 20 percent of

TikTok search results on prominent news topics contain misinformation.

Social media's profitability depends on growth and engagement. More eyes on their content for longer time leads to more advertising dollars and revenue generation. Addictive algorithms are fine-tuned to optimize growth and engagement without necessarily taking into account potential harms to users.

Children and teens are particularly vulnerable. Frequent online use of interactive media on digital devices is associated with increased levels of depression among middle and high school students. Research has found that TikTok's addictive algorithms recommend videos to teens that create and exacerbate feelings of emotional distress, including videos promoting suicide, self-harm, and eating disorders.

Public outrage and hollow apologies alone are not going to rein in Big Tech. Congress has to enact laws protecting the American public from such online harms, and we simply cannot wait any longer to pass the comprehensive privacy legislation that I authored with then ranking member, now Chair Rodgers, last Congress that overwhelmingly advanced out of the committee. It ensures that companies, wherever they live—it ensures, I should say, that consumers, wherever they live in this country, will have meaningful control over their personal information.

Our legislation establishes baseline data minimization requirements, ensuring that companies only collect, process, and transfer data necessary to provide a service. And it provides heightened privacy protections for children and teenagers. So I think it is time to make this legislation the law of the land.

And we also have to examine the reforms needed to section 230 of the Communications Decency Act. The liability shield for social media platforms has for too long been abused and led to a lack of accountability for social media platforms. So I hope we can find a bipartisan path forward on that issue too—and I think you are having a hearing next week on it—so we can stop the very real harms to our country and democracy under the current law.

I look forward to the discussion today as we continue to bring accountability to Big Tech.

And let me say to Mr. Chew I know this is about TikTok, but I am focusing all my attention not only on TikTok but on these concerns, wide concerns about social media and the protection of privacy.

[The prepared statement of Mr. Pallone follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.

Hearing on "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms"

March 23, 2023

Big Tech has transformed the information superhighway into a superspreader of harmful content, invasive surveillance practices, and addictive and damaging design features. Data is Big Tech's most valuable commodity. And by collecting far more user data than they need, Big Tech platforms can use, share, and sell information to generate billions of dollars in revenue. Today, the American people are powerless to stop this invasion of their privacy. We can't wait any longer to pass comprehensive, national privacy legislation that puts people back in control of their data.

We must hold Big Tech accountable for its actions, and transparency is critical to that accountability. In the past several Congresses, this Committee has heard from senior executives of other social media platforms about troubling and repeated instances where they've put profits over people.

Today we intend to bring more transparency to TikTok, which is controlled by its Beijing Communist-based parent company ByteDance. While TikTok videos provide a new, fun way for people to express their creativity and enjoy the videos of others, the platform also threatens the health, privacy, and security of the American people. And I am not convinced that the benefits outweigh the risks that it poses to Americans in its present form.

More than 130 million people in the United States use TikTok every month, including two-thirds of American teenagers.

TikTok collects and compiles vast troves of valuable personal information to create an addictive algorithm that is able to predict with uncanny accuracy which videos will keep users scrolling—even if the content is harmful, inaccurate, or feeds destructive behavior or extremist beliefs.

The combination of TikTok's Beijing Communist-based ownership and its popularity exacerbates its dangers to our country and to our privacy. The Chinese Communist government can compel companies based in Beijing, like TikTok, to share data with the Communist government through existing Beijing law or coercion. National security experts are sounding the alarm, warning that the Chinese Communist government could require TikTok to compromise device security, maliciously access American user data, promote pro-Communist propaganda, and undermine American interests.

Disinformation campaigns could be launched by the Chinese Communist government through TikTok, which has already become rife with misinformation and disinformation, illegal activities, and hate speech. A recent report found that 20 percent of TikTok search results on prominent news topics contained misinformation.

Social media's profitability depends on growth and engagement—more eyes on their content for longer time leads to more advertising dollars and revenue generation. Addictive algorithms are fine-tuned to optimize growth and engagement without necessarily taking into account potential harms to users.

Children and teens are particularly vulnerable. Frequent online use of interactive media on digital devices is associated with increased levels of depression among middle and high school students. Research has found that TikTok's addictive algorithms recommend videos to teens that create and exacerbate feelings of emotional distress, including videos promoting suicide, self-harm, and eating disorders.

Public outrage and hollow apologies alone are not going to rein in Big Tech. Congress has to enact laws protecting the American public from such online harms.

We simply cannot wait any longer to pass the comprehensive privacy legislation I authored with then Ranking Member Rodgers last Congress that overwhelmingly advanced out of the Committee. It ensures that consumers—wherever they live in this country—will have meaningful control over their personal information. Our legislation establishes baseline data minimization requirements, ensuring that companies only collect, process, and transfer data necessary to provide a service. And it provides heightened privacy protections for children and teenagers.

It's time we make this legislation the law of the land. We must also examine the reforms needed to Section 230 of the Communications Decency Act. The liability shield for social media platforms has for too long been abused and led to a lack of accountability for social media platforms. I hope we can find a bipartisan path forward on that issue too, so we can stop the very real harms to our country and democracy under the current law.

I look forward to the discussion today as we continue bringing accountability to Big Tech.

Mr. PALLONE. And with that, I yield back. Thank you again, Madam Chair, for having this very important hearing.

Mrs. RODGERS. Our witness today is Mr. Shou Chew, chief executive officer of TikTok.

You are recognized for 5 minutes.

STATEMENT OF SHOU CHEW, CHIEF EXECUTIVE OFFICER, TIKTOK, INC.

Mr. CHEW. Thank you. Chair Rodgers, Ranking Member Pallone, members of the committee, thank you for your time.

I am Shou Chew, and I am from Singapore. That is where I was born, as were my parents. And after serving in Singapore's military, I moved to the U.K. to attend college, and then here to the U.S. to attend business school. I actually met my wife here. By the way, she was just born a few miles away from here in Virginia.

Two years ago I became the CEO of TikTok. Today we have more than a billion monthly active users around the world, including over 150 million in the United States. Our app is a place where people can be creative and curious, and where close to 5 million American businesses, mostly small businesses, go to find new customers and to fuel their growth.

Now, as TikTok has grown, we have tried to learn the lessons of companies that have come before us, especially when it comes to the safety of teenagers. While the vast majority of people on TikTok are over 18, one of—and one of our fastest-growing demographics are people over 35, we have spent a lot of time adopting measures to protect teenagers. Many of those measures are firsts for the social media industry.

We forbid direct messaging for people under 16, and we have a 16-minute watch time by default for those under 18. We have a suite of family pairing tools so that parents can participate in their teens' experience and make the choices that are right for their family.

We want TikTok to be a place where teenagers can come to learn, which is why we recently launched a feed that exclusively features educational videos about STEM. STEM videos already have over 116 billion views on TikTok, and I think TikTok is inspiring a new generation to discover a passion for math and science.

I would also like to talk about national security concerns that you have raised that we take very, very seriously. Let me start by addressing a few misconceptions about ByteDance, of which we are a subsidiary. ByteDance is not owned or controlled by the Chinese Government. It is a private company. Sixty percent of the company is owned by global institutional investors, 20 percent is owned by the founder, and 20 percent owned by employees around the world. ByteDance has five board members; three of them are American.

Now, TikTok itself is not available in mainland China. We are headquartered in Los Angeles and in Singapore, and we have 7,000 employees in the U.S. today. Still, we have heard important concerns about the potential for unwanted foreign access to U.S. data and potential manipulation of the TikTok U.S. ecosystem. Our approach has never been to dismiss or trivialize any of these concerns. We have addressed them with real action. Now, that is what

we have been doing for the last 2 years: building what amounts to a firewall that seals off protected U.S. user data from unauthorized foreign access.

The bottom line is this: American data stored on American soil by an American company overseen by American personnel. We call this initiative Project Texas. That is where Oracle is headquartered. Today U.S. TikTok data is stored, by default, in Oracle's servers. Only vetted personnel operating in a new company called TikTok U.S. Data Security can control access to this data.

Now, additionally, we have plans for this company to report to an independent American board with strong security credentials.

Now there is still some work to do. We have legacy U.S. data sitting in our servers in Virginia and in Singapore. We are deleting those, and we expect that to be complete this year. When that is done, all protected U.S. data will be under the protection of U.S. law and under the control of the U.S.-led security team. This eliminates the concern that some of you have shared with me that TikTok user data can be subject to Chinese law.

This goes further, by the way, than what any other company in our industry has done.

We will also provide unprecedented transparency and security for the source code for the TikTok app and recommendation engine. Third-party validators like Oracle and others will review and validate our source code and algorithms. This will help ensure the integrity of the code that powers what Americans see on our app.

We will further provide access to researchers, which helps them study and monitor our content ecosystem. Now, we believe we are the only—the only—company that offers this level of transparency.

Now, trust is about actions we take. We have to earn that trust with decisions we make for our company and our products. The potential security, privacy, content manipulation concerns raised about TikTok are really not unique to us. The same issues apply to other companies. We believe what is needed are clear, transparent rules that apply broadly to all tech companies. Ownership is not at the core of addressing these concerns.

Now, as I conclude, there are more than 150 million Americans who love our platform, and we know we have a responsibility to protect them, which is why I am making the following commitments to you and to all our users.

Number one: We will keep safety, particularly for teenagers, as a top priority for us.

Number two: We will firewall protect U.S. data from unwanted foreign access.

Number three: TikTok will remain a place for free expression and will not be manipulated by any government.

And fourth, we will be transparent and we will give access to third-party independent monitors to remain accountable for our commitments.

I will be grateful for any feedback that you have, and I look forward to your questions. Thank you very much.

[The prepared statement of Mr. Chew follows:]

Testimony Before the U.S. House Committee on Energy and Commerce

Written Statement of Testimony

Testimony of Shou Chew

Chief Executive Officer, TikTok Inc.

March 23, 2023

Chair Rodgers, Ranking Member Pallone, and Members of the Committee:

Thank you for the opportunity to appear before you today to talk about TikTok and our mission to inspire creativity and bring joy to more than 1 billion people worldwide. I look forward to discussing what makes TikTok so special to the diverse audiences it serves, as well as our efforts to promote minor safety, data privacy, and platform security. I also welcome the chance to update you about our efforts to develop cutting-edge, multi-pronged initiatives to address national security concerns.

My name is Shou Chew, and I am the Chief Executive Officer of TikTok. I am responsible for all of TikTok's business operations and our strategic direction worldwide. A third-generation Singaporean, I am a graduate of University College of London and Harvard Business School. I am a veteran of the Singapore Armed Forces, a husband, and a father, and I currently reside in Singapore with my wife and two children.

Long before I became CEO, I was a content creator, and I have seen firsthand the transformative capability of short-form video. I am passionate about TikTok's ability to brighten people's lives, introduce them to new ideas and interests, and help businesses connect to their audiences.

On TikTok, we aim to provide three things. The first is a window to discover. This window, the For You feed, opens to a stream of videos curated to your interests, making it easy to find content and creators you love. The second is a canvas to create. Whether it's demonstrating a new science experiment or the latest cooking trend, people around the world use TikTok to unleash creativity. The third is a bridge to connect. Through TikTok, people have discovered new communities, cultures, and interests. As an example, BookTok, with more than 100 billion views, has connected readers across the globe and changed the way people consume literature. Although some people may still think of TikTok as a dancing app for teenagers, the reality is that our platform and our community have become so much more for so many.

TikTok has empowered millions of Americans to express their voices in their own authentic way and has provided a global stage for their creativity in a way that cannot be replicated on any other platform or in any other medium. More than 150 million people in the United States use TikTok on a monthly basis, with the average user today being an adult well past college age. Their videos provide a lens through which the rest of the world can experience American culture. Examples include TikTok's role in bringing exposure to American musicians, artists, chefs, and many more. While users in the United States represent 10 percent of our global community, their voice accounts for 25 percent of the total views around the world.

In addition to being a destination to express creativity, we pride ourselves on being a platform that helps companies—many of them small businesses—thrive. These are businesses like Country Lather Soap Works in Perkinston, Mississippi. Country Lather Soap Works is a no-frills producer of handcrafted soaps and bath products located on the Mississippi Gulf Coast. Founder Jessie Whittington had been making soap as a hobby for years before sharing her passion on TikTok while furloughed from her job as a bus driver. In a short time, sales exploded and she was shipping her products across the country, allowing her to quit her 9-to-5 and realize her dream of running her own small business.

TikTok enabled many small businesses to weather the darkest days of the pandemic, and a recent study found that an overwhelming majority of small businesses view TikTok as both fun and easy to use. TikTok's Small Business Resource Center helps people leverage the power and creativity of TikTok to grow their brands and better connect with their audience. If you talk to the millions of people and businesses who are on TikTok, I believe you'll hear incredibly powerful stories of discovery, creation, and connection that contribute to people's livelihoods and well-being.

Although I could talk all day about how TikTok enriches people's lives, I am also here to address concerns that have been raised by some members of this Committee. I know that trust is something that is earned through action, not words, and I welcome the opportunity to discuss not only our commitments, but also tangible evidence from TikTok's efforts to become a leader in safety and security.

Having met with a number of members of the Committee in recent weeks, the concerns that I have heard fall primarily into four categories: minor safety, data privacy and security, real-world harms from online activities, and the risk of foreign content manipulation. I would like to address each of these in turn. After that, I will compare some myths about TikTok to reality, including with regard to perceived foreign influence. First, however, I want to take a moment to highlight TikTok's commitment to an open and transparent relationship with Congress generally and this Committee specifically.

There are more than 150 million Americans who love our platform, and we know we have a responsibility to protect them, which is why I'm making the following commitments to you and our users:

1) We will keep safety—particularly for teenagers—a top priority for us;

2) We will firewall protected U.S. user data from unauthorized foreign access;

3) Tiktok will remain a platform for free expression and will not be manipulated by *any* government;

4) We will be transparent and give access to third-party independent monitors, to remain accountable for our commitments.

TikTok's Commitment to Transparency

Although this is my first time testifying before Congress, TikTok has long considered Congress an important stakeholder, and we have engaged actively with this Committee and others. TikTok routinely and voluntarily provides documents, briefings, and testimony to congressional committees.

For instance, over the past several months, TikTok has provided four briefings to the bipartisan staffs of this Committee and the House Committee on Oversight and Accountability on issues including data access and security. We also separately briefed this Committee in January on our efforts related to minor safety. Through these briefings, TikTok has answered questions about our robust policies and the improvements that we have made and will continue to make to even further strengthen our capabilities.

Because we value Congress's important oversight role, we regularly provide documents and information well beyond our legal obligations. We look forward to continuing to engage in a transparent and productive dialogue with this Committee and others.

TikTok's engagement with Congress is emblematic of our broader approach to transparency. Every quarter, we release a Community Guidelines Enforcement Report. These reports contain detailed information about the type and volume of content we remove. Twice a year, we also disclose data about requests we receive from law enforcement or governments.

Additionally, we are developing platform research and content moderation Application Programming Interfaces (APIs) as part of our commitment to bringing transparency to how our platform operates. As of last month, we have launched a research API that allows U.S.-based academic researchers to more easily analyze public content posted to the platform.

We provide detailed information about our content moderation process and recommendation system in our Transparency and Accountability Center. After offering virtual tours during the pandemic, we recently opened the doors to the first physical Transparency and Accountability Center in Los Angeles. Another center is planned for Washington, D.C. We would be happy to arrange a virtual or in-person tour for Members and Committee staff at your convenience.

Minor Safety

Safety and wellness—in particular for teens—is a core priority for TikTok. And as a father of two, these issues are personal for me. Today's youth are growing up in a digital media world, and TikTok is eager to be part of the conversation about creating more robust protections. TikTok supports creating additional protections, including potential updates to the Children's Online Privacy Protection Act, to address the modern online ecosystem. We would similarly welcome a conversation around legislation to enshrine better industry standards for age verification. We are committed to working constructively and collaboratively with the Committee on this important legislation.

In addition to forward-thinking legislation, good product design is also central to minor safety. To help teens safely manage their experience, TikTok provides them with age-appropriate settings and controls. The settings TikTok has developed reflect careful consideration of not only the differences between people under 13 and teenagers, but also within the 13-17 teenage group.

As an initial matter, TikTok offers a separate experience in the United States for people under 13. In the United States, people under 13 are directed to a separate, curated viewing experience, with stringent safeguards and privacy protections designed specifically for them. In this experience, younger users can view on their devices fun, creative, and educational videos that are vetted by a third-party expert, Common Sense Networks. However, they cannot post videos on

the platform, comment on others' videos, message with others, or maintain a profile or followers. No advertisements are shown in the under-13 experience.

TikTok also has taken numerous steps to help ensure that teens under 18 have a safe and enjoyable experience on the app. Many of these measures impose restrictions not shared by other platforms. We launch great products with a safety-by-design mentality, even if those features limit our monetization opportunities.

For example, accounts registered to teens under 16 are set to private by default. They are also prevented from sending direct messages, and their content is ineligible for recommendation into the For You feed. These measures go far beyond what any of our peers do. We also prevent teens from receiving late-night push notifications and give parents and guardians the ability to create further restrictions on these notifications.

Additionally, only accounts registered to people 18 or older can host a livestream on the platform. All livestream hosts in the United States are required to have a minimum of 1,000 followers on TikTok. To participate in monetization programs such as gifts, they must also be at least 18 years old. In addition to an industry standard age gate, TikTok also uses both technology (*e.g.*, text-based models like Natural Language Processing) and human moderation to help determine whether a user may be under 18 years old. If a user is suspected of being under 18, the livestream is sent for human moderation. People on TikTok can also report potentially underage users. If a moderator concludes the host appears to be under 18 years old, the livestream is stopped immediately and the user is suspended.

Earlier this month, we announced that every account belonging to a person under age 18 will be set by default to a 60-minute daily screen time limit. We consulted experts from the Digital Wellness Lab at Boston Children's Hospital in choosing this limit. If the 60-minute limit is reached, teens will be prompted to enter a passcode in order to continue watching, requiring them to make an active decision to extend that time. In our under-13 experience, the daily screen time limit will also be set to 60 minutes, and a parent or guardian will need to set or enter a passcode to enable 30 minutes of additional watch time.

TikTok's Minor Safety team holds a high bar of rigor for developing policy. TikTok is staffed with experts from the fields of adolescent development, prevention science, and child protection. TikTok works with leading youth safety and well-being experts, as well as adolescent psychologists, to inform our approach, including the Family Online Safety Institute, Common Sense Networks, the Digital Wellness Lab at Boston Children's Hospital, ConnectSafely, and the Cyberbullying Research Center, as well as our own U.S. Content Advisory Council. TikTok is also active with the Technology Coalition, an organization that works to protect children from online sexual exploitation and abuse, and serves on its board of directors and as chair of its transparency committee.

TikTok rigorously screens content for indications of potential predatory or abusive behavior. TikTok's moderation system uses models to identify content, including videos, captions, and comments, that violates our Youth Safety and Wellbeing Policy. Each and every video uploaded to TikTok goes through automated moderation, and potentially violative content is automatically

removed or escalated for human review by one of our expert moderators who have undergone specialized training to detect the signs of grooming or predatory behavior.

In addition to our own technology, TikTok has integrated with Hash Sharing Web Services from the National Center for Missing & Exploited Children (NCMEC) to enable the detection and removal of known violative content at the point of upload to TikTok. In 2021, we made 154,618 reports to NCMEC and were alone among major platforms in not receiving *any* takedown requests from NCMEC. Put differently, TikTok's swift actions resulted in the removal of abusive content before NCMEC received reports of it from other sources.

TikTok also recognizes that parents and caregivers are critical partners in ensuring the safety of teens. Parents and guardians cannot do it alone, and neither can we. TikTok is continuously looking for ways to involve parents and guardians in their teens' experience on the platform. To that end, in 2020, TikTok unveiled Family Pairing.

Family Pairing allows a parent or guardian to link their account (from the parent or guardian's device) with their teenager's account and enable privacy and safety controls. Parents and guardians can also set screen time limits and decide whether their teens can search for content, accounts, hashtags, or sounds. These features empower parents and guardians to customize their teens' privacy and safety settings, which TikTok continues to improve in consultation with youth and family safety experts.

Although we have accomplished a lot, we are always working vigilantly to stay ahead of the curve. As a result, we will never consider our work done, and we will never stop looking for ways to improve. I'm sure I will learn of new areas where we can improve today. I am both proud that TikTok has been a leader on these issues and encouraged to see that other platforms have adopted some of the protections that we have pioneered.

Data Privacy

Protecting the privacy of the people who use our platform is critical to our mission. To that end, we fully endorse congressional efforts to adopt comprehensive federal privacy legislation. This Committee, led by Chair Rodgers and Ranking Member Pallone, has been at the forefront of these issues, and we look forward to working with this Committee to help enact baseline privacy legislation that establishes consistent and strong privacy standards.

Privacy is built into TikTok by design so that our community can confidently discover, create, and enjoy entertaining content. People on TikTok have access to a wide range of privacy settings, including choosing whether their account is private or public; selecting to whom we may suggest their account; setting limits on who can interact with their videos, including with features like Stitch and Duet, or who can comment on their videos; and picking who can tag and mention them in a post, from "Everyone" to "No One."

We collect a limited amount of information when people set up an account, such as date of birth and username. Depending on how the individual signs up, we may also collect a phone number or email address. Unlike some other platforms, we do not require people on TikTok to provide us

with their real names during registration, nor do we ask them about their employment or relationship status. Current versions of the app do not collect precise or approximate GPS information from U.S. users.

Another important part of being a responsible steward of user data is owning up to our mistakes and making changes to address them. That's why we promptly took action, including a company-wide disclosure, when we learned late last year that certain (now former) employees had accessed TikTok user data in an unsuccessful and misguided attempt to trace the source of a leak of confidential TikTok information. We also notified this Committee about these ill-advised actions within moments of informing our employees. I condemn this misconduct in the strongest possible terms.

I understand that we have provided the Committee with a briefing on this subject and have committed to ongoing cooperation. In particular, to demonstrate that we have zero tolerance for the former employees' misconduct, we have provided the Committee with a full accounting of factual findings and remediation efforts through the outside law firm that is conducting the investigation into the matter. These remediation efforts include restructuring the department involved in the misconduct, creating a new Oversight Council, and strengthening policies and operational controls relating to U.S. user data access.

Keeping TikTok Safe for All

As CEO, I consider the safety of the platform to be paramount. More than 40,000 people globally work exclusively on trust and safety issues for TikTok. This includes in-house and contract moderators, as well as teams focused on safety policy, product, and operations. TikTok invests heavily in these teams, as well as in technology to detect potential violations and suspicious accounts at scale. For instance, in 2021, TikTok spent approximately $1 billion on trust and safety. Trust and safety represents our largest labor expense for TikTok's U.S. operations.

We are very cognizant of the fact that online conduct can have real-world consequences. We strive to provide a safe environment for the TikTok community and to remove content that violates our policies, including those that prohibit bullying, hateful behavior, promotion of disordered eating, and violent extremism. Through our quarterly Community Guidelines Enforcement Reports, we regularly update the public on how we are measuring up to this ideal. For instance, in the third quarter of 2022, we proactively removed 96.5 percent of violative content before receiving any reports from users or others. In 92.7 percent of cases, the removal occurred within 24 hours of when the content was posted.

People come to TikTok to feel inspired, be creative, and watch uplifting content. It is not the platform of choice for individuals seeking to engage in harmful conduct. However, we also realize that threats to online platform safety are far from static. Content moderation, which is a core element of platform safety, is an exceptionally complicated, dynamic, and constantly evolving process. TikTok's content moderation successes—and challenges—reflect common industry experiences for digital and short-form video platforms. TikTok constantly works to improve, adjust, and make more consistent the development and implementation of content

moderation policies. Among other initiatives, TikTok's U.S. Content Advisory Council, which brings together outside experts, helps advise on how to respond to emerging challenges.

Our Advertising Policies also reflect our commitment to platform safety. We value being an environment where creative, joyful content can flourish, and we have made decisions that prioritize safety over short-term commercial success. For example, we do not allow paid political ads on the platform, even though they could be a source of significant revenue. Nor do we accept advertisements for categories of content that may hurt our efforts to support the safety of our community, such as advertisements associated with violence or threats, including guns, weapons, and tactical gear.

Other categories not permitted in the U.S. market under our Advertising Policies include promotion of: alcohol, invasive cosmetic procedures, and multi-level marketing recruitment, among many additional subjects. Our Community Guidelines apply with full force to all advertisements on the platform, such that any content that would not be permitted if uploaded by a user would not be allowed as a paid advertisement.

Data Security

I want to take this opportunity to address the work, of which I am incredibly proud, that TikTok is doing to become the most trusted and secure digital platform. But I know that simply describing our efforts is not enough. Congress and the American people understandably want proof that we are living up to our ideals. So I will also address the numerous layers of oversight that TikTok has voluntarily embraced.

Trust must be earned through action, not words. Building trust is above all an engineering and governance effort, not a public relations exercise. We will go above and beyond, so our community and regulators can see and verify our actions. And we hope you will give us that chance.

The centerpiece of our work is called Project Texas. Project Texas is an unprecedented initiative dedicated to safeguarding both U.S. user data and U.S. national security interests. This initiative addresses key issues of corporate governance, content recommendation and moderation, data security, and system access. It is a comprehensive package of measures with layers of independent oversight to protect against backdoors into TikTok that could be used to manipulate the platform or access U.S. user protected data.

Project Texas puts the concepts of transparency and accountability into action by addressing national security concerns head-on with concrete, measurable solutions. Project Texas is designed to introduce layers of transparency and vetting that are commonly used for defense contractors but are unheard of for consumer platforms.

Given that this is a fluid and dynamic process, I want to take some time to address what we've done already and what we're working on.

First, we have already taken substantial steps to make Project Texas a reality, including spending roughly $1.5 billion to date on implementation. We have formed a special-purpose subsidiary, TikTok U.S. Data Security Inc. (USDS), that currently has nearly 1,500 full-time employees. We expect that number to grow significantly over the coming year. USDS includes the functions that oversee protected U.S. user data and the underlying TikTok U.S. platform.

To ensure that the data of all Americans is stored in America and hosted by an American headquartered company, we have contracted with Oracle, an industry leader in cloud-based services, to store TikTok's U.S. user data. Currently, 100 percent of U.S. user traffic is being routed to Oracle and USDS-controlled infrastructure in the United States. USDS is running our recommendation system for U.S. users, which determines what appears in the For You feed, in the Oracle Cloud Infrastructure. Moreover, Oracle has already begun inspecting TikTok's source code and will have unprecedented access to the related algorithms and data models. No other social media company, or entertainment platform like TikTok, provides this level of access and transparency. As of January 18, 2023, TikTok's access to systems containing new protected data are exclusively controlled by USDS.

Next, I want to address what we're working on now. I know that there has been a lot of speculation about Project Texas recently based on media coverage. While conversations with the government are ongoing, our work on Project Texas has continued unabated. We are working hard every day to reach new milestones. For example, earlier this month, we began the process of deleting historical protected U.S. user data stored in non-Oracle servers; we expect this process to be completed later this year. When that process is complete, all protected U.S. data will be under the protection of U.S. law and under the control of the U.S.-led security team. Under this structure, there is no way for the Chinese government to access it or compel access to it.

In addition, as of January 2023, all access to systems containing new protected U.S. user data has been exclusively controlled by USDS, and all access to the new protected data is limited to approved USDS employees. There are some limited exceptions where non-USDS employees may be granted access to protected data, for example, for legal and compliance, but such access must be expressly authorized by USDS pursuant to a robust data access protocol. Furthermore, no employees of Beijing Douyin Information Service Co., Ltd. have access to any databases that contain any protected U.S. user data.

We also have a vision for where we can go in the future. For instance, there would be clear eligibility criteria for new USDS personnel. Data access would also be subject to information security controls that would be approved by both a U.S. government-approved third-party monitor and a third-party auditor. And USDS employees would report into an independent USDS board of directors who would be approved by and owe a fiduciary duty to the federal government.

We are eager to hear feedback and to address any concerns. We continue to believe that imposing state-of-the-art access and security controls is the best path forward, not only for TikTok, but for the industry as a whole, and we remain committed to continued consultation and to finding innovative answers to what we firmly believe are solvable concerns.

I am well aware that the fact that ByteDance has Chinese founders has prompted concerns that our platform could be used as or become a tool of China or the Chinese Communist Party. There have even been calls to ban us or require divestment.

I steadfastly believe that all concerns that have been raised have solutions. Bans are only appropriate when there are no alternatives. But we do have an alternative—one that we believe addresses the concerns we've heard from this Committee and others. We do not believe that a ban that hurts American small businesses, damages the country's economy, silences the voices of over 150 million Americans, and reduces competition in an increasingly concentrated market is the solution to a solvable problem.

Likewise, divestment doesn't address the fundamental concerns that I have heard, as a change in ownership would not impose any new restrictions on data flows or access. This is not an issue of nationality. All global companies face common challenges that need to be addressed through safeguards and transparency. I am proud that TikTok is taking the lead in this area, and I welcome the chance to continue having conversations with the U.S. government to make this model even better.

To be clear, our commitment under Project Texas is for the data of all Americans to be stored in America, hosted by an American headquartered company, with access to the data controlled by USDS personnel. We offer this framework so that we can continue to accomplish what we value most: being a platform for free expression beloved by more than 1 billion people, including over 150 million Americans.

Myths Versus Reality

Finally, I'd like to address some misconceptions about TikTok.

First, I understand that there are concerns stemming from the inaccurate belief that TikTok's corporate structure makes it beholden to the Chinese government or that it shares information about U.S. users with the Chinese government. This is emphatically untrue.

TikTok is led by an executive team in the United States and Singapore and has global offices, including in Los Angeles, Silicon Valley, Nashville, New York, Washington, D.C., Dublin, London, Paris, Berlin, Dubai, Singapore, Jakarta, Seoul, and Tokyo. Our headquarters are in Los Angeles and Singapore. TikTok is not available in mainland China. As CEO, I am responsible for all business operations and strategic decisions for TikTok.

TikTok, as a U.S. company incorporated in the United States, is subject to the laws of the United States. TikTok has never shared, or received a request to share, U.S. user data with the Chinese government. Nor would TikTok honor such a request if one were ever made. Indeed, a 2021 report from Citizen Lab, an internationally renowned security research laboratory, found that there was no overt data transmission by TikTok to the Chinese government and that TikTok did not contact any servers within China.

TikTok publishes information about all requests we receive from law enforcement in our semiannual Information Requests Report. This includes information about the countries from which the requests originate. As reflected in this data, no requests have come from China.

TikTok's parent company, ByteDance, was founded by Chinese entrepreneurs, but has evolved into a global enterprise since its founding. ByteDance is a privately-held global company, with

roughly 60 percent owned by global institutional investors (such as Blackrock, General Atlantic, and Sequoia), approximately 20 percent owned by the company's founders, and approximately 20 percent owned by its employees—including thousands of Americans. It is not owned or controlled by any government or state entity. ByteDance's board is comprised of CEO Rubo Liang, Bill Ford of General Atlantic, Arthur Dantchik of Susquehanna International Group, Philippe Laffont of Coatue, and Neil Shen of Sequoia China.

Let me state this unequivocally: ByteDance is not an agent of China or any other country. However, for the reasons discussed above, you don't simply have to take my word on that. Rather, our approach has been to work transparently and cooperatively with the U.S. government and Oracle to design robust solutions to address concerns about TikTok's heritage.

Second, there are misconceptions about the type of data that TikTok collects. For instance, there have been a number of press stories alleging that TikTok "tracks" people. This is not accurate. As noted above, current versions of the app do not collect precise or approximate GPS information from U.S. users.

These are just a couple examples of some common misconceptions. I look forward to addressing these inaccuracies and others during my testimony.

Conclusion

TikTok is a vibrant marketplace for a diverse group of more than 1 billion creators. As we fulfill our mission to inspire creativity and bring joy, we remain resolute in our commitment to safety and security, and we look forward to earning the trust of this Committee and the American public. We also look forward to partnering with the Committee on developing clear, consistent rules for the entire industry.

When it comes to protecting our community, we know there's no finish line. The industry as a whole faces dynamic and ever-evolving challenges. We will always work to deploy our teams, tools, and resources to meet them and to demonstrate our hard work and transparency.

Thank you for the opportunity to appear today and to answer questions on these important issues.

Mrs. RODGERS. As you know, the testimony that you are about to give is subject to title 18, section 1001 of the United States Code.

As you state in your testimony, ByteDance is TikTok's parent company. Is it accurate to say that you are in regular communication with the CEO of ByteDance, Liang Rubo?

Mr. CHEW. Chair Rodgers, yes, I am in——

Mrs. RODGERS. Thank you.

Mr. CHEW [continuing]. Communication with him.

Mrs. RODGERS. OK. Kelly Zhang is the CEO of ByteDance China, overseeing Douyin, the Chinese version of TikTok. Are you in regular communication with Kelly?

Mr. CHEW. I am not in regular communication with her.

Mrs. RODGERS. The ByteDance editor in chief is Zhang Fuping, correct?

Mr. CHEW. I believe so.

Mrs. RODGERS. And Wu Shugang is a Beijing ByteDance Technology board member, and also an official of the Cyberspace Administration in China. Is this correct?

Mr. CHEW. I believe so. I—they are not in the right——

Mrs. RODGERS. Thank you. All of these individuals work or are affiliated with the Chinese Communist Party, are at the highest levels of leadership at ByteDance, a company where you previously served as the chief financial officer and where you regularly communicate with their CEO.

TikTok has told us that you weren't sharing data with the CCP. But leaked audio from within TikTok has proven otherwise. TikTok told us that you weren't tracking the geolocation of American citizens. You were. TikTok told us you weren't spying on journalists. You were.

In your testimony you state that ByteDance is not beholden to the CCP. Again, each of the individuals I listed are affiliated with the Chinese Communist Party, including Zhang Fuping, who is reported to be the Communist Party Secretary of ByteDance and who has called for the party committee to "take the lead" across all party lines to ensure that algorithm is enforced by "correct political direction."

Just this morning The Wall Street Journal reported that the CCP is opposed to a forced sale of TikTok by ByteDance, quoting a CCP spokesman as saying the Chinese Government would make a decision regarding any sale of TikTok. So the CCP believes they have the final say over your company. I have zero confidence in your assertion that ByteDance and TikTok are not beholden to the CCP.

Next question. Heating content is a way of promoting and moderating content. In your current or previous positions within Chinese companies, have employees engaged in heating content for users outside of China? Very quickly, yes or no?

Mr. CHEW. Our heating process is approved by our local teams——

Mrs. RODGERS. So——

Mr. CHEW [continuing]. In the various countries.

Mrs. RODGERS [continuing]. The answer is yes. Thank you.

Have any moderation tools been used to remove content on TikTok associated with the Uyghur genocide, yes or no?

Mr. CHEW. We do not remove that kind of content. TikTok is a place for freedom of expression and, Chair Rodgers, like I said, if you use our app you can go on it and you will see a lot of users around the world——

Mrs. RODGERS. Thank you.

Mr. CHEW [continuing]. Expressing content——

Mrs. RODGERS. Thank you.

Mr. CHEW [continuing]. On that topic and many others.

Mrs. RODGERS. Thank you. What about the massacre in Tiananmen Square, yes or no?

Mr. CHEW. I am sorry, I didn't hear the question.

Mrs. RODGERS. The massacre in Tiananmen Square.

Mr. CHEW. That kind of content is available on our platform. You can go and search it.

Mrs. RODGERS. I will remind you that making false or misleading statements to Congress is a Federal crime.

Mr. CHEW. I understand. Again, you can go——

Mrs. RODGERS. OK, thank you.

Mr. CHEW [continuing]. On our platform. You will find that content.

Mrs. RODGERS. Next question—OK, thank you. Reclaiming my time, can you say with 100 percent certainty that ByteDance or the CCP cannot use your company or its divisions to heat content to promote pro-CCP messages for an act of aggression against Taiwan?

Mr. CHEW. We do not promote or remove content at the request of the Chinese Government.

Mrs. RODGERS. The question is——

Mr. CHEW. We will——

Mrs. RODGERS. The question is are you 100 percent certain that they cannot use your company to promote such messages?

Mr. CHEW. It is our commitment to this committee and all our users that we will keep this free from any manipulation——

Mrs. RODGERS. If you can't—OK.

Mr. CHEW [continuing]. By any government.

Mrs. RODGERS. If you can't say 100 percent certain, I take that as a no.

As I previously referenced, TikTok spied on American journalists. Can you say with 100 percent certainty that neither ByteDance nor TikTok employees can target other Americans with similar surveillance techniques?

Mr. CHEW. Chair Rodgers, I, first of all, disagree with the characterization that it is spying. It was an internal investigation on——

Mrs. RODGERS. Surveillance. Yes or no, can you do surveillance of other Americans?

Mr. CHEW. We will protect the U.S. user data and fire it all from all unwanted foreign access is a commitment that we have given to the committee.

Mrs. RODGERS. So I guess my question is, can—I want you to—I wanted to hear you say with 100 percent certainty that neither ByteDance nor TikTok employees can target other Americans with similar surveillance techniques as you did with the journalists.

Mr. CHEW. Again, I disagree with the characterization as surveillance, and we have given our commitments, Chair Rodgers, the

four commitments. I think—is our commitment that we will not be influenced by any government on these issues.

Mrs. RODGERS. DoJ is investigating this surveillance right now.

To the American people watching today, hear this: TikTok is a weapon by the Chinese Communist Party to spy on you, manipulate what you see, and exploit for future generations. A ban is only a short-term way to address TikTok. And a data privacy bill is the only way to stop TikTok from ever happening again in the United States.

I yield back. I now yield to the ranking member for 5 minutes.

Mr. PALLONE. Thank you, Madam Chair.

Let me just start out by saying, Mr. Chew, that I don't find what you suggested with Project Texas and this firewall that is being suggested to whoever will be—will be acceptable to me. In other words, you know, the—I still believe that the Beijing communist government will still control and have the ability to influence what you do. And so this idea, this Project Texas, is simply not acceptable.

According to a recent report, TikTok is on target to make between 15 and 18 billion dollars in revenue this year. Is that an accurate forecast?

Mr. CHEW. Congressman, as a private company we are not sharing our——

Mr. PALLONE. I thought that is what you would say.

Mr. CHEW [continuing]. Numbers publicly.

Mr. PALLONE. How much money will TikTok make by delivering personalized advertisements just to your users in the United States? Will you give me that information?

Mr. CHEW. Again, Congressman, respectfully——

Mr. PALLONE. I thought——

Mr. CHEW [continuing]. As a private company, we are not disclosing that.

Mr. PALLONE. I thought that is what you would say.

Look, my—the impression you are giving—and I know, you know, I can understand why you are trying to give that impression—is that, you know, that you are just performing some kind of public service here, right? I mean, this is a benign company that is just performing a public service. I—maybe you are not, maybe that is not what you are saying, but I don't buy it, right?

My concern here is primarily about the privacy issue, the fact that TikTok is making all kinds of money by gathering private information about Americans that they don't need for their business purposes, and then they sell it.

And I mentioned this legislation that the ranking—that the Chair and I have that would minimize data collection and make it much more difficult for TikTok and other companies to do that. So what—if you want to make some commitments today, why don't—I will ask you to make some commitments with regard to this legislation. And, you know, you are going to tell me, well, "The bill isn't passed, and so therefore I don't have to do it." But, you know, you say you are benign, you want to do good things for the public.

So let me ask you, why not—what about a commitment that says that you won't sell the data that you collect, would you commit to that, not selling the data you collect?

Mr. CHEW. Congressman, I believe we don't sell data to any data brokers.

Mr. PALLONE. You don't sell to anyone.

Mr. CHEW. We don't sell data to data brokers.

Mr. PALLONE. I didn't ask you—data brokers. Do you sell it to anyone?

In other words, under our bill, you could only use the data for your own purposes, not to sell it to anyone. Would you commit to not selling your data to anyone?

Mr. CHEW. Congressman, I actually am in support of some rules about privacy——

Mr. PALLONE. I didn't ask you whether——

Mr. CHEW. Yes.

Mr. PALLONE [continuing]. Rules. I asked you whether the company, TikTok, would commit to not selling its data to anyone, and just using it for its own purposes internally.

Mr. CHEW. I can get back to you on the details of that.

Mr. PALLONE. OK, get back to me. All right.

Another thing that is in our bill says that we would prohibit targeting marketing to people under the age of 17. Would you be willing to agree to prohibit targeted marketing to people, Americans, under the age of 17?

Mr. CHEW. Congressman, we have actually stricter rules for our advertisers in terms of what they can show to our users——

Mr. PALLONE. So do you prohibit——

Mr. CHEW [continuing]. Under the age of 18.

Mr. PALLONE. Would you be willing to prohibit targeted marketing to those under 17? That is what is in our bill.

Mr. CHEW. I understand that there is some talk and some legislation around this around the country——

Mr. PALLONE. Well, again, I am not interested—I wanted you to make that commitment without the legislation. Since you say you are a good company, you want to do good things, why not?

Mr. CHEW. It is something we can look into and get back to you.

Mr. PALLONE. OK, I appreciate that. OK, we also have in our bill a requirement of heightened protection for sensitive data, particularly location and health data. Would you commit to not gathering or dealing with location or health data unless you get affirmative consent from the consumer?

In other words, under our bill those are categorized as sensitive. And unless the person specifically says, "I want you to collect that data," you wouldn't be able to, location and health data. Would you commit to that?

Mr. CHEW. Congressman, in principle I support that, which—by the way, we do not collect precise GPS data at this point, and I do not believe we collect any health data.

Mr. PALLONE. All right. So would you be willing to make that commitment, that from now on you won't collect location and health data without—well, you are saying at all. Is that a commitment?

Mr. CHEW. Congressman, this is data that is frequently collected by many other companies.

Mr. PALLONE. I know other companies do it. I don't think they should without affirmative consent. You said you want to be a good actor, so why not make that commitment to me today?

Mr. CHEW. We are committed to be very transparent with our users about what we collect. I don't think what we collect—I don't believe what we collect is more than most players——

Mr. PALLONE. You see——

Mr. CHEW [continuing]. In the industry——

Mr. PALLONE [continuing]. My problem here is you are trying to give the impression that you are going to move away from Beijing and the Communist Party. You are trying to give the impression that you are a good actor. But the commitments that we would seek to achieve those goals are not being made today. They are just not being made. You are going to continue to gather data. You are going to continue to sell data. You are going to continue to do all these things and continue to be under the aegis of the Communist Party through the—through your, you know, organization that owns you. So in any case, thank you.

Thank you, Madam Chair.

Mrs. RODGERS. The gentleman yields back. The Chair now recognizes the gentleman from Texas, Mr. Burgess, for 5 minutes.

Mr. BURGESS. I thank the Chair. Thank you, Mr. Chew, for joining us today.

I think we have heard you say multiple times that TikTok is not a Chinese company, that ByteDance is not a Chinese company. But according to an article in today's Wall Street Journal—quoting here—"China's Commerce Ministry said Thursday that a sale or divestiture of TikTok will involve exporting technology [that has] to be approved by the Chinese Government." Continuing to quote: "The reported efforts by the Biden administration would severely undermine global investors' confidence in the U.S., said Shu Jueting, a ministry spokeswoman." Continuing to quote: "'If [the news] is true, China will firmly oppose it,' she said, referring to the forced sale."

So despite your assertions to the contrary, China certainly thinks it is in control of TikTok and its software. Is that not correct?

Mr. CHEW. Congressman, TikTok is not available in mainland China. And today we are headquartered in Los Angeles and Singapore. But I am not saying that, you know, the founders of ByteDance are not Chinese, nor am I saying that we don't make use of Chinese employees, just like many other companies around the world. We do, you know, use their expertise on some engineering projects.

Now——

Mr. BURGESS. But according to their ministry spokeswoman, it would be a divestiture of exporting technology from China. So they—again, China thinks they own it, even though you do not.

Madam Chair, I would just like to ask unanimous consent to put today's Wall Street Journal article——

Mrs. RODGERS. Without objection, so ordered.

Mr. BURGESS [continuing]. Into the record.

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

Mr. BURGESS. Now, Mr. Chew, I wouldn't ask you to discuss any privileged attorney-client materials, but did anyone, aside from your lawyers, assist you in preparation for today's hearing?

Mr. CHEW. I prepared for this hearing with my team here in DC.

Mr. BURGESS. Did anyone at ByteDance directly provide input, help, or instruction for your testimony today?

Mr. CHEW. Congressman, this is a very high-profile hearing. My phone is full of well-wishers, you know, but I prepared for this hearing with my team here in DC.

Mr. BURGESS. Are you willing to share who helped prepare you for this hearing with the committee? And you can do that in writing.

Mr. CHEW. I can follow up with you, if you like.

Mr. BURGESS. OK. Can you guarantee that no one at ByteDance had a role in preparing you for today's hearing?

Mr. CHEW. Like I said, Congressman, this is a high-profile hearing. A lot of people around the world were sending me wishes and unsolicited advice, but I prepared for this hearing with my team here in DC.

Mr. BURGESS. Are the attorneys representing TikTok also representing ByteDance?

Mr. CHEW. Yes, I believe so.

Mr. BURGESS. What percentage of TikTok revenue does ByteDance retain? Just give me a ballpark estimate, if you don't precisely know.

Mr. CHEW. Congressman, like I said, as a private company we are not prepared to disclose our financials in public today.

Mr. BURGESS. Can we ask you to get back to us with a ballpark? We are not asking for the precise figures, but to get—so the committee can have some understanding of the percentage of TikTok revenue that ByteDance retains.

Mr. CHEW. I understand the question. Respectfully, as a private company we are not disclosing our financials today.

Mr. BURGESS. Prior to today's hearing, did anyone affiliated with the Chinese Communist Party discuss this hearing with you or anyone else on TikTok's senior management?

Mr. CHEW. Congressman, since I have been CEO of this company I have not had any discussions with Chinese Government officials.

Mr. BURGESS. So what—but what about the Chinese Communist Party itself? Have any of those officials discussed this with you?

Mr. CHEW. Like I said, I have not had any discussion with Chinese Government officials. I don't know the political affiliation of everybody I speak to, so I can't verify the statement.

Mr. BURGESS. Let me ask you a question in a different direction.

A few weeks ago this committee had a field hearing down in McAllen, Texas, and it was on the issue of fentanyl and illegal immigration. And one of our witnesses, Brandon Judd, a 25-year veteran Border Patrol agent, said that all social media platforms play a role in illegal immigration. That is one of the ways cartels advertise their services throughout the world and convince people to put themselves in their hands and come to the United States. The cartels all use social media platforms. Are you aware of this phenomenon?

Mr. CHEW. Any content that promotes human abuse is violative of our community guidelines, which dictates what is allowed and not allowed on our platform. We proactively identify and remove them from our platform.

Mr. BURGESS. Well, it would be very helpful if you would share with the committee examples of how you have removed people, because what we heard at the hearing was that TikTok was one of the platforms that recruits adolescents in the United States to help with transporting people who are in the—who have been trafficked into the country, as well as contraband substances. Would you help us with that, understanding who you have removed from your platform?

Mr. CHEW. Congressman, I would be delighted to check with my team and get back to yours and be collaborative.

Mr. BURGESS. Thank you.

I yield back.

Mrs. RODGERS. The gentleman's time has expired. The Chair recognizes the lady from California, Ms. Eshoo, for 5 minutes.

Ms. ESHOO. Thank you, Madam Chairwoman.

Mr. Chew, thank you for being here today.

As Members of Congress, our very first and top responsibility is to protect and defend, protect and defend our Constitution and the national security of our country. So I view this entire issue—now, there are many parts of it that are not part of our national security, in my view, but first and foremost, for our national security.

So in examining TikTok breaking away from ByteDance, I would like to ask you some questions about that, and how a severance in terms of the relationship with ByteDance, how user data, American user data, would be protected.

Now, under Beijing's security laws, article 7 compels companies to provide data; article 10 makes the reach of the law extra—extraterritorial. Now, this is very clear. I don't need to read all of it into the record, but that—those are the laws of the PRC.

How does ByteDance—how does TikTok, rather—how do you convince the Congress of the United States that there can be a clean break? Why would the Chinese Government sidestep their national law, including article 7, article 10, in terms of user data?

Mr. CHEW. Congresswoman, thank you for the question. I am glad you asked this.

As I said in the opening statement, our plan is to move American data to be stored on American soil by an American company——

Ms. ESHOO. I understand that. I understand that. But you are sidestepping—or I haven't read anything in terms of TikTok—how you can actually say—and you spoke in your opening statement about a firewall relative to the data, but the Chinese Government has that data. What—how can you promise that that will move into the United States of America and be protected here?

Mr. CHEW. Congresswoman, I have seen no evidence that the Chinese Government has access to that data. They have never asked us. We have not provided.

Ms. ESHOO. Well, you know what? I find that——

Mr. CHEW. I have asked that question——

Ms. ESHOO. I find that actually preposterous.

Mr. CHEW. I have looked, and——

Ms. ESHOO. I really do.

Mr. CHEW [continuing]. I have seen no evidence of this happening. And in order to assure everybody here and all our users, our commitment is to move the data into the United States, to be stored on American soil by an American company, overseen by American personnel. So the risk will be similar to any government going to an American company asking for data, if that——

Ms. ESHOO. Well, I am one that doesn't believe that there is really a private sector in China. And when you look at their national law, and what—specifically, these two articles, article 7 and article 10, are very clear. So I think that there is a real problem, a real problem relative to our national security about the protection of the user data.

I don't believe that TikTok has—that you have said or done anything to convince us that that information, the personal information of 150 million Americans, that the Chinese Government is not going to give that up. So can you tell me——

Mr. CHEW. Congresswoman, if I——

Ms. ESHOO. Can you tell me who writes the algorithms for TikTok?

Mr. CHEW. Today the algorithm that powers the U.S. user experience is running in the Oracle Cloud infrastructure.

Yes, you know, in the—initially, there were parts of the source code, especially in the infrastructure layer, that doesn't touch the user experience. Now, that is a collaborative global effort, including built by engineers in China, just like many other companies, by the way. The phone you use, the car you drive is a global collaborative effort. Now, but today the business sites and the main parts of the code for TikTok is written by TikTok employees.

And, Congresswoman, what we are offering is third-party monitoring of our source code. I am not aware of any company, American companies or otherwise, that has actually done that, because we are saying we want to give you transparency and rely on third parties to make sure that we get all the comfort that we need about the experience.

Ms. ESHOO. Well, I—my time is up, and I yield back. Thank you.

Mrs. RODGERS. The lady yields back. I am pleased to yield to the gentleman from Ohio, Mr. Latta, for 5 minutes.

Mr. LATTA. Well, thank you, Madam Chair. Unlike the Chinese Communist Party, the United States believes in individual freedom, innovation, and entrepreneurship. That is in part why Congress enacted section 230 of the Communications Decency Act. Our goal is to promote growth of the online ecosystem in the United States and to protect companies from being held liable for good-faith efforts to moderate their platforms.

Last year a Federal judge in Pennsylvania found that section 230 protected TikTok from being held responsible for the death of a 10-year-old girl who participated in a blackout challenge also known as the Choking Challenge. TikTok actively pushed this video on her feed. Unfortunately, this is one of the many devastating examples of children losing their lives because of content promoted by TikTok.

Section 230 was never intended to shield companies like yours from amplifying dangerous and life-threatening content to children. Do you consider this to be a good-faith moderation?

Mr. CHEW. Congressman, as a father myself, when I hear about the tragic deaths of——

Mr. LATTA. And my question——

Mr. CHEW [continuing]. People, it is heartbreaking.

Mr. LATTA. Do you find that good-faith moderation?

Mr. CHEW. Well, Congressman, section 230 is a very complex issue.

Mr. LATTA. OK, you know, yes or no?

Mr. CHEW. We are very focused on safety, and all these dangerous——

Mr. LATTA. OK, I am going to have to——

Mr. CHEW [continuing]. Challenges are removed when we find them.

Mr. LATTA [continuing]. Assume that is a no.

Do you believe TikTok deserves this liability protection?

Mr. CHEW. I am sorry, Congressman, I didn't——

Mr. LATTA. Do you believe that TikTok deserves this liability protection under section 230?

Mr. CHEW. Congressman, as you pointed out, 230 has been very important for freedom of expression on the Internet. It is one of the commitments we have given to this community and our users, and I do think it is important to preserve that.

But companies should be raising the bar on safety. I really agree with that——

Mr. LATTA. Let me follow up real quickly, from your own testimony. When you told us—and you repeated it—"We will keep safety, particularly for teenagers, a top priority for us," you are saying you are making that following commitment. Why did you have to wait until now to make that following commitment now, and not having done it before, when this 10-year-old lost her life?

Mr. CHEW. Congressman, I am reiterating the commitment internally in all my priorities, which is public to my employees——

Mr. LATTA. OK, this is a——

Mr. CHEW. Safety has always been a priority.

Mr. LATTA. This company is a picture-perfect example of why this committee in Congress needs to take action immediately to amend section 230.

When we recently met I asked you if the Chinese Communist Party can currently access user data, and you did not have a clear answer. So today I want to follow up. You heard it a little bit, but I want to be absolutely sure of this answer.

Are employees of ByteDance subject to Chinese law, including the 2017 national intelligence law which requires any organization or citizen to support, assist, and cooperate with State intelligence work in accordance with the law?

Mr. CHEW. Like many companies, including many American companies, we rely on a global workforce, including engineers in China.

Mr. LATTA. OK, but yes or no——

Mr. CHEW. So in the past, yes. In the past, yes, yes. But we are building Project Texas, and we are committing to firewall off——

Mr. LATTA. OK, I am taking that as——

Mr. CHEW [continuing]. All protected data from unwanted foreign access.

Mr. LATTA. I am taking that as a yes, because, again, your article 7—the article 7 of the 2017 national intelligence law, which I just said, because it says, in addition—as was asked a little bit earlier—the 2014 counterespionage law states that, when the State security organ investigates and understands the situation of espionage and collects relevant evidence, the relevant organizations and individuals—it does not say "maybe," it says "shall" provide it truthfully and may not refuse.

Yes or no, do any ByteDance employees in China, including engineers, currently have access to U.S. user data?

Mr. CHEW. Today all U.S. user data is stored by default in the Oracle Cloud infrastructure——

Mr. LATTA. Answer the question.

Mr. CHEW [continuing]. And access to that is controlled——

Mr. LATTA. The question is do any ByteDance——

Mr. CHEW [continuing]. By American personnel.

Mr. LATTA [continuing]. Employees in China, including engineers, currently have access to U.S. data?

Mr. CHEW. Congressman, I would appreciate—this is a complex topic. Today all data is stored by default——

Mr. LATTA. Yes or no? It is not that complex. Yes or no, do they have access to user data?

Mr. CHEW. We have—after Project Texas is done, the answer is no. Today there is still some data that we need——

Mr. LATTA. Yes, we have——

Mr. CHEW [continuing]. To delete——

Mr. LATTA. Yes, we have heard already from the ranking member that he hasn't, and—that he doesn't really see that Project Texas is going to be useful.

So I think I am taking that as a no because, again, the question is—come up earlier—that on December the 22nd of last year, when ByteDance confirmed some of its Chinese employees had accessed TikTok data to monitor and track the physical location of journalists. So I took that as a yes from an earlier answer.

You know, earlier this week you posted a TikTok video asking American users to mobilize in support of your app and oppose the potential U.S. Government action to ban TikTok in the United States. Based on the established relationship between your company and the Chinese Communist Party, it is impossible for me to conclude that the video is anything different than the type of propaganda the CCP requires Chinese companies to push on its citizens.

And I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the lady from Colorado, Ms. DeGette, for 5 minutes.

Ms. DEGETTE. Thank you—thank you very much, Madam Chair.

Mr. Chew, like my colleagues I am concerned about the influence of China on TikTok and what that does for U.S. users. But I am also concerned about how the content in TikTok is being distributed, particularly to young people.

This is not a problem unique to TikTok, but TikTok has 150 million users in the United States, and so I think you will agree that

TikTok has a particular responsibility to monitor content to make sure that it is safe and accurate. Would that be fair to say?

Mr. CHEW. Yes, I agree with that.

Ms. DEGETTE. So, you know, I know you said in your opening statement there is a ban for or limited for kids under 13 and under 18 and so on, but I am—I know it won't be news for you that computer-savvy kids actually can bypass some of those restrictions quite frequently, and they can do it even if they have parental oversight.

And so what I want to ask you is, rather than putting the burden on young people and parents to accurately put in the birth date and so on when registering for TikTok, I want to ask you what TikTok can do to make sure to monitor this content.

And I want to give you some examples of some of the extreme content. Mr. Latta talked about the Blackout Challenge and the—some of the dangers to young people's safety. But there is also extreme content around healthcare information.

In one study, 13 out of 20 results for the question "Does mugwort induce abortion?," it is—it talked about herbal so-called abortifacients like papaya seeds, which don't work. And so, if people searching for information on safe abortions went on TikTok, they could get devastatingly incorrect information.

Another study showed that TikTok was—had a hydroxychloroquine tutorial on how to fabricate this from grapefruit. Now, there's two problems with that. Number one, hydroxychloroquine is not effective in treating COVID. So that is one issue. The second issue is you can't even make hydroxychloroquine from grapefruit. So, again, this is a really serious miscommunication about healthcare information that people looking at TikTok are able to get. And in fact, it is being pushed out to them.

So I want to know from you—and I will give you time to answer this—you have current controls, but the current controls are not working to keep this information mainly from young people, but from Americans in general. What more is TikTok doing to try to strengthen its review to keep this information from coming across to people?

Mr. CHEW. Thank you for the question, Congresswoman. The dangerous misinformation that you mentioned is not allowed on our platform. It violates them.

Ms. DEGETTE. I am sorry to report it is on your platform, though.

Mr. CHEW. Congresswoman, I don't think I can sit here and say that we are perfect in doing this. We do work very hard——

Ms. DEGETTE. So how can you make yourself more perfect? I don't want you to say it is not there, or you apologize. What can you do to limit it as much as possible, more than what you are doing now?

Mr. CHEW. We invest a significant amount in our content moderation work. I shared that number in our—in my written testimony.

Ms. DEGETTE. I know you are investing.

Mr. CHEW. Yes.

Ms. DEGETTE. But what steps are you taking to improve the AI, or whatever else you are doing to limit this content?

Mr. CHEW. For example, if you search for certain search terms, we do direct you on TikTok to resource—safety resources. That is one of the things we have done. We will continue to invest in this.

I recognize and fully align with you that this is a problem that faces our industry, that we need to really invest and address. I am very in alignment.

The vast majority of our users come to our platform for entertaining, safe content. But there are people who do have some—who do spout some dangerous misinformation, and we need to take that very seriously, invest in it, proactively identify it, and remove it from our platform.

Ms. DEGETTE. OK. I am going to stop you right now. I asked you specifically how you were increasing—how you were trying to increase your review of this, and you gave me only generalized statements that you are investing, that you are concerned, that you are doing more. That is not enough for me. That is not enough for the parents of America.

I am going to ask you to supplement your testimony and have your—have your experts tell me what you are doing to make this a higher level of scrutiny, not just pablum at a hearing. Thank you.

I yield back.

Mr. CHEW. Thank you.

Mrs. RODGERS. The lady yields back. The Chair recognizes the gentleman from North Carolina, Mr. Hudson, for 5 minutes.

Mr. HUDSON. Thank you, Chairwoman McMorris Rodgers, for holding this important hearing. I appreciate the witness, Mr. Shou Chew, for making yourself available here today.

While many consider TikTok to be just another video-sharing app, in reality TikTok has been functioning as a massive surveillance program, collecting vast swaths of personal data from more than a billion people worldwide. This includes data from the personal devices of Federal employees, contractors, and, most concerning, U.S. military service members and their families at places like Fort Bragg in North Carolina.

As Fort Bragg's congressman, I have serious concerns about the opportunities TikTok gives the Chinese Communist Party to access the nonpublic, sensitive data of our men and women in uniform. This personal data and location information can be harvested and could be used for blackmail, to conduct espionage, and possibly even reveal troop movements.

While the Department of Defense and most agencies have banned TikTok on Government-issued devices, I believe more needs to be done at the command level to urge troops and their dependents to erase the app from the personal devices and keep them off home WiFi. Having an app banned on a device in one pocket but downloaded on your device in the other doesn't make a whole lot of sense to me. I believe Congress and DoD should address the continued use of TikTok on military installations, as well as any use that depicts U.S. military operations.

Mr. Chew, does TikTok access the home WiFi network?

Mr. CHEW. Only if the user turns on the WiFi. I am sorry, I may not understand the——

Mr. HUDSON. So if I have the TikTok app on my phone, and my phone is on my home WiFi network, does TikTok access that network?

Mr. CHEW. It will have to access the network to get connections to the Internet, if that is the question.

Mr. HUDSON. Is it possible, then, that it could access other devices on that home WiFi network?

Mr. CHEW. Congressman, we do not do anything that is beyond any industry norms. I believe the answer to your question is no. It could be technical. Let me get back to you.

Mr. HUDSON. OK. I would appreciate it if you could answer that.

I would like to change directions real quick. Do you receive personal employment, salary, compensation, or benefits from ByteDance?

Mr. CHEW. Yes, I do.

Mr. HUDSON. What is your salary from ByteDance?

Mr. CHEW. Congressman, if you don't mind, I would prefer to keep my compensation private.

Mr. HUDSON. OK. Do you personally have any company shares or stock in ByteDance or Douyin?

Mr. CHEW. Congressman, if you don't mind, I would like to keep my personal assets private.

Mr. HUDSON. Is TikTok, the company, your only source of employment compensation? Where is your other source of income outside of TikTok?

Mr. CHEW. It is my only source of compensation.

Mr. HUDSON. Do you have any financial debts or obligations to ByteDance, Douyin, or any other ByteDance-affiliated entity?

Mr. CHEW. Personally? No, I do not.

Mr. HUDSON. Does your management team receive separate salary, compensation, or benefits from ByteDance?

Mr. CHEW. We receive salaries from the employer—the entities that we are employed in, but we——

Mr. HUDSON. Is that——

Mr. CHEW [continuing]. Do share in the employee stock option plan that is available from the ByteDance top company.

Mr. HUDSON. So your primary salary comes from TikTok, but you have other compensation that comes directly from ByteDance?

Mr. CHEW. You can characterize it as that, yes.

Mr. HUDSON. Does your management team have company shares or stock in ByteDance or Douyin?

Mr. CHEW. Yes, we—some of our employees are compensated in shares in ByteDance.

Mr. HUDSON. Does TikTok share technological resources with Douyin?

Are the two technology systems or IT systems interconnected in any way?

Mr. CHEW. They are. As with many companies, some share resources on some services, but it doesn't include—anything that involves U.S. user data, Congressman, is in Project Texas, as we talked about, stored by default in American soil by an American company.

Mr. HUDSON. Well, but currently there is shared technology or interconnected IT systems.

Mr. CHEW. Congressman, with respect, I have to get back to you. This could be a very broad question. Like, for example, we could all be using Microsoft Windows.

Mr. HUDSON. If you could get back with details on that, I would appreciate it.

Mr. CHEW. Yes.

Mr. HUDSON. Can Douyin personnel or employees access TikTok user data?

Mr. CHEW. Not after Project Texas. This is not allowed.

Mr. HUDSON. Are there employees who are employed by both Douyin and TikTok?

Mr. CHEW. I do not believe so.

Mr. HUDSON. OK. So, "I don't believe so," is that a—I mean, again, I will allow you to come back in written response, if you could give me a definitive answer.

Mr. CHEW. I will go back and check to be very sure.

Mr. HUDSON. OK. Thank you. I am also concerned about an issue that our chairwoman brought up about an apparent pattern of misinformation or misrepresentation from your company in regards to the amount and extent of data that you are collecting, as well as how much has been accessed from inside China.

There are dozens of public reports that conclude individuals in the People's Republic of China have been accessing data on U.S. users, directly contradicting several public statements by TikTok employees. And I am referencing Project Raven, which was first reported on by Forbes last October. Their investigation revealed—I am sorry, I am about out of time. Do you want to respond to that?

Mr. CHEW. Yes, Congressman. We do not condone the effort by certain former employees to access U.S. TikTok user data in an attempt to identify the source of leaked confidential information. We condemn these actions.

After learning about them, we found a highly reputable law firm to thoroughly investigate the incident. We took swift disciplinary action against employees who were found to be involved and are implementing measures to make sure this doesn't happen again. We have made this team available to you. They—I think they have briefed many of you in this committee very extensively, and I will continue to make them very available to you as part of our transparent commitment.

Mr. HUDSON. Thank you. My time is expired.

I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the lady from Illinois, Ms. Schakowsky, for 5 minutes.

Ms. SCHAKOWSKY. Thank you. So today in The Wall Street Journal, they said—today China's commerce minister said that China opposes the sale of TikTok because it would involve exporting China's technology and would—and this is the important part—and would need to be approved by the Chinese Government, would need to be approved by the Chinese Government.

So all of what you have been saying about the distance between TikTok and China has been said to be not true in the paper today. And I would like to see what you have to say in response.

Mr. CHEW. Congresswoman, I do disagree with that characterization. I think we have designed Project Texas to protect U.S. user interests and to move forward here in the U.S.

Again, it is the protections of storing American data on American soil by an American company looked after by American personnel. And I do not think that the—you know, our commitments to this committee and all our users is impacted by any event that you mentioned.

Now, the whole, you know, discussion on this, the resolution of this, is an ongoing and developing event. So we will continue to pay attention to this, and we will get back to you when we have more specifics. But my commitment stands——

Ms. SCHAKOWSKY. So if—OK.

Mr. CHEW. Yes.

Ms. SCHAKOWSKY. So if it is an ongoing debate, apparently, with China, so it is hard to say with any certainty that China would not have any influence.

But let me ask another question. So last fall, along with Gus Bilirakis, who—were chair and cochair of the subcommittee together—were told that TikTok had surveilled—was involved in surveillance of users' very personal information. And you might say, well, not more than other companies. And I agree with Ranking Member Pallone that I really don't want to go by that standard, particularly, but that TikTok's in-app browser surveilled everything from Americans, including passwords and credit card numbers, et cetera.

So I just want to ask you if TikTok did track and collect this sensitive data that Americans don't want to have disclosed.

Mr. CHEW. Congressman, thank you. I am glad you asked this question because, like you pointed out, we actually do not believe we collect more data than any other social media company out there. A lot of these reports—and I—we can talk about which specific one you are talking about—a lot of them are not that accurate. Some of them we have contacted, we have actually gotten in touch with the authors to help them understand the data that we are collecting. A lot of it is speculation. You know, this is something they could do, they could do.

But if you look at the subtext, this is something that any company could do——

Ms. SCHAKOWSKY. So I am running out of time. Let me just say that if TikTok chose not to take the sensitive—this sensitive information that you don't need for a transaction and support our comprehensive privacy bill, that would be—that would be very helpful.

The other thing I wanted to ask—so really, this is a yes or no, that TikTok—does TikTok share user information from companies, from parent companies, from affiliated or—or send user information to—overseas?

Mr. CHEW. In the past, yes, for interoperability purposes. Now, after Project Texas, all protected U.S. data will be stored here, with the access controlled by a special team of U.S. personnel.

Again, Congresswoman, this is something that, as far as I understand, no other company, including American companies, are willing to go. So maybe this is something that we can ask the industry to provide, not just us, to protect U.S.——

Ms. SCHAKOWSKY. But in the case of sharing information, I do want to quote from employees that you had that—and here is the quote—"Everything is seen in China" is really what they said. People who were in touch with the sensitive data were saying that. How do you respond to that?

Mr. CHEW. I disagree with that statement.

Ms. SCHAKOWSKY. Well, I know you disagree with that statement. But my point is, how does that happen that employees of the company are saying that if, in fact, that is not true?

Mr. CHEW. I cannot speak to—I don't know who this person is, so I cannot speak to what a person has or has not said. What I can say is, you know, based on my position in this company and the responsibility that I have, that statement is just not true.

Ms. SCHAKOWSKY. OK. Unfortunately—and I will close, I guess I am over my time—we need to look into the facts of this, and so do you.

And I yield back.

Mrs. RODGERS. The gentlelady yields back. The Chair recognizes the lady from Florida, Mrs. Cammack, for 5 minutes.

Mrs. CAMMACK. Thank you, Madam Chairwoman.

Mr. Chew, are you aware of Chinese Communist Party leader Chairman Xi Jinping's comments in May 2021 during a Communist Politburo study session, where he instructed colleagues to target different countries, different audiences with short-form video? Are you aware of these comments, yes or no?

Mr. CHEW. Congresswoman, I am not aware of these comments.

Mrs. CAMMACK. OK. Well, and as was pointed out by Chairwoman Rodgers, you have regular contact with Chinese Communist Party Secretary Mr. Zhang Fuping, who is your boss at ByteDance, correct?

Mr. CHEW. No.

Mrs. CAMMACK. No?

Mr. CHEW. No.

Mrs. CAMMACK. Interesting.

Mr. CHEW. He is neither my boss, nor do we have frequent contact.

Mrs. CAMMACK. But you have regular contact with ByteDance.

Mr. CHEW. With the CEO of ByteDance.

Mrs. CAMMACK. Who is—Mr. Zhang Fuping is the editor in chief.

Mr. CHEW. He is not——

Mrs. CAMMACK. My colleague, Representative Burgess, a few minutes ago exposed that TikTok and ByteDance share legal teams. You confirmed this, correct?

Mr. CHEW. Our general counsel is——

Mrs. CAMMACK. Yes? Yes or no?

Mr. CHEW [continuing]. An American lawyer, a veteran of Microsoft——

Mrs. CAMMACK. Yes. Also——

Mr. CHEW. And——

Mrs. CAMMACK [continuing]. My colleague, Representative Latta, confirmed that your parent company, ByteDance, currently can access user data. Yes?

Mr. CHEW. Let's——

Mrs. CAMMACK. Yes.

Mr. CHEW. We have to be more specific.

Mrs. CAMMACK. Yes.

Mr. CHEW. After Project Texas, no.

Mrs. CAMMACK. You say—I am not asking after Project Texas. I am asking now. Yes.

Mr. CHEW. Some user data is public data, Congresswoman, which means everybody——

Mrs. CAMMACK. So you confirm that.

Mr. CHEW [continuing]. Can search around the Internet.

Mrs. CAMMACK. What is interesting to me is that you have used the word "transparency" over a half a dozen times in your opening testimony and subsequently again in your answers to my colleagues. Yet the interesting thing to me is that ByteDance, your parent company, has gone out of their way to hide and airbrush corporate structure ties to the CCP, the company's founder, and their activities.

You can look no further than the fact that ByteDance's website has been scrubbed. In fact, we found web pages from the Beijing Internet Association, the industry association charged with Communist Party building work of Internet companies in Beijing. They have been archived but since deleted. It makes you kind of wonder why.

Yes or no, ByteDance is required to have a member of the Chinese Government on its board with veto power. Is that correct?

Mr. CHEW. No, that is not correct. ByteDance owns some Chinese businesses, and you are talking about a very special subsidiary that is——

Mrs. CAMMACK. Mr. Shou——

Mr. CHEW [continuing]. For Chinese business licensing——

Mrs. CAMMACK. Mr. Shou, I am going to have to move on.

You have said repeatedly that there is no threat, that this is a platform for entertainment and for fun. I have to ask you then, if there is no threat to Americans, if there is no threat to our data privacy, security, why did an internal memo from TikTok corporate headquarters explicitly coach senior management to "downplay the parent company ByteDance"? Why would they say, downplay the China association and downplay AI?

This is from an internal memo from your company. Why, if you had nothing to hide, would you need to downplay the association with ByteDance in China?

Mr. CHEW. Congresswoman, I have not seen this memo.

Mrs. CAMMACK. You can't answer that question.

Mr. CHEW. I can say——

Mrs. CAMMACK. Mr. Shou, I would like to direct your attention to the screen for a short video, if you don't mind.

[Video shown.]

Mrs. CAMMACK. Mr. Shou, that video was posted 41 days ago. As you can see, it is captioned "Me asf [sic] at the House Energy and Commerce Committee on March 23rd of this year." This video was posted before this hearing was publicly noticed. I think that is a very interesting point to raise.

But more concerning is the fact that it names this chairwoman by name. Your own community guidelines state that you have a firm stance against enabling violence on or off TikTok: "We do not

allow people to use our platform to threaten or incite violence, or to promote violent extremist organizations, individuals, or acts. When there is a threat to public safety or an account is used to promote or glorify off platform violence, we ban the account.'' This video has been up for 41 days. It is a direct threat to the chairwoman of this committee, the people in this room, and yet it still remains on the platform. And you expect us to believe that you are capable of maintaining the data security—privacy and security of 150 million Americans, where you can't even protect the people in this room?

I think that is a blatant display of how vulnerable people who use TikTok are. You couldn't take action after 41 days, when a clear threat, a very violent threat to the chairwoman of this committee and the members of this committee, was posted on your platform. You damn well know that you cannot protect the data and security of this committee or the 150 million users of your app, because it is an extension of the CCP.

And with that I yield back.

Mr. CHEW. Can I respond, Chair?

Mrs. RODGERS. No, we are going to move on. The gentlelady yields back.

The chairman recognizes the lady from California, Ms. Matsui, for 5 minutes.

Ms. MATSUI. Thank you very much, Madam Chair. And I am really glad that we are having this very important hearing here today.

And let me just say, make no mistake, the Chinese Government represents a real and immediate threat. Look no further than even the vulnerable gear still in our telecom networks that needs to be ripped and replaced.

But we can't lose sight of the important Internet governance issues TikTok and other social media companies represent. I am especially committed to demanding transparency from large platforms about the algorithms that shape our online interactions, especially for teenagers and young users. And that is why I introduced the Algorithmic Justice and Online Platform Transparency Act to bring greater visibility into this ecosystem.

My bill would require—would prohibit algorithms that discriminate on the basis of race, age, gender, ability, and other protected characteristics. It also would establish a safety and effectiveness standard for algorithms, while requiring new forms of inner sight—oversight. Now, this bill would require online platforms to publish annual public reports detailing their content moderation practices, which I believe should be a baseline requirement to enable meaningful oversight and consumer choice.

Mr. Chew, just yes or no: Do you believe a requirement for annual content moderation practices for social media platforms would be beneficial? Yes or no.

Mr. CHEW. Yes.

Ms. MATSUI. This transparency bill would also require online platforms to maintain detailed records describing their algorithmic process for review by the Federal Trade Commission in compliance with key privacy and data de-identification standards.

Mr. Chew, does TikTok currently maintain records describing their algorithmic processes? Yes or no.

Mr. CHEW. Congressman, I would need to check and get back to you on what kind of specific records you are talking about.

Ms. MATSUI. I wait for that.

Over the past few years, alarming information brought to light by whistleblowers have shown that social media companies are intimately aware of the effect their products have on young women, political extremism, and more. Despite this, they withheld those studies or declined to investigate further. In either case, it shows a pattern—evasive or negligent behavior that I find concerning in the extreme.

Mr. Chew, does TikTok conduct its own studies on the effect of its algorithms and content distribution models on mental health or safety?

And if so, how and when are those findings made public?

And if not, do you believe they are necessary?

Mr. CHEW. Congresswoman, we rely on external third parties and fund their research to help us understand some of these issues. For example, we worked with the Digital Wellness Lab at the Boston Children's Hospital to understand the 60-minute time limit that we put for all our under-18 users. And we are supportive of legislation that provides more funding for research like, for example, for the NIH.

Ms. MATSUI. OK. TikTok tailors its recommended content based on user activity to encourage people to spend more time on the app. While this practice is by no means unique to TikTok, given the prevalence of young users and the digestible nature of short-form video, I am concerned about the app's tendency to exacerbate existing mental health challenges.

Mr. Chew, does TikTok have different policies for amplifying content that would be related to depression or dieting, versus content like gardening and sports? If yes, describe these policy differences. If no, why not?

Mr. CHEW. Congresswoman, thank you for that. This is a great question. The answer is yes. We are trying out some policies together with experts to understand certain contents that are not inherently harmful, like extreme fitness, for example, but shouldn't be seen too much. And this is—these are models that we are building, and we are trying to understand, you know, together with experts, how to best implement them across our platform, particularly for younger users.

Ms. MATSUI. OK, so——

Mr. CHEW. Under 18, yes.

Ms. MATSUI [continuing]. In cases where users have been engaging with potentially harmful content, I believe it is imperative that the app takes steps to moderate that behavior rather than continuing to promote it. That means, in a sense——

Mr. CHEW. I apologize, I——

Ms. MATSUI [continuing]. Very intentional about that.

Mr. CHEW. I wasn't clear. First, anything that is violative and harmful we remove. What I meant to say were things—content that is not inherently harmful, like some of the extreme fitness videos about people running 100 miles, it is not inherently harmful,

but if we show them too much—the experts are telling us that we should disperse them more, and make sure that they are not seen too regularly——

Ms. MATSUI. So you are very intentional——

Mr. CHEW [continuing]. Especially by younger users.

Ms. MATSUI [continuing]. About that, then. It is something that you are——

Mr. CHEW. We are working on it, yes, yes.

Ms. MATSUI. You are working on it?

Mr. CHEW. Yes.

Ms. MATSUI. OK, I yield back.

Mrs. RODGERS. The gentlelady yields back. The Chair recognizes the gentleman from Florida, Mr. Bilirakis, for 5 minutes.

Mr. BILIRAKIS. Thank you, Madam Chair. I appreciate it very much. Thanks for holding this hearing.

Mr. Chew, your algorithms have prioritized providing harmful content directly to children, like self-harm challenges and even suicide. Just 3 days ago, Italy opened an investigation into the TikTok over user safety concerns after the so-called French Scar Challenge went viral on your platform.

I know you know about the Blackout Challenge, which others may know as the Choking Challenge that encourages children to bring them to the point of unconsciousness or, in some cases, tragically, death. If that isn't enough, I want to share the story of Chase Nasca, a 16-year-old boy from New York who tragically ended his life a year ago by stepping in front of a train.

I want to thank his parents again. They are here. I want to thank his parents for being here today, and allowing us to show this.

Mr. Chew, your company destroyed their lives. Your company destroyed their lives. I admire their courage to be here and share Chase's story in the hopes that it will prevent this from happening to other families. The content in Chase's For You page was not a window to discovery, as you boldly claimed in your testimony. It wasn't content from a creator that you invited to roam the Hill today, or STEM education content that children in China see. Instead, his For You page was, sadly, a window to discover suicide. It is unacceptable, sir, that, even after knowing all these dangers, you still claim TikTok is something grand to behold.

I want you to see what Chase would see. And I think if you want—again, would you share this content with your children, with your two children? Would you want them to see this?

And again, I want to warn everyone watching that you may find this content disturbing, but we need to watch this, please.

[Video shown.]

Mr. BILIRAKIS. Mr. Chew, please, your technology is literally leading to death. Mr. Chew, yes or no: Do you have full responsibility for your algorithms used by TikTok to prioritize content to its users? Yes or no, please.

Mr. CHEW. Congressman, I would just like to—respectfully, if you don't mind, I would just like to start by saying it is devastating to hear about the news of——

Mr. BILIRAKIS. Yes, yes.

Mr. CHEW. As a father myself, this is tragic.

Mr. BILIRAKIS. Sir, yes or no. I will repeat the question: Do you have full responsibility over the algorithms used by TikTok to prioritize content to its users? Yes or no, please.

Mr. CHEW. Congressman, we do take these issues very seriously.

Mr. BILIRAKIS. Yes or no?

Mr. CHEW. And we do provide resources for anyone who types in anything that——

Mr. BILIRAKIS. Sir, yes or no.

I see you are not willing to answer the question or take any responsibility for your parent companies, the technology, and the harms it creates. It is just very, very sad. Very sad.

Mr. CHEW. It is very sad. I——

Mr. BILIRAKIS. This is why Congress needs to enact a comprehensive privacy and data security law to give Americans more control over their information, and to protect our children. We must save our children from Big Tech companies like yours who continue to abuse and manipulate them for your own gain.

And I will yield back, Madam Chair.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the lady from Florida, Ms. Castor, for 5 minutes.

Ms. CASTOR. Well, thank you, Madam Chair.

Colleagues, it is urgent that the Congress pass an online data privacy law that protects the personal privacy of Americans online, and particularly our kids. While this hearing shines a light on TikTok, this hearing also should serve as a call to action for the Congress to act now to protect Americans from surveillance, tracking, personal data gathering, and addictive algorithmic operations that serve up harmful content and has a corrosive effect on our kids' mental and physical well-being.

For many years I have sounded the alarm in this committee of how Big Tech platforms like TikTok and Facebook and Instagram incessantly surveil, track, gather personal, private information, and use it along with data brokers to target and influence our behavior. This is a much broader issue than TikTok in China. There are other malign actors across the world who gather data to use it as an element of social control and influence peddling and worse.

And as I detailed in this committee last year when we passed the—our online privacy law, the harms to children are very serious and demand swift action. Big Tech platforms profit immensely from keeping children addicted. They do not care about the privacy, safety, and health of our kids. They are the modern-day tobacco and cigarette companies that for so long resisted and misled Congress. And it took the Congress—it took action by the Congress to actually protect our kids and to outlaw smoking by young people.

In early 2020, based upon the growing body of evidence to harm of—to kids online, I introduced the Kids Privacy Act and the KIDS Act. And I want to thank all of the researchers, the young people, the parents, the Surgeon General of the United States, who have explained the correlation between social media usage and body dissatisfaction, disordered eating habits, anxiety, depression, self-injury, suicide ideation, and cyber-bullying.

Heck, Frances Haugen, the Facebook whistleblower, was right here and testified to us that Facebook and Instagram conducted research on this topic. They knew and understood the harms, but

they continued to elevate profits over the well-being of children. And TikTok does the same.

Last Congress, when we passed the ADPPA, the committee incorporated many of these important child online privacy and safety provisions from my bills. But we can make the 118th Congress' version of this bill, of this new law, even more protective of children. And I look forward to working with the Chair and the ranking member to make that happen.

Mr. Chew, TikTok has incredible sway over children in the U.S., but you don't have a very good track record. In 2019 TikTok was hit with the largest civil penalty by the Federal Trade Commission in a children's privacy case. Four years later, TikTok still has not taken sufficient action to fix the problems, I assume, because child users are incredibly profitable to your bottom line.

So answer me this: TikTok allows advertisers to specifically target advertising to children aged 13 to 17, correct?

Mr. CHEW. Congresswoman, I do want to disagree with the statement——

Ms. CASTOR. Yes or no?

Mr. CHEW [continuing]. That child abuses are not allowed on our platform.

Ms. CASTOR. Just yes or no.

Mr. CHEW. It is deplorable conduct, and it is not allowed on our platform.

Ms. CASTOR. Do you target—do you target—do you target advertising to young people aged 13 to 17?

Mr. CHEW. We do serve personalized advertising——

Ms. CASTOR. OK, thank you.

Mr. CHEW [continuing]. At this point, but the policies are very safe for them.

Ms. CASTOR. And how much money—how much money does TikTok make off selling ads targeted to minors?

Mr. CHEW. Congresswoman, can I clarify? Minors in what age?

Ms. CASTOR. From just say age 13 to 17.

Mr. CHEW. For the teenager population, I want to clarify that. We do have a 13—under 13 experience, and with zero advertising on that platform. For those——

Ms. CASTOR. Well, that is a whole other topic. OK.

Mr. CHEW. Between 13 and 17, if you don't mind, I will check in with my team and get back to you on those answers.

Ms. CASTOR. You know, TikTok could be designed to minimize the harm to kids, but a decision was made to aggressively addict kids in the name of profits. And it is our responsibility, Members, to act swiftly to address this. This has gone on for too long. We have dilly-dallied too much. This committee, thankfully, we have taken responsibility and enacted, but we have an enormous responsibility to act swiftly, and get this bill to the floor of the House and passed into law as soon as possible.

Thank you. I yield back my time.

Mrs. RODGERS. The gentlelady yields back. The Chair recognizes the gentleman from Ohio, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Madam Chair.

Mr. Chew, I am an information technology professional. I have been doing it for the most of my life. You have been evasive in

many of your answers. I am going to talk to you in some language that maybe you will better understand, ones and zeros. OK?

Let's talk about the Citizen Lab Report. This is something your team frequently mentions in hearings as a way to exonerate yourself. For example, in the limitations section it reads, "We could not examine every source code component and test in the apps in every circumstance, which means our methods could not find every security issue, privacy violation, and censorship event. So it is an incomplete assessment." The report notes that TikTok's data collection using third-party trackers was in apparent conflict with the GDPR, and that multiple themes were censored by TikTok.

What is shocking to me is the shared source code between TikTok in the United States and the CCP-centered Douyin. The Citizen Labs Report says that many of the functions and classes were identical and that the differences in behavior between TikTok in the United States and Douyin in China are slight changes in hard-coded values. Incredibly, specific censorship parameters from Douyin are present in TikTok, but just turned off. The authors say that, for unknown reasons, the parameter variable itself is preserved.

So while Citizen Labs may have been afraid to say the obvious conclusion, Mr. Chew, I am not. TikTok's source code is riddled with backdoors and CCP censorship devices. Here is the truth: In a million lines of code, the smallest shift from a zero to a one on just one of thousands of versions of TikTok on the market will unlock explicit CCP censorship and access to American data.

Mr. Chew, as CEO of TikTok, why have you not directed your engineers to change the source code?

Mr. CHEW. Congressman, thank you for the question. I——

Mr. JOHNSON. Have you directed them to change the source code?

Mr. CHEW. Like what we are offering——

Mr. JOHNSON. Yes or no, have you directed them to change that source code?

Mr. CHEW. Congressman, if you give me a bit of time to just——

Mr. JOHNSON. No, I don't—it is a yes or no question. Have you directed your engineers to change that source code?

Mr. CHEW. I am not sure I understand.

Mr. JOHNSON. Why are you allowing TikTok to continue to have the capacity for censorship, and yet you claim here that you don't?

Mr. CHEW. It doesn't——

Mr. JOHNSON. Let me remind you of something. Do you realize that making false and misleading statements to Congress is a Federal crime?

Mr. CHEW. Yes, I do.

Mr. JOHNSON. OK. So have you directed your engineers to change that source code?

Mr. CHEW. I am giving third-party access monitoring by experts.

Mr. JOHNSON. OK.

Mr. CHEW. And Congressmen, you are an expert on this——

Mr. JOHNSON. What percentage——

Mr. CHEW [continuing]. You could agree with me that no other company does this——

Mr. JOHNSON. What percentage of TikTok source code is the same as Douyin? What percentage?

Mr. CHEW. I can get back to you on the specifics.

Mr. JOHNSON. OK, I would appreciate that.

Where was the source code for TikTok developed? Was it developed in China or in the United States?

Mr. CHEW. It is a global collaborative effort, like a lot of——

Mr. JOHNSON. And was it developed in——

Mr. CHEW [continuing]. Codes in a lot of countries.

Mr. JOHNSON. Was it developed in China? Some of it?

Mr. CHEW. Some of it is.

Mr. JOHNSON. OK. And ByteDance.

Can the—when it is compiled in the compilation process, can byte code be manipulated? We have talked a lot about source code. What about the byte code, the ones and zeros that actually execute on the device?

Mr. CHEW. That is——

Mr. JOHNSON. Can it be manipulated?

Mr. CHEW. Congressman?

Mr. JOHNSON. Yes.

Mr. CHEW. Congressman, to give you comfort, that is why we are giving third-party monitors.

Mr. JOHNSON. As——

Mr. CHEW. As an expert, I think you can agree that very few companies do this——

Mr. JOHNSON. I have got the report here by Citizen Lab. I want to read you something from Ron Deibert. Specifically, in your written testimony to Congress you stated on page 9, "Citizen Lab found that there was no overt data transmission by TikTok to the Chinese Government, and that TikTok did not contact any servers within China." You implied that Citizen Lab exonerated TikTok from any information-sharing with China.

Well, the director of Citizen Lab saw this and issued a statement correcting the record yesterday. And I am quoting Ron Deibert, the director of the lab: "I am disappointed that TikTok executives continue citing the Citizen Lab's research in their statements to government as somehow exculpatory. I have called them out on this in the past, and it is unfortunate that I have to do it again."

He goes on to say, and I quote, "We even speculated about possible mechanisms through which the Chinese Government might use unconventional techniques to obtain TikTok user data via pressure on ByteDance."

Mr. Chew, you sent Congress written testimony citing this lab as a support of your claim that China cannot access user data, U.S. user data. And now this lab has come out to say, "We never said that, that is misleading." Mr. Chew, I hope you understand what that is. That is misleading. Mr. Chew, this is yet another instance of TikTok attempting to mislead Americans about what their technology is capable of, and who has access to their information.

Madam Chair, I would like to——

Mr. CHEW. Madam Chair, I would like to respond to that very quickly, please.

Mr. JOHNSON [continuing]. Enter this statement by Ron Deibert and the Citizens Lab into the record.

Mrs. RODGERS. Without objection, so ordered.

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

Mr. JOHNSON. With that I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair yields to the gentleman from Maryland, Mr. Sarbanes. Five minutes.

Mr. SARBANES. Thanks very much, Madam Chair.

Mr. Chew, I am going to pick up on a theme we have already covered here, which is the effect that your platform, along with many other social media platforms, by the way, has in terms of mental and behavioral health in this country. I won't speak to what is happening elsewhere in the world, but we have talked about the impact that it is having on children, on teens.

We took some action last year in this committee to try to improve access to resources, reauthorize critical programs to address mental health needs. But we need to do even more than that. And we have got to address what the Big Tech companies like TikTok are doing, because those are platforms that expose children and teens to additional risks.

The more time that middle and high schoolers spend on social media, the evidence is, the more likely they are to experience depression and anxiety. And this is particularly troubling since, apparently, 16 percent of American teenagers report that they use TikTok, quote, "almost constantly." That is, I think, about 5 million teenagers in this country that are on TikTok all the time.

And we know that Big Tech, including TikTok, uses design features that can manipulate users, including children and teens, to keep them engaged, designed to feed them a never-ending stream of content, keep their attention for hours on end, which includes capitalizing on the desire for others' approval through "like" features, preying on the fear of missing out through push notifications, and so forth.

Again, you are part of an industry that is set up to do this. You, in some sense, don't appear to be able to help yourselves in reaching out and finding that new user and then holding onto them. TikTok itself has acknowledged that these features and others, like the endless scroll feature, can have an outsized effect on teens, and we have been discussing today how your app only intensifies that harm by amplifying dangerous content and misinformation.

I don't want to be too paternalistic here, because we have young people in the audience. We have got TikTok users that are watching this hearing, and I am sure they have their own ideas about how this technology is being managed by TikTok and other social media platforms. They like to access the platforms, and they should be able to do that safely. So it is certainly in their interest, and they can drive this conversation, I think, perfectly well.

But it is not a fair fight, is it? I mean, the algorithms are on one side of the screen. The human brain is on the other side of the screen, drowning in these algorithms, in many instances, at an age where the brain is not even fully developed yet. So those addictive impulses are being sort of perfected by the technology. And again, it leaves the users sort of helpless in the face of that.

Are you looking at ways to redesign core features like the ones I mentioned to be less manipulative—excuse me—and addictive for users, and can you commit to making some of those modifications here today?

Mr. CHEW. Congressman, thank you. We do want to be leading in terms of safety of our users, particularly for teenagers. We were the first to launch a 60-minute watch limit.

Mr. SARBANES. Yes, let's talk about the 60-minute watch limit.

Mr. CHEW. And I am very glad to see people, others in our industry, follow.

For many of your recommendations, we will study them very seriously. We actually have a series of features. Like, for example, if you are under 16 you cannot use a direct messaging feature because, you know, we want to protect those younger users. If you are under 16, you cannot go viral by default. If you are under 18, you cannot go live. And——

Mr. SARBANES. Let me go back to the 60-minute limit, because my understanding is that teens can pretty easily bypass the notification to continue using the app if they want to.

I mean, let's face it, our teens are smarter than we are by half, and they know how to use the technology, and they can get around these limits if they want to. Are you measuring how many teens continue to exceed the 60 minutes of time on that app——

Mr. CHEW. We understand——

Mr. SARBANES [continuing]. How that is working?

Mr. CHEW. We understand those concerns. What we—our intention is to have the teens and their parents have these conversations about what is the appropriate amount of time for social media. That is why we give the parents what we call Family Pairing——

Mr. SARBANES. Let me ask you this question before I run out of time. If you concluded that putting some reasonable limits in place and trying to find a way to enforce them would lead some percentage of your users to leave TikTok and go somewhere else, is that something that you are prepared to accept?

Mr. CHEW. Yes.

Mr. SARBANES. Really? Well, I would love to get the research on how these limits are being implemented, how they are being bypassed, and the things that you are taking—the measures you are taking to address those issues going forward. Please bring that information back to our committee as we move forward.

Mr. CHEW. I will be happy to.

Mr. SARBANES. I yield back.

Mrs. RODGERS. The gentleman yields. The Chair recognizes the gentleman from Kentucky, Mr. Guthrie, for 5 minutes.

Mr. GUTHRIE. Thank you, Madam Chair, for yielding. I appreciate the time.

Mr. Chew, your terms of service specifically state that TikTok does—and I quote—"not allow the depiction, promotion, or trade of drugs or other controlled substances." Despite this content being against your terms of service—and I have brought this up with other service providers—but despite this content being against your terms of service, content on your platform related to illicit drugs like fentanyl, drug trafficking, and other illicit activity is pervasive and racks up hundreds of thousands of views.

For example, in 2020 the Benadryl Challenge resulted in the death of an American teenager. And we heard of another one, a challenge earlier today that brought a death of a teenager.

While you were at ByteDance—you were the CFO for ByteDance—did Douyin allow related illicit drug trafficking or challenges resulting in death or injury to kids?

Mr. CHEW. Congressman, I represent TikTok here today. I can tell you that TikTok does not allow illegal drugs——

Mr. GUTHRIE. Does Douyin——

Mr. CHEW [continuing]. On our platform.

Mr. GUTHRIE. Does Douyin do it in China?

Mr. CHEW. I believe they don't allow this, but I will need to check. I don't run that business.

Mr. GUTHRIE. So my question is——

Mr. CHEW. I can tell you TikTok does not allow this.

Mr. GUTHRIE. Because all we are concerned about—and my guess—and would Douyin allow for 41 days a threat against a member of the Chinese Communist Party to stand on their site for 41 days?

Mr. CHEW. Again, I cannot speak for Douyin and, I am sorry, I didn't hear the second part of what you said.

Mr. GUTHRIE. Well, we had a threat against the chairman of our committee that was on your site for 41 days. My guess is that would not be allowed in China.

Mr. CHEW. That content is violative. I would look into the specifics, and I would—if it violates our guidelines, it will be taken down on TikTok.

Mr. GUTHRIE. Yes, surely——

Mr. CHEW. Yes.

Mr. GUTHRIE [continuing]. It appears that it does. But the problem is that—what I am trying to get at is you seem to be able to prevent this content in China, but you—so not even taking it down, just prevent it from being posted. And yet it is all—it is on your website.

So I have a couple of questions about—you said earlier as soon as you find this information, you take it down. So how quickly does your algorithm detect keywords or content that involve illicit drug trafficking before these posts are self-reported or used by others?

Mr. CHEW. We have about 40,000 people working on this now, together with the machines that we train. I don't think any company in our industry can be perfect at this. This is a real big challenge for our industry, but our goal is to get this—any violative content, including illegal drugs, down to a very, very small number.

Mr. GUTHRIE. That is the problem. When we have these hearings, we have CEOs of different companies, and of your colleagues and competitors. And we always hear apologies, and we always hear, "We want to do better at this," but it just doesn't seem to keep improving. And we are hearing stories of our children and, obviously, that has been talked about today.

So how many posts and accounts have been identified and removed from TikTok due to content posts posted related to illicit drugs or other controlled substances?

Mr. CHEW. Congressman, we do publish that in a transparency report. I can get my team to get the information to yours.

Mr. GUTHRIE. Thank you. I appreciate that.

Also, we understand that the way that people use TikTok or other platforms similar to yours is that they ensure flagged user

content isn't permitted to jump from—so my question—so what we have heard is that the instances—the users see a drug advertisement and then give a code to go to another site. So my question is, do you work with other platforms to ensure flagged user content isn't permitted to jump from one platform to others?

Mr. CHEW. I will check with my team. I would love to work with our industry to make sure that we stamp out these problems. You know, violative content should not be allowed on any platforms, in my opinion.

Mr. GUTHRIE. Well, this is what is, you know, kind of frustrating to all of us here, is that we look at what is happening on your sites and others, and particularly that—we know, because we have done the research, that you can't have access to illicit drug information on Douyin, which is a sister company, as you say, in China. And so it absolutely—if you can prevent it on one and not the other, you obviously have the ability to stop it from moving forward, and yet you don't.

Would you like to expand how one of your sister companies can prevent that, and you not—I know you don't represent Douyin, but they don't allow it. But it happens on your platform. What is the difference?

Mr. CHEW. First of all, the majority of the content on TikTok is fun, entertaining, informative, and very positive for our users. Like other companies that operate in this country, we have to deal with some bad actors who come and publish some content on illegal drugs, you know, other——

Mr. GUTHRIE. But the bad actors don't seem to be able to access Douyin.

Mr. CHEW. The TikTok U.S. experience should be compared to other U.S. companies, because this is a common——

Mr. GUTHRIE. But your parent company has the technology to prevent it, because you prevent it in China, but you can't prevent it here. What is the difference? That is what I am asking.

Mr. CHEW. Oh, Congressman, there is no technology that is perfect in doing this. We have to deal with the reality of the country that you are operating in. And here in the United States, as with other companies, we share this challenge. We are investing a lot to address the challenge. But we are—you know, it is a shared challenge——

Mr. GUTHRIE. But you invest a lot to—seem to be able to address it in China, but not here.

Mr. CHEW. Again, you know, I think the comparison has to be within the single country. You know, we face the same set of challenges here in the U.S.——

Mr. GUTHRIE. What is the difference—oh, I am sorry, I am out of time. But what is the difference in China and here?

Mr. CHEW. Let me give you an example, Congressman. In my home country, Singapore, there is almost no illegal drug content because Singapore has very strict drug laws.

Mr. GUTHRIE. Thank you.

My time is expired, and I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentleman from New York, Mr. Tonko, for 5 minutes.

Mr. TONKO. Thank you, Madam Chair. I am concerned that TikTok's algorithm prize—preys on vulnerable people, including those struggling with addiction, eating orders—disorders, and other mental health conditions. The platform is designed to push content to users that will watch more frequently and for longer periods of time.

Unfortunately for many people suffering from certain mental health disorders, videos that reinforce their fears or negative self-image are more engaging. On top of that, TikTok has received sensitive patient health information and records of browsing activity from multiple telehealth companies like BetterHelp and Cerebral.

People's personal struggles should not be fuel for TikTok's profits. People should be able to seek help to address serious medical concerns without being afraid that their information will be shared with social media companies trying to push more products, services, or content at them.

So, Mr. Chew, will TikTok continue to get information from third parties on its users' health, including their mental health? Yes or no.

Mr. CHEW. We will continue to work with experts—yes, if that is the question—to identify these issues.

Mr. TONKO. Will you continue to get information from these third parties, including their mental health? Yes or no.

Mr. CHEW. Congressman, I am sorry. I may not understand your question. If your question is if I am working with them on these issues, the answer is yes.

Mr. TONKO. It is not the question. It is, will you continue to get information from these third parties on its users' health?

Mr. CHEW. Get information? We do not get any user health information from third parties, Congressman.

Mr. TONKO. You have talked a lot about user privacy and safety. Will you commit here today to no longer using data about users' health, particularly their mental health, to push them content or sell ads? Yes or no.

Mr. CHEW. We take our users' mental health very seriously. We——

Mr. TONKO. Yes or no?

Mr. CHEW. As far as I am aware, we don't do that, Congressman. It is not what——

Mr. TONKO. So the answer is no, you will no longer use data about users' health.

TikTok systematically exploits users' anxieties by pushing alarming and distressing content onto their For You page. For example, in May of 2022, the LA Times found that some pregnant users searching for information about their pregnancies on TikTok were then shown information about miscarriages, stillbirths, and delivery room traumas.

Your company knows that distressing content can have the perverse effect of feeding user engagement. And for TikTok, engagement means money. In the course of a week, what percentage of content that a user sees is considered potentially harmful or distressing content?

Mr. CHEW. Congressman, we work with a lot of experts on this. Even before we set the 60-minute time limit for under 18s, if you

spend too much time on our platform—you can try it. If you spend too much time, we will actually send you videos to tell you to go out and get some air and get off the platform.

Mr. TONKO. What percentage of content that a user sees is considered potentially harmful?

Mr. CHEW. I would need to follow up with my team and get back to you on that, if that is OK.

Mr. TONKO. Well, a ballpark.

Mr. CHEW. I would need to follow up with my team.

Mr. TONKO. So are teenagers in particular shown more distressing content?

Mr. CHEW. The opposite is true. We actually put in more restrictions to make sure that our teenagers get a better experience, you know——

Mr. TONKO. Are expectant or new parents showing more distressing content?

Mr. CHEW. I know of many parents, including one I met recently, who actually used our platform to find communities to connect with other parents and learn a lot more. I have heard amazing stories of creators who have difficulties, you know——

Mr. TONKO. Reclaiming my time, are individuals with eating disorders shown more distressing content?

Mr. CHEW. We do not—we remove all content that glorifies eating disorders, and we have worked with experts to look at certain inherently—certain content that may not inherently be harmful, like diet trends, and make sure that we disperse them more throughout our algorithm.

Mr. TONKO. What about those with mental health issues, are they given——

Mr. CHEW. This is an issue——

Mr. TONKO [continuing]. More distressing content?

Mr. CHEW. If a user searches, you know, words that expresses mental health issues, we actually redirect them to a safety page. Like, for example, if you—I don't know if I should say this in public—if you search "I want to die," we will redirect you to a safety page, for example.

Mr. TONKO. So what about those suffering from addiction? Are they given more distressing content?

Mr. CHEW. I am sorry, Congressman, I missed that question.

Mr. TONKO. Those suffering from addiction, are they given more distressing content?

Mr. CHEW. I missed the first few words, I apologize.

Mr. TONKO. Those—what about those suffering from addiction? Are they given more distressing content?

Mr. CHEW. Oh, those suffering from——

Mr. TONKO. Addiction.

Mr. CHEW. Addiction? Do you mean drug addiction or——

Mr. TONKO. Yes, or any order of addiction.

Mr. CHEW. If people search for content—and you can try it on a variety of subjects—we will actually direct you to a safety page to give you more resources.

And a lot of recovering addicts have actually found communities on TikTok. And it has really helped them, you know, find the

voices and the community and the courage to really overcome their addiction. I personally have heard stories of that.

Mr. TONKO. Well, I appreciate your answers, but I was looking for yes or no, and we did not get those. And again, I think the more that they watch this distressing content, the more profit TikTok makes. And that is distressing.

I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentleman from Michigan, Mr. Walberg, for 5 minutes.

Mr. WALBERG. Thank you, Madam Chair.

And we are glad that you are here, Mr. Chew. As Chair Rodgers and Representative Burgess mentioned this morning, The Wall Street Journal reported that China will firmly oppose any forced sale or divestiture of TikTok. And this is based not on conjecture, but it is based on comments provided by the official spokesperson at the Ministry of Commerce, who said that any TikTok sale or spinoff would amount to a technology export and would have to adhere to Chinese law and approval. This spokesperson was quoted as saying the Chinese—and I quote—"The Chinese Government will make decisions according to the law." The Chinese Government.

Mr. Chew, do you agree with this official? Yes or no.

Mr. CHEW. Congressman, I cannot speak on behalf of a Chinese Government official.

Mr. WALBERG. Do you agree with that official?

Mr. CHEW. We will need to look at this, because Project Texas is designed to move forward here in the United States, and we are not discussing this. So I don't have specifics.

Mr. WALBERG. You know, your company is valued at upwards of $50 billion and has been on the verge of forced sale or ban for 3 years, at least, correct?

Do you expect this committee to believe you haven't already discussed this scenario with your team?

And you should have an answer to this, yes or no: "I agree with the Communist Party" or "I don't agree with the Communist Party."

So I guess I would say at that point you disagree with the Communist Party. Explain your discrepancy.

Mr. CHEW. Congressman, for 2 years we spent a billion and a half U.S. dollars to build Project Texas. This is after very extensive discussions with relevant folks——

Mr. WALBERG. Project Texas is just something expanded for the future. We are talking about now. We are talking about what you are doing now, what your expectations are now, what your relationship is with the Communist Party, which is our major concern of what the impact that will be with a country—let me rephrase that—with the Communist Party that doesn't care about America and sees us as standing in their way for super power. That is our concern.

And for you to have direct relationship, direct ownership with ByteDance, and to not have a characterization or an agreement or disagreement that you say—explicitly with this party policy, it is hard for us to believe what you are saying.

Let me move on. Following up on what Mr. Latta asked about data access by Chinese engineers, in responding to Mr. Latta you talked about where American user data would be stored in the future. But the question was about access today. Storage in the future versus access today. This is total redirection. This blows up any trust we could desire to develop.

So to be clear, Mr. Chew, today do ByteDance employees in Beijing have access to American data?

Mr. CHEW. Congressman, we have been very open about this. We have relied on global interoperability——

Mr. WALBERG. You have access to American data.

Mr. CHEW. Congressman, I am answering your question, if you give me just a bit of time. We rely on global interoperability, and we have employees in China. So, yes, the Chinese engineers do have access to global data.

Mr. WALBERG. They have access to global data.

Mr. CHEW. We have heard.

Mr. WALBERG. Not storage.

Mr. CHEW. No, storage has always been in Virginia and Singapore. The physical servers——

Mr. WALBERG. You have no access to storage, to American data today.

Mr. CHEW. That is not what I said. I said——

Mr. WALBERG. So you do have access to American data, and you have storage of American data.

Mr. CHEW. The American data has always been stored in Virginia and Singapore in the past, and access of this is on an as-required basis——

Mr. WALBERG. As required of who?

Mr. CHEW. By engineers for business purposes.

Mr. WALBERG. By engineers.

Mr. CHEW. This is a private——

Mr. WALBERG. ByteDance?

Mr. CHEW. ByteDance——

Mr. WALBERG. The Communist Party.

Mr. CHEW. No, no.

Mr. WALBERG. How can you say that——

Mr. CHEW. This is a——

Mr. WALBERG [continuing]. If they have access?

Mr. CHEW. This is a private business. And like many other businesses, many other American companies, we rely on a global workforce.

Mr. WALBERG. So the global workforce that includes ByteDance, which is connected directly to the Chinese Communist Party, has access——

Mr. CHEW. That is a characterization that we disagree with.

Now, in the future——

Mr. WALBERG. That is not what we can disagree with. That is a fact.

Mr. CHEW. It is not, unfortunately.

Mr. WALBERG. The CEO of ByteDance and your relationship to them——

Mr. CHEW. It is not—Congressman, respectfully, in my opening statement I said this is a private company. It is owned 60 percent

by global investors. Three out of the five board members of ByteDance are Americans. This is a private business.

Mr. WALBERG. And you report directly to ByteDance, with a CEO who is a member of the Communist Party. Let me move on.

Mr. CHEW. He is not.

Mr. WALBERG. I think we got the answer, sadly, at this point.

I believe my time is expired, so I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes Ms. Clarke for 5 minutes.

Ms. CLARKE. Thank you, Chairwoman Rodgers, thank the Ranking Member Pallone for holding today's hearing.

Throughout this hearing—I also want to thank our witness for being here to testify on what are very important issues before us today.

Throughout this hearing, my colleagues have outlined the potential threat posed by the security of Americans' data by TikTok being affiliated—and some would say owned—by a Chinese company. Foreign adversaries having direct access to Americans' data as well as the ability to influence this content Americans see on a prolific social media platform represents an unprecedented threat to American security and to our democracy. However, the problems of social media platforms' content moderation, algorithmic discrimination, and safety are neither new nor unique to TikTok.

Mr. Chew, I share the concerns raised by my colleague, Congresswoman Matsui, related to algorithms. I believe that without mitigation against bias, platforms will continue to replicate, exacerbate discrimination that is illegal under civil rights law as well as exclude important dialogue about sensitive topics like race from occurring on the platform. For example, I was disturbed by reports that TikTok content moderation algorithm flagged words like Black or Black Lives Matter as inappropriate content.

So my first question, Mr. Chew, is do you agree that platforms like TikTok should be subject to regular audits or transparency requirements to identify whether policies have a disparate impact on communities that are protected classes like race, religion, national origin, or gender?

Mr. CHEW. I think, Congresswoman, I think platforms should be very transparent on what they do there and disclose a lot of information. We can get back on the specifics of what we mean by an audit.

But I do agree very strongly that platforms should be very transparent, and it is a commitment that we are giving to this committee and all our users that our platform will be a place for freedom of expression. We embrace all diverse points of view, all ethnic minorities. You can come and say whatever you want, as long as you don't violate the rules of safety that were put in place.

And we will—we also commit to be free of all and any government manipulation. So I think I am in strong agreement with a lot of what you said.

Ms. CLARKE. Well, thank you. My bill, the Algorithmic Accountability Act, would require platforms to be transparent about their algorithms, measure disparate impact, and require risk mitigation. It is vital that the diverse culture of the United States is reflected online.

But I am concerned the algorithms and content moderation practices employed by TikTok are ignorant to the fundamental diversity, while also failing to remove content that is harmful, like child sexual abuse material, hate speech, or domestic terrorism content.

My next question to you is, it is my understanding that users must be in good standing to be eligible for compensation from TikTok's Creator Fund. For example, they can't have violated community guidelines. Is this correct?

Mr. CHEW. There are some details there, but directionally, yes.

Ms. CLARKE. If TikTok's algorithm is flagging content incorrectly, resulting in creators violating community guidelines when in fact they have not, those creators would not be eligible to receive compensation under the Creator Fund, correct?

Mr. CHEW. We do have an appeals process.

Ms. CLARKE. You have an appeals process. OK.

Mr. CHEW. Yes——

Ms. CLARKE. In my view, if TikTok employs algorithms that disproportionately misremove content from Black creators, it disproportionately silences and excludes Black creators from compensation opportunities. And this problem happens in parallel to the lack of adequate recognition, attribution, and compensation to Black creatives for their content.

The exploitation, cultural misappropriations, the erasure of Black creatives' ownership of their fashion, art, and media is nothing new. We need transparency, accountability, and bold action to mitigate against misinformation, bias, and exclusion of certain communities from the opportunities present on platforms like TikTok.

So let me—let me just say this: I am concerned about transparency, I am concerned about algorithmic accountability, and I am not clear that your organization holds those values. So I want to ask that you take a look at this, because this is all part and parcel of what we are concerned about with respect to social media platforms and the misappropriation, the ways in which those algorithms can discriminate within the context of the social media platform.

With that, Madam Chair, I yield back.

Mr. CHEW. Congresswoman, is it OK if I just very quickly respond? This is a very important topic.

Mrs. RODGERS. Unfortunately, we only have 4½ hours with you, and I am going to try to get to every Member. So we are going to keep going.

Mr. CHEW. It is very important. I would love to follow up.

Mrs. RODGERS. Well, there will be other opportunities. The lady yields back. The gentleman from Georgia, Mr. Buddy Carter, is recognized for 5 minutes.

Mr. CARTER. Thank you, Madam Chair.

Mr. Chew, welcome to the most bipartisan committee in Congress. We may not always agree on how to get there, but we care about our national security, we care about our economy, and we sure as heck care about our children. We sure do.

And that is why you are here today, because two-thirds of all the youth in our country are on your app. They spend an average of 95 minutes on your app. And, you know, research has shown that TikTok is the most addictive platform out there. And the reason for

that is, we have been told, is because it has the most advanced algorithm. And the Chinese Communist Party knows this. And I don't speak for everyone, but there are those on this committee, including myself, who believe that the Chinese Communist Party is engaged in psychological warfare through TikTok to deliberately influence U.S. children.

[Slide]

Mr. CARTER. You know, you see behind me, if you look behind me, Mr. Chew, you see some of the challenges that we have seen on TikTok. You know about them. You know about the Milk Crate, you know about the, about the Blackout Challenge, you know about the NyQuil Chicken Challenge, the Benadryl Challenge, the Dragon's Breath Liquid Nitrogen Trend, or the challenge that promotes car theft.

I want to ask you. As I understand it, there is a sister app in China, Douyin—I am sorry if I am butchering the pronunciation. Do they have these same things over there? Do they have these kind of challenges in China?

Mr. CHEW. Congressman, I am really glad you asked this question.

Mr. CARTER. Do they, yes or no?

Mr. CHEW. I am not sure, because——

Mr. CARTER. Whoa, whoa, whoa, come on, now. You are not sure?

Mr. CHEW. I really am not sure.

Mr. CARTER. Remember, you took—the chairlady, she said you got to tell the truth, OK? Do you know whether they have these kind of challenges like this over in China? Because it is my understanding they don't.

Mr. CHEW. I am not sure, because I spend my energies running TikTok.

Mr. CARTER. And you don't look at any of your other competitors, or look at anything similar to yours. So you don't know whether they have—they don't have this over in China.

Mr. CHEW. I did——

Mr. CARTER. We have it here, but they don't have it here. And that is why I am asking you this: Why is it that TikTok consistently fails to identify and moderate these kinds of harmful videos?

Mr. CHEW. Did——

Mr. CARTER. Why is it? Why is it that you allow this to go on? We have already heard, God bless you, from parents who are here with us who have lost children. I submit to you everybody up here cares about the children of this country. Tell me, tell me why.

Mr. CHEW. This is a real industry challenge, and we are working very hard——

Mr. CARTER. No, no, no. It is not industry. This is TikTok.

Mr. CHEW. It is——

Mr. CARTER. We are talking about TikTok. We are talking about why is it that you can't control this?

And—although I believe in giving credit where credit is due. I want to thank you. It is my understanding that the video that threatened the life of the chairwoman has been removed. Thank you for doing that. Sorry we had to bring it to your attention here, but it has been removed.

Tell me why this goes on.

Mr. CHEW. This is an industry challenge for all of us here, operating in this industry.

Mr. CARTER. OK. So much for industry challenge. I want to shift gears real quick.

I want to talk about biometric matrix, and I want to talk specifically—can you tell me right now, can you say with 100 percent certainty that TikTok does not use the phone's camera to determine whether the content that elicits a pupil dilation should be amplified by the algorithm? Can you tell me that?

Mr. CHEW. We do not collect body, face, or voice data to identify our users. We do not. The only——

Mr. CARTER. You don't?

Mr. CHEW. No. The only face data that you will get that we collect is when you use the filters to have, say, sunglasses on your face. We need to know where your eyes are.

Mr. CARTER. Why do you need to know where the eyes are, if you are not seeing if they are dilated?

Mr. CHEW. And that data is stored on your local device and deleted after use if you use it for facial. Again, we do not collect body, face, or voice data to identify our users.

Mr. CARTER. I find that hard to believe. It is our understanding that they are looking at the eyes.

How do you determine what age they are, then?

Mr. CHEW. We rely on age gating as our key age assurance——

Mr. CARTER. Age——

Mr. CHEW. Gating, which is when you ask the user what age they are.

We have also developed some tools, where we look at their public profile to go through the videos that they post to see whether——

Mr. CARTER. Boy, that is creepy. Tell me more about that.

Mr. CHEW. It is public. So if you post a video that is—you choose that video to go public, that is how you get people to see your video. We look at those to see if you—it matches up the age that you talked about.

Now, this is a real challenge for our industry, because privacy versus age assurance is a really big problem.

Mr. CARTER. Look, look, you keep talking about the industry. We are talking about TikTok here. We are talking about children dying. Do you know how many children have died because of this? Do you have any idea? Can you tell me?

Mr. CHEW. Congressman, again, it is heartbreaking.

Mr. CARTER. Can you tell me if——

Mr. CHEW. It is heartbreaking.

Mr. CARTER. How many children in America have died because of challenges like this?

Mr. CHEW. The majority of people who use our platform use it for positive experiences. There are——

Mr. CARTER. That is not what I asked you.

Mr. CHEW. There are some——

Mr. CARTER. I asked you, tell me the number of children, of U.S. children who have died because of these challenges.

Mr. CHEW. Congressman, again, the majority of people who come on our platform get a good experience——

Mr. CARTER. I am not talking about the majority of children. I want to know a number.

Mr. CHEW. Dangerous [inaudible] are not allowed on our platform. If we find them, we will remove them. We take this very seriously.

Mr. CARTER. Obviously, you found one today and you removed it. We had to bring it to your attention.

And I know I am out of time. Thank you for being here. Welcome again to the most bipartisan committee in Congress.

Mrs. RODGERS. The gentleman yields back. We will now take a brief recess and resume in 10 minutes. The committee stands in recess.

[Recess.]

Mrs. RODGERS. The Chair recognizes the gentleman from California, Mr. Cárdenas, for 5 minutes—Cárdenas, sorry.

Mr. CÁRDENAS. That's good. Thank you, Madam Chairwoman. I appreciate this opportunity for this committee to have this important hearing regarding TikTok and its effect on the American people, especially the American children, and the potential effect—not potential, but the effects that it has had and may have in the future when it comes to our democracy and misinformation and disinformation that permeates on TikTok.

It is unfortunate that I think most Americans—or most parents—think that TikTok is this innocent little thing where kids get on there, and they do a little dance or something like that. But TikTok is much, much more, as some of my colleagues—and I thank them for bringing up some of these serious issues, literally life and death issues that TikTok is right in the middle of.

And also, what I would like the witness to acknowledge is that it appears that Ms. Cammack, my colleague, brought up those two posters, and since then TikTok has taken them down. Since then, not before then. Are you aware of that, Mr. Chew?

Mr. CHEW. I was briefed during the break that they are taken down, Congressman.

Mr. CÁRDENAS. OK. How do you feel about the fact that they were—it was up for apparently 40-some days, 41 days, and yet in the middle of this hearing it was brought directly to your attention. And as a result, it has been taken down so quickly.

Mr. CHEW. It goes to show the enormous challenge that we have to make sure that, although the vast majority of our users come for a good experience, we need to make sure that bad actors don't pose violative content.

Mr. CÁRDENAS. Yes. And the way, Mr. Chew, that you can make sure is that you can make sure that you choose to invest more resources, more money into more ability to pull down damaging and deadly information from your platform.

Are you investing more and more and more every day into bringing down that kind of content? That is my question. Are you?

Mr. CHEW. Yes. And I have committed to investing more in this regard to stay on top of the growth.

Mr. CÁRDENAS. Right here in the United States, many, many languages are used and spoken. For example, TikTok in the United States is being used in many languages. Specifically, when it comes to Spanish language, are you dedicating more resources today than

you did months ago, years ago, on making sure that you are combing through that content to make sure that, if content is dangerous or damaging or deadly, that you are bringing it down as quickly as possible?

Mr. CHEW. Yes, we are investing in more Spanish-language content moderation. And yes, we will—once we identify——

Mr. CÁRDENAS. OK.

Mr. CHEW [continuing]. Violative content, we will take it down as soon as possible.

Mr. CÁRDENAS. And—thank you. And your testimony today isn't the only opportunity for you to commit to answering questions to this committee. So I would like you to forward to this committee—again, I am not asking for trade secrets, but I would like to get some semblance of understanding as to how much you are investing with the number of bodies, the number of people, the number of resources in making sure that you are investing more in pulling down content that is either deadly or dangerous on your platform. Can you forward that to the committee?

Mr. CHEW. I will check with my team and get back to you on this, Congressman.

Mr. CÁRDENAS. Thank you very much. I appreciate that opportunity.

As was mentioned earlier, it might sound a little funny, but you have in fact been one of the few people to unite this committee—Members, Republicans and Democrats—to be in agreement that we are frustrated with TikTok. We are upset with TikTok. And yes, you keep mentioning that there are industry issues that not only TikTok faces, but others. You remind me a lot of Mike Zuckerberg. He—when he came here, I said to my staff, "He reminds me of Fred Astaire, a good dancer with words," and you are doing the same today. A lot of your answers are a bit nebulous. They are not yes or no.

So I would like to ask you a question. Yes or no, is your revenue going up at TikTok month over month or year over year?

Mr. CHEW. Yes, our revenue is going up year over year.

Mr. CÁRDENAS. OK. And with that, some of the answers I would like you to forward this committee is, are you investing more and more money into making sure that content that is dangerous and/or deadly, you are investing more and more resources in that aspect of your expenditures and your commitment to your users and to your organization?

Mr. CHEW. Yes, I commit to that, and we will—we are investing more, and we will continue to do that.

Mr. CÁRDENAS. OK. My last question is this: Are you a Chinese company?

Mr. CHEW. TikTok is a company that is now headquartered in Singapore and Los Angeles.

Mr. CÁRDENAS. OK.

Mr. CHEW. We are not available in mainland China. Our users are in other countries around the world.

Mr. CÁRDENAS. OK. Is there a corporation that has any authority above TikTok?

Mr. CHEW. TikTok is a subsidiary of ByteDance, which is founded by a Chinese founder.

Mr. CÁRDENAS. And ByteDance is a Chinese company?

Mr. CHEW. Well, ByteDance owns many businesses that operates in China.

Mr. CÁRDENAS. Is it or is it not a Chinese company?

Mr. CHEW. Congressman, the way we look at it, it was founded by Chinese entrepreneurs——

Mr. CÁRDENAS. No, no, no, no, I am not asking you how you look at it. Fact. Is it a Chinese company or not?

For example, Dell is a company. It is an American company. They have activities all over the world.

Is it a Chinese company?

Mr. CHEW. I frequently have this discussion with others on what is a company that is now global.

Mr. CÁRDENAS. That is OK. I prefer you answer the question and stop dancing verbally on it.

Madam Chair, my time is expired. Thank you very much.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentleman from California, Mr. Obernolte.

Mr. OBERNOLTE. Well, thank you very much.

Mr. Chew, it is nice to see you again. If I could just bring us back up to 30,000 feet for a second, I just want to talk about what we are afraid of here, you know, what we fear might happen.

Social media companies—and TikTok is unique in this—is not unique in this—gather a tremendous amount of user data, and then use powerful AI tools to use that data to make eerily accurate predictions of human behavior, and then seek to manipulate that behavior. And that is something that it is not just TikTok, it is all our social media companies that are doing this.

Ultimately, the solution is to enact comprehensive Federal data privacy legislation that will prevent that kind of behavior, or at least allow users to consent to it. And that is, I know, something that the Chair is working on, the ranking member. I hope that this committee will act on that this year.

The specific concern here, though, as regards TikTok is that this type of capability falling into the hands of foreign countries is something that has national security implications. And that is why Congress is getting involved on this issue. So I know that you have proposed Project Texas in an effort to alleviate these fears. So I wanted to ask some specific technical questions about Project Texas, and the way that you believe that it will solve this problem.

So one of the things that you have said in your testimony is that part of Project Texas will have engineers at Oracle going through the source code for TikTok. How large is that code base?

Mr. CHEW. Well, it is not small, but it is not just Oracle, Congressman. We are also inviting other third-party monitors. We are in the process of figuring out who the best——

Mr. OBERNOLTE. Sure. So we are talking—are we talking millions, tens of millions of lines of code? How big is the base?

Mr. CHEW. It is significant, but it is something that we believe can be done. And again, I want to say that I don't—I have not heard of another company, American or not, allowed for this to happen.

Mr. OBERNOLTE. I mean, you are kind of at a unique position, having to answer these concerns of Congress.

So are they going through the code for just the app, or the app and the server code?

Mr. CHEW. I can get back to you on the——

Mr. OBERNOLTE. OK.

Mr. CHEW [continuing]. On the technical details.

Mr. OBERNOLTE. Well——

Mr. CHEW. But it is comprehensive, including the software that powers the—a lot of the software that powers the experience.

Mr. OBERNOLTE. And how long will that review take?

Mr. CHEW. I need to get back to you on the timeline, but we are progressing quite well on Project Texas, and whenever we hit a milestone I commit to be very transparent about it.

Mr. OBERNOLTE. OK. So I am wondering, because I am also concerned, as a software engineer, about the process in which new code is introduced into the code base. Do you use a software configuration management system at TikTok?

Mr. CHEW. The way we plan for new code to be done is that, even before the code becomes live, it has to be reviewed. The changes have to be reviewed by the——

Mr. OBERNOLTE. OK, so you are talking about——

Mr. CHEW [continuing]. Third-party monitor.

Mr. OBERNOLTE [continuing]. A code review. That was good. That was another question I had for you. So the code review, is it done with a team of engineers or just with a single engineer?

Mr. CHEW. Oh, it is going to be a team effort.

Mr. OBERNOLTE. OK.

Mr. CHEW. Yes.

Mr. OBERNOLTE. And that is going to be done at Oracle or elsewhere?

Mr. CHEW. It is going to be done in one of our transparency centers, so that we—you know, we still need to make sure that the code itself is secure, and, you know, so——

Mr. OBERNOLTE. OK, so——

Mr. CHEW. Yes.

Mr. OBERNOLTE. What I am hearing you say is that, even though the code might be written by someone not in the United States, before the code is integrated it will be reviewed in a code review by a team of engineers within the United States?

Mr. CHEW. That is the plan.

Mr. OBERNOLTE. OK. And then back to the question about the software configuration management system. How do you manage the integration of that code change into the rest of the TikTok code base?

Mr. CHEW. The long and short of it is we have built a team of American personnel with security credentials. The person who leads the team used to work for the Secret——

Mr. OBERNOLTE. No, no, I understand, but, I mean, there is a software solution for integrating those code changes into the code base. What solution is that?

Mr. CHEW. I would need to check——

Mr. OBERNOLTE. Is it a commercial one?

Mr. CHEW [continuing]. And get back to you on the details.

Mr. OBERNOLTE. OK.

Mr. CHEW. Yes.

Mr. OBERNOLTE. Well, specifically, what I would like to know is to make sure that this isn't something that TikTok has created custom, which many companies do, because that would mean that you would have to review the source code for that, as well——

Mr. CHEW. Yes.

Mr. OBERNOLTE [continuing]. For security.

How do you protect against threats like the—a malicious actor being hired not by TikTok but by Oracle, for example, or by USDS?

Mr. CHEW. The approach that most companies take for these things is to have several layers of monitoring to make sure that everything that somebody has reviewed, there is a secondary review so that one malicious actor is not able to create the damage that the malicious actor can do.

But you rightly pointed out these kind of problems are industry-wide problems.

Mr. OBERNOLTE. Right.

Mr. CHEW. Every company has to deal with them.

Mr. OBERNOLTE. OK. Well, let me ask a specific question about that. I mean, I—in thinking about—if I were a malicious actor, a software engineer on one of your projects, how I would go about writing a malicious code, I wouldn't put it right there and say, "Hey, I am malicious." I would put unrelated lines of code in different sections of the code that work together to do something malicious. How do you think that that could get caught?

Mr. CHEW. Again, you know, we have to rely on third-party experts to help us with that. I think there are enough experts who can catch a lot of these things. The work on security globally, on all data security, is never perfect.

Mr. OBERNOLTE. Yes, I understand.

Mr. CHEW. But we can have a lot of oversight to keep it safer than any other experience.

Mr. OBERNOLTE. I appreciate the effort. My concern, Mr. Chew, is I don't believe that it is technically possible to accomplish what TikTok says it will accomplish through Project Texas. I just think that there are too many backdoors through that process to allow that to be possible, and I think a malicious actor would succeed in inserting malicious code in there if they wanted to. But I hope we—I see we are out of time. I hope we get an opportunity to talk some more about this.

I yield back, Madam Chair.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentlelady from Michigan, Mrs. Dingell, for 5 minutes.

Mrs. DINGELL. Thank you, Chairman Rodgers and Ranking Member Pallone, for holding this hearing, and to Mr. Chew for testifying here today. Your good news: You are halfway through with me.

As screen time increases, so do inherent risks. And with the proliferation and popularity of new social media platforms, so does the potential reach of dangerous, provocative, and often harmful content and, my fear, the abuse of collected data.

As a representative from the State of Michigan, I can speak from experience on how social media has been used to target members of the Michigan delegation, including a plot to kidnap our Governor, and how it can be weaponized to perpetuate harms towards

individuals and communities, and you saw firsthand how it targeted the Chair of this committee.

Today many of my colleagues on both sides of the aisle have raised legitimate concerns about protecting children online, misinformation, and securing our data, concerns that I share and, as has been said by many of my colleagues, are bipartisanly shared. I think, in many ways, these myriad of issues highlight the need for comprehensive data privacy legislation that would ensure the safety and integrity of every American's data on every social media platform and mitigate potential harms.

One important area of concern I have regarding data collection is geolocation data and how it can be abused. I have seen it abused. I have seen women die because it has been abused. This subject has dangerous implications for survivors of domestic violence, people seeking medical care, and protecting children from potential predators.

Mr. Chew, in your testimony you wrote that current versions of the app do not collect precise or approximate GPS information from U.S. users. Yes or no answers, please: Mr. Chew, have any prior versions of TikTok's app collected precise GPS information from U.S. users? Yes or no.

Mr. CHEW. Yes, from back in 2020, about 3 years ago.

Mrs. DINGELL. Are there currently TikTok users who still hold old versions of the app that collect precise GPS information from U.S. users? Yes or no.

Mr. CHEW. There could be, but that is a small percentage today.

Mrs. DINGELL. Still dangerous. Has TikTok at any time fed precise GPS information collected from U.S. users into algorithms to serve user ads? Yes or no.

Mr. CHEW. I will need to check on the details, because we do not currently collect that. So I need to check on the details.

Mrs. DINGELL. Yes, I am sure there is a yes there. But has TikTok at any time fed precise GPS information collected from U.S. users into algorithms—I am having—talk today—to make inferences about users? Yes or no.

Mr. CHEW. I am not sure of the specifics. I——

Mrs. DINGELL. I would like answers, yes or no, after this. Has TikTok at any time sold precise GPS information collected from U.S. users? Yes or no.

Mr. CHEW. We do not sell data to data brokers, if that is the question.

Mrs. DINGELL. That—and you have never done that?

Mr. CHEW. I do not believe so.

Mrs. DINGELL. Has TikTok at any time sold or shared with third parties algorithmic inferences that were made using, in part or in whole, precise GPS information collected from U.S. users, yes or no?

Mr. CHEW. Congresswoman, I need to check on these specifics. What I can tell you is right now we do not collect precise GPS location data in the United States.

Mrs. DINGELL. All right. Does TikTok still use inferences that were made using, in part or in whole, precise GPS information collected from U.S. users?

Mr. CHEW. I am sorry. Would you repeat that?

Mrs. DINGELL. Does TikTok still use inferences that you have gained that were made using, in part in—or whole, precise GPS information collected from U.S. users in your algorithms?

Mr. CHEW. That will be a very technical question. I would have to check and get back to you.

Mrs. DINGELL. Has TikTok at any time provided the Chinese Government with either precise GSP information collected from U.S. users or inferences made from that data?

Mr. CHEW. That I can give you a straight—no.

Mrs. DINGELL. Mr. Chew, even in Congress—even if Congress were to ban TikTok, I am concerned that China or others would still have access to U.S. consumer data by purchasing it through data brokers. Will you commit not to sell any of TikTok's data to data brokers now or in the future?

Mr. CHEW. We do not do that. We do not sell data to data brokers now.

Mrs. DINGELL. Will you commit to not do it in the future?

Mr. CHEW. This is a—there are certain members of our industry who do this. You know, I think this has to be broad legislation to help us, the whole industry, address this problem.

Mrs. DINGELL. I think I am out of time.

Thank you, Madam Chair. I will yield back.

Mrs. RODGERS. The gentlelady yields back. The Chair yields 5 minutes to the gentleman from Alabama, Mr. Palmer.

Mr. PALMER. Thank you.

When the Chinese Communist government bought a share of ByteDance, it has been described as the Chinese Communist government's way of quieter form of control. And the companies have little choice in selling a stake to the government if they want to stay in business.

And what I would like to know is when the Chinese Communist government moved to buy shares of ByteDance, were you informed beforehand? Yes or no.

Mr. CHEW. No. Congressman——

Mr. PALMER. OK.

Mr. CHEW. ByteDance——

Mr. PALMER. Were——

Mr. CHEW [continuing]. Hasn't——

Mr. PALMER. Were you or anyone with TikTok asked for your opinion about the sale of shares of ByteDance to the Chinese Communist government? Yes or no.

Mr. CHEW. It just—this hasn't happened.

Mr. PALMER. Did you or anyone employed by or affiliated with TikTok state any objections or concerns about the possibility of the Chinese Communist government, once they had shares in ByteDance, exercising control over content, using your platform for conducting misinformation campaigns, or restrictions ensuring nothing is posted that reflects badly on the Chinese Communist government, or for surveillance and data collection for use against anyone?

Did any of your—you or anyone affiliated with TikTok raise any concerns about that?

Mr. CHEW. Congressman, we do not collect—we do not promote——

Mr. PALMER. I didn't ask you that.
Mr. CHEW. We do not promote——
Mr. PALMER. Yes or no, did you raise any concerns about it? Because that is why we are here.
Mr. CHEW. But we do not promote or remove any content on——
Mr. PALMER. I didn't ask you that.
Mr. CHEW [continuing]. The behalf of the Chinese Government.
Mr. PALMER. Did you communicate in any form or fashion with the directors of ByteDance that there might be concerns about government control over content? Yes or no, did—you either did or you didn't.
Mr. CHEW. Congressman, I——
Mr. PALMER. You didn't.
Mr. CHEW. I just want to make this clear. We do not remove——
Mr. PALMER. Let me ask you this.
Mr. CHEW [continuing]. Or promote content at the request of the Chinese Government.
Mr. PALMER. TikTok insiders have already said that the company is tightly controlled by ByteDance. It even gets down to the hours they work. So obviously, you didn't say anything. There is a serious concern by Chinese companies, privately held companies, about doing anything against what the Chinese Communist government wants.
I want to ask you this: Does TikTok screen against manipulative content from child predators? Yes or no.
Mr. CHEW. Do we screen against——
Mr. PALMER. Do you screen against them——
Mr. CHEW. Yes, we do this——
Mr. PALMER. How about——
Mr. CHEW [continuing]. Child predator——
Mr. PALMER. How about drug cartels?
Mr. CHEW. Drug cartels, child predatory content, this is all violative——
Mr. PALMER. You had a drug cartel that was engaged in a police chase with Spanish authorities, and they posted it on TikTok and got over a million views. Why wasn't that taken down? And are you doing it with human traffickers or terrorists?
I mean, do you withhold content from nations that might be committing crimes against humanity? Yes or no.
Mr. CHEW. Congressman, our platform is a place of——
Mr. PALMER. Yes or no?
Mr. CHEW [continuing]. Freedom of expression. And users come here, and——
Mr. PALMER. Yes or no? I know, you talk about that. But yes or no, do you screen against content from nations that commit crimes against humanity?
Mr. CHEW. Congressman, our users come and——
Mr. PALMER. Yes or no?
Mr. CHEW. Our users come and——
Mr. PALMER. Yes or no?
Mr. CHEW [continuing]. Present any points of views that they want, and——
Mr. PALMER. You don't.
Mr. CHEW. And it is a commitment to keep this free from——

Mr. PALMER. Let me ask you this. Michael Beckerman, who is your vice president and head of public policy for the Americas, right? Is he part of the team that helped you prepare for this meeting? Yes or no.

Mr. CHEW. Can I clarify who you mean?

Mr. PALMER. Michael Beckerman?

Mr. CHEW. Yes, he is.

Mr. PALMER. OK. Where is he at this moment?

Mr. CHEW. I am sorry?

Mr. PALMER. Where is Mr. Beckerman at this moment?

Mr. CHEW. He is probably here.

Mr. PALMER. No, you know he is here. He is sitting right behind you. I want to know why, when Mr. Beckerman was on with Jake Tapper on CNN and asked repeatedly to condemn Chinese Communist government's treatment of the Uyghurs when that treatment has been classified by the United States as a genocide, when a UN report classifies it as a crime against humanity, why after multiple questions Mr. Beckerman refused to address that. Are you afraid of the Chinese Communist government?

Mr. CHEW. No, because you——

Mr. PALMER. Are you concerned that——

Mr. CHEW [continuing]. Can find that content on our platform. Any content that our users want to express their views on this issue——

Mr. PALMER. Well, why couldn't your——

Mr. CHEW [continuing]. Is freely available on our platform.

Mr. PALMER [continuing]. Vice president of public policy, the guy who is head of public policy for the Americas, and an American on an American television news channel, why couldn't he say—why couldn't he condemn that?

Mr. CHEW. I think it is very important to look at our platform. And if you use our—and open our app, and search for any content——

Mr. PALMER. I am not talking about your platform. I am asking about your personnel now, because personnel is policy. Everybody in this room understands that, except maybe you. Personnel is—let me just conclude with this. And I hate to bring this up, because I—this is part of the stuff that I have studied. But deception is fundamental to the Chinese Communist Party's political intelligence and military strategy. And you have repeatedly used the word "transparency" throughout this hearing. And every time you have said it, what I have heard is deception.

And I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentleman from Texas, Mr. Veasey, for 5 minutes.

Mr. VEASEY. Thank you, Madam Chair. I got to tell you, Mr. Chew, as a father of a 16-year-old that likes social media, the—a lot of your evasiveness today in answering many of these questions really disturbs me, because I can tell you that the teenagers of today, they really don't want to be on Facebook. They want—they want your platform. And you were asked to come before this committee to testify about many things, and a lot of us are worried about our kids' personal data.

As the cochair of the Congressional Voting Rights Caucus, I also worry that TikTok is the world's most powerful and extensive propaganda machine, allowing the Chinese Communist Party to use TikTok's platform to influence public opinion and undermine the integrity of our democratic elections.

And I have a report called "TikTok and Facebook Failed to Detect Election Disinformation in the U.S., While YouTube Succeeds." And this report was published by the nonprofit Global Witness and the Cybersecurity for Democracy Team at NYU. And the purpose of the study was to test platforms like TikTok and whether or not they can detect and take down false political ads targeted at U.S. voters, young voters, ahead of last year's midterm elections. And according to this report, 90 percent of election disinformation ads tested were approved by your platform.

Again, that is 90 percent of ads containing false and misleading election misinformation went undetected on TikTok. And just to add some color to the type of misleading ads that were approved by TikTok, this included ads that were live on TikTok that said the wrong election day and actually encouraged people to vote twice.

You do know that voting twice is a felony. Mr. Chew, you do know that it is illegal to vote twice.

Mr. CHEW. Congressman, any misinformation that comes around a political action——

Mr. VEASEY. OK.

Mr. CHEW [continuing]. Is something we take very seriously.

Mr. VEASEY. Let me—I am particularly troubled about this type of information, because it can run rampant on TikTok. And given that TikTok—again, you all are appealing to a very young and diverse user base. That is exactly the people that we have seen targeted time and time again with voter suppression campaigns run by malicious actors.

Mr. Chew, do you agree with me that is—that it is completely unacceptable that 90 percent of these ads were undetected on your platform?

And can you detail for us right now TikTok's policy regarding election misinformation and paid political ads, and how the company monitors such information, and how you plan to get that number down to zero?

Mr. CHEW. Well, TikTok is a place for our users to come and express their points of views freely. We do take misinformation, dangerous misinformation particularly around an election, very seriously. And we will work with third-party experts to identify misinformation——

Mr. VEASEY. Do you call allowing 90 percent of false content, political content on your platform, to be taken—you call that—you define that as being taken seriously?

Mr. CHEW. I need to look into the specifics. I am, you know, not sure where the number came from, but I can tell you, Congressman, that we are the only platform that I know of that doesn't actually take political ads. We don't accept money. I don't think other platforms can say that.

Mr. VEASEY. Mr. Chew, can you detail how you responded to that report? Did you respond to that report that I just mentioned?

Mr. CHEW. I need to look at the specifics of the report, Congressman, and I can get back to you on that.

Mr. VEASEY. All right, Mr. Chew, I want to shift to Project Texas.

I know that we have discussed this initiative throughout today's hearing, but I want to dive deeper into your notion that promises about Project Texas should give us any confidence in TikTok's ability to localize U.S. data and discontinue access to that data to ByteDance employees in China.

Why? Because we have already had a TikTok executive appear before Congress and give sworn testimony about the comfort that we should take in TikTok's U.S.-based resources. Well, TikTok data security practices were being scrutinized by the U.S. Government—and unfortunately, we have since found out from a—from journalists and recorded conversations that those assurances were worthless.

In your testimony you also mentioned that Oracle has already begun inspecting TikTok's source code and has access to the platform's recommendation algorithm. Why should this give the American public any great assurances, particularly given that Oracle now owns a stake in TikTok and stands to gain monetarily, the more revenue that TikTok and its algorithm generates?

Mr. CHEW. Congressman, not only is Project Texas unprecedented in our industry in protecting U.S. user data and interests, we are inviting third parties to come in and monitor this. And we will, you know, be transparent in that process. And this is more—beyond most—all companies that I know of in my industry——

Mr. VEASEY. Thank you, Madam Chair. I am out of time.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentleman from Florida for 5 minutes, Mr. Dunn.

Mr. DUNN. Thank you very much, Madam Chair.

Mr. Chew, I am aware that on arriving in DC this week you appeared on TikTok and boasted you had 150 million U.S. users, 5 million U.S. businesses. That represents a lot of data. You also referenced your appearance before this committee as a chance to share all that TikTok is doing to protect Americans using the app.

Mr. Chew, has ByteDance spied on Americans at the direction of the Chinese Communist Party?

Mr. CHEW. No.

Mr. DUNN. Madam Chair, I would like to enter into the record this October 2022 Forbes article entitled "TikTok Parent ByteDance Planned To Use TikTok to Monitor the Physical Location of Specific U.S. Citizens."

Mrs. RODGERS. Without objection, so ordered.

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

Mr. DUNN. Thank you. The project assigned this to a Beijing-led team, and they were going to follow individual American citizens.

I ask you again, Mr. Chew, has ByteDance spied on American citizens?

Mr. CHEW. I don't think that spying is the right way to describe it. This is ultimately——

Mr. DUNN. We can differ on that.

Mr. CHEW. This is, ultimately, an internal investigation——

Mr. DUNN. Any TikTok or ByteDance data that is viewed, stored, or passes through China is subject to the laws of China, a one-

party, authoritarian state hostile to all American standards of privacy.

China's court system reports to and falls under the Chinese Communist Party. And like fentanyl analogues, which we all know are also manufactured in China, although they are illegal there, I fear TikTok will grow into a much bigger problem—a cancer, if you will. And I am deeply worried that it may be too late to stop the spread of this cancer. Like fentanyl, another China export which causes addiction and death, dangerous algorithms and the Chinese Communist Party are not good for Americans, not good for our families, and definitely not good for the United States.

Mr. Chew, prior to serving as the CFO of ByteDance, you served as a CFO and director of global operations for Xiaomi from 2015 to 2021. Is that correct?

Mr. CHEW. Are you asking me in 2015?

Mr. DUNN. Very good——

Mr. CHEW. Would you mind repeating that, please?

Mr. DUNN. Madam Chair, I would like to enter another article into evidence. This is from the National Cyber Security Centre in Lithuania.

Mrs. RODGERS. Without objection, so ordered.[1]

Mr. DUNN. Thank you. This report outlines numerous data security risks, including how the privacy of European users was violated in clear cases of unauthorized collection of user data by Xiaomi. This sounds exactly—what many of my colleagues have been talking about today.

Worse yet, the Xiaomi phones sold to Europeans had a list of 449 words and phrases which would be automatically censored on the device. Censored phrases included "the Voice of America" and "democratic movement," among others. This analysis was conducted on devices which were manufactured and sold to Europeans while you were the head of operations for Xiaomi.

It does not follow that you expect us to believe that you would not censor on behalf of the Chinese Communist Party, since you have already done so.

Mr. CHEW. I want to be unequivocal on this. We do not remove or promote content on behalf of——

Mr. DUNN. I reclaim my time.

Mr. CHEW [continuing]. The Chinese Government.

Mr. DUNN. While TikTok, in your words, strives to deliver on their "mission to inspire creativity and bring joy" to American users, I assure you that is not the mission or goal of the Chinese Communist Party, which runs the People's Republic of China, that TikTok's parent company, ByteDance, is domiciled in.

Mr. Chew——

Mr. CHEW. Congressman, you can check with our users——

Mr. DUNN [continuing]. Straightforward——

Mr. CHEW [continuing]. To see the experience that they are getting.

Mr. DUNN [continuing]. Answer. You have not given straightforward answers. We don't find you credible on these things.

[1] The information has been retained in committee files and is included in the Documents for the Record at https://docs.house.gov/meetings/IF/IF00/20230323/115519/HHRG-118-IF00-20230323-SD030.pdf.

And with that, Madam Chair, I would like to yield the balance——

Mr. CHEW. Congressman, you have given me no time to answer your questions.

Mr. DUNN [continuing]. To Congressman Obernolte of California.

Mr. CHEW. I reject the characterizations.

Mr. DUNN. I yielded to Mr.——

Mrs. RODGERS. Who are you yielding to?

Mr. DUNN [continuing]. Obernolte.

Mrs. RODGERS. Dr. Dunn, Mr. Obernolte?

Mr. DUNN. Yes.

Mrs. RODGERS. OK.

Mr. OBERNOLTE. Well, thank you, Madam Chair.

Mr. Chew, I would like to continue our discussion of Project Texas, if we could.

Part of Project Texas is that engineers at Oracle will review the algorithms used by TikTok to confirm that they are free of foreign influence. I have a question about that, because we are talking about AI. That is a very generic term. Do you use machine learning to influence the algorithms at TikTok?

Mr. CHEW. This gets very technical, and we have published several blogs about this, which I can forward to your team.

Mr. OBERNOLTE. OK.

Mr. CHEW. But yes, it is mainly based on interest signals.

Mr. OBERNOLTE. Right, OK.

Mr. CHEW. Yes.

Mr. OBERNOLTE. So here is my question: How could looking at the algorithm confirm that it is for—free from foreign influence? Because the algorithm is just a neural net architecture with inputs and outputs and weights, and how to train that.

I mean, the influence is an external factor. So I would appreciate it if you could give us—I see we are out of time again—a written answer to that.

But again, I am concerned that what you are proposing with Project Texas just doesn't have the technical capability of providing us the assurances that we need.

I yield back, Madam Chair.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes Ms. Kuster.

Ms. Kuster is not here. Ms. Barragán for 5 minutes.

Ms. BARRAGÁN. Thank you, Madam Chair.

Mr. Chew, TikTok warns users when content is graphic or disturbing and labels state-affiliated media accounts to ensure the viewers aren't seeing propaganda. Does TikTok provide similar information to Spanish speakers—users, as well as English speakers?

Mr. CHEW. I believe so, Congresswoman. I will get back to you on that.

Ms. BARRAGÁN. OK. And do you know if TikTok has a specific strategy for tackling Spanish-language content that violates its trust and safety guidelines?

Mr. CHEW. We do. I will get back to you on the specifics on that.

Ms. BARRAGÁN. OK. When offensive English-language search terms or hashtags are blocked for violating community guidelines

in English, is the Spanish translation of the term or the hashtag automatically blocked, as well?

Mr. CHEW. I believe so, but let me check the specifics and get back to you.

Ms. BARRAGÁN. Do you have any idea how many people that you might have working at TikTok that addresses Spanish misinformation?

Mr. CHEW. I know ballpark. It is quite a significant team, but I can get back to you on the details.

Ms. BARRAGÁN. You said significant. So are you saying it is—do you have a ballpark at all you can give us? Would you say it is like 10 percent of your force, or more than——

Mr. CHEW. It is an important number, so I want to be precise, and I will get back to you.

Ms. BARRAGÁN. OK. Do you happen to know how TikTok—how—if TikTok can effectively ensure that Spanish-speaking users between the ages of 13 and 17 are not being targeted by ads promoting harmful content?

Mr. CHEW. We have very strict policies for our users who are in the teenage age group, and regardless of what language that they speak. So we want to make sure that they are given a very safe experience on our platform, regardless of the language they——

Ms. BARRAGÁN. Well, I know. I am just trying to—I am trying to ascertain resources you may be putting into Spanish-speaking—Spanish language.

Last year the Congressional Hispanic Caucus met with TikTok. This was one of the conversations, and a source of the discussion was addressing Spanish-language disinformation and misinformation. It remains an urgent priority for the Congressional Hispanic Caucus, as Hispanics across the country increasingly turn to social media for vital information.

We heard earlier in this hearing that there was, you know, video—there was a TikTok post threatening the Chair of the committee, and it took some 40 days to take it down. So I guess I am a little concerned if you—if your team doesn't have the resources and the capability to flag that, what kind of capability is it going to have to bring down misinformation, disinformation to Spanish speakers, which I am assuming is a smaller fraction of the workers that you have at TikTok?

Mr. CHEW. TikTok is a place for, you know, all our users to come and express their very diverse views. And, you know, we are open to all ethnicities, you know, and we are open to all, everyone to come here and express their—freely express their views.

So it is our commitment to make sure that the safety of those users, regardless of the language, you know—and of course, you know, the Spanish-language user base is super important to us.

Ms. BARRAGÁN. OK, so you can't——

Mr. CHEW. So we need to make sure that we continue to invest in that——

Ms. BARRAGÁN. OK, so you don't—you don't have an answer, then. OK. I will look forward in your coming—your coming back.

We have heard a lot about the concerns about children who may be on TikTok. Mr. Chew, at what age do you think it would be appropriate for a young person to get on TikTok?

Mr. CHEW. We have three different experiences here in the United States. There is an experience for under 13s, which is highly, highly restricted.

Ms. BARRAGÁN. I am asking what—I am asking what you think would be the appropriate age to have a child get on TikTok.

Mr. CHEW. Our approach is to give differentiated experiences for different age groups and let the parents have these conversations with their children to decide what is best for their family.

Ms. BARRAGÁN. So you think that there is a sufficient safety mechanism for an 8-year-old to be able to access TikTok?

Mr. CHEW. An 8-year-old's experience on TikTok would be so highly restricted that every single piece of content he or she will see will be vetted by common sense, our third-party child safety expert, and the 8-year-old would not be able to post, and the 8-year-old would not be able to see any personalized feed, and zero advertising in that experience. So I believe, yes, it is the appropriate experience for an 8-year-old.

Ms. BARRAGÁN. Well, then why don't you let your 8-year-old child on TikTok?

Mr. CHEW. I have seen these news articles. I would like to address that. My kids live in Singapore. And in Singapore we do not have the under-13 experience. If they lived here in the United States, I would let them use the under-13 experience.

Ms. BARRAGÁN. OK. So you are saying it is because of the country you live in doesn't have the same mechanisms. Is there a reason you don't have those same mechanisms everywhere?

Mr. CHEW. In principle, we want to provide, you know, a good experience for our users in general. We don't want to monetize from people who are under 13. In the U.S. we are COPPA compliant, and as part of that we will deem as a—I want to get the specifics right. We will deem as a particular type of audience—mixed audience app. We want to make sure that that is right. And as a result of that, we have to provide an experience to our under-13 users in this country, as well.

Ms. BARRAGÁN. My time has expired. Thank you.

I yield back.

Mrs. RODGERS. The gentlelady yields back. The Chair recognizes the gentleman from Utah, Mr. Curtis.

Mr. CURTIS. Thank you, Madam Chair.

Mr. Chew, my children are getting ready to run a marathon. And I know that during this hearing that they will be running for about the same amount of time that you will be sitting in that chair today. Unfortunately, I only get you for 5 minutes. So instead of a marathon, I would like to do a sprint with you. And I want to go back up to that 30,000-feet level.

Would you agree with me that section 230 was created to protect platforms like yours from lawsuits when you distribute information?

Mr. CHEW. I——

Mr. CURTIS. Don't overcomplicate it. Just, like, 30,000 feet.

Mr. CHEW. I understand.

Mr. CURTIS. Yes.

Mr. CHEW. Yes.

Mr. CURTIS. So then would you agree that there is a line drawn between publishers of information and distributors of information in——

Mr. CHEW. I——

Mr. CURTIS. Specifically in the section 230 language.

Mr. CHEW. I think 230 is a very complex topic.

Mr. CURTIS. Yes, I understand. But remember, we are at 30,000 feet. So in short, your platform distributes content that other peoples publish.

One of the early challengers to section 230 was when AOL refused to take down a post of somebody that had inappropriately put a phone number—associated a phone number with the Oklahoma City bombings. The courts ruled that AOL was not liable for that post because of section 230.

Now, I want you to do a hypothetical with me, because I am going to use the absurd to try to make a point here. Let's suppose, hypothetically, that AOL, instead of just posting that, actually wanted to magnify that voice, and so they took out an ad in the Wall Street Journal linking that phone number with the Oklahoma City bombing. And let's suppose they didn't stop there, but they went further and they took out a Super Bowl ad linking that phone number with the Oklahoma City bombing. And let's suppose, hypothetically, they didn't stop there, they sent a flier to every home in America linking that phone number to the bombing.

And I guess the question is, would AOL have moved from a distributor to a publisher in this made-up example?

Mr. CHEW. Congressman, respectfully, I——

Mr. CURTIS. I think everybody can see that they would. This is not a hard question. Moving that far away from the intent would have moved them to a publisher.

So my question is—platforms are protected because they post content. But I want this room to see—not just you—that protection has limits. And if AOL moves to a distributor instead of a publisher, they go outside of those limits.

Now let's talk algorithms just super quickly. We have thrown that word around a lot today. Let me here again go 30,000 feet, and we will use another platform so it is not sensitive. But Pinterest, I like to go on Pinterest. My home—my wife and I are building a home. I am working on the yard right now. If you went on my Pinterest page, you would see swing sets and things made for my grandkids.

Now, another hypothetical. Let's suppose there is some devious intent inside Pinterest, and they decide they want to influence John Curtis with these algorithms, and they want me to believe it is the end of the world. And all of a sudden now I am buying bomb shelters instead of swing sets for my kids. Have they become a publisher? And should that be protected from section 230?

And if you don't feel—I am pretty sure the room understands that they have crossed this line, and you can tell me if you think they have or not.

Mr. CHEW. Congressman, I will have to study that specific example and get back to you.

Mr. CURTIS. It is a hypothetical, but you can see the—at some point they have crossed a line, and they have become a publisher and a distributor.

So we have touched on this today, but I want to be super specific. Is it possible that TikTok had enough data—could get enough data on me that you could use artificial intelligence and your algorithms and machine learning to write an algorithm that could persuade me to change how I view a policy issue? Does that possibility exist?

Mr. CHEW. The way we look at it——

Mr. CURTIS. Thirty-thousand feet. We are on the sprint.

Mr. CHEW. I will stay very high level.

Mr. CURTIS. OK, please.

Mr. CHEW. The way we look at it is our users come in and express whatever views they want.

Mr. CURTIS. But that is not the point. The point is you could write an algorithm that would change. And we have actually seen—the Washington Post reported the Stop the Willow campaign shows how TikTokers are tackling climate change. I think that is all fine, right, and all good, unless somebody has interjected into that and magnified or diminished voices in that. And what I am proposing to you today is that that pushes them across the line from a distributor to a publisher if they make those decisions.

Now, serious allegations have been made against your platform and others, many of them here today. And you are not new to these, right, to these allegations. This isn't your platform, but some time ago there was an allegation that a platform recommended ISIS-related videos. We have talked about the weight loss videos, we have talked about—we didn't talk about it, but the stealing the elections. Whatever the motivation, I am trying to point out that as you move from a publisher, you manipulate this data with algorithms, that you step out from the protections of section 230. Do you see that logic?

Mr. CHEW. This is a very complex——

Mr. CURTIS. I understand it is very complex.

Mr. CHEW. Yes.

Mr. CURTIS. But you see the logic. In your mind, has TikTok ever stepped across the line from a distributor to a publisher?

Mr. CHEW. Congressman, again, this is a very complex topic. I would need to get back to you on——

Mr. CURTIS. I understand that. OK.

And finally, very quickly, you produced a video that now is well known about your visit here today in Washington, DC. Can you tell me 100 percent that no TikTok employees manually manipulated that to get more views?

Mr. CHEW. I checked. And as far as I know, there was no boosting and heating. I went viral organically.

Mr. CURTIS. OK. Madam Chair, I am sorry, I am out of time. I yield my time.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes Ms. Blunt Rochester for 5 minutes.

Ms. BLUNT ROCHESTER. Thank you, Madam Chair.

Mr. Chew, as I am sure you know, this hearing is part of an ongoing effort by our committee to examine data security and other concerns with social media companies broadly. And I have to tell

you, I came to this hearing interested to hear the actions that TikTok is taking to combat misinformation, protect our young people, and ensure our national security. But I have not been reassured by anything you have said so far. And I think, quite frankly, your testimony has raised more questions for me than answers.

As some of my colleagues already noted, platforms like TikTok can easily manipulate and undermine user autonomy with addictive features, invasive data collection practices, and disseminating misinformation and disinformation. That is why I will be reintroducing the DETOUR Act to mitigate this harm.

Mr. Chew, 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. CHEW. In principle——

Ms. BLUNT ROCHESTER. It is just a yes or no.

Mr. CHEW. In principle, I agree that the kind of practices is not——

Ms. BLUNT ROCHESTER. And can TikTok users opt out of targeted ads, yes or no?

Mr. CHEW. At this moment in time, we believe that this is a very important part of the experience——

Ms. BLUNT ROCHESTER. Yes or no? Time is ticking.

Mr. CHEW. It is an important part of the experience.

Ms. BLUNT ROCHESTER. If—even if someone wants targeted ads, do you give a user a clear opportunity to prevent TikTok from using tools like pixels to collect their data and track them off of the TikTok platform?

Mr. CHEW. We give our users a lot of tools to control their privacy settings on our app.

And by the way, if you are below 16, it is private by default. So you cannot even go viral.

Ms. BLUNT ROCHESTER. An August of 2022 response to a letter I wrote to your company on abortion misinformation, TikTok asserted several actions to address abortion misinformation. In light of recent attacks on safe and effective medication abortion, I am—remained worried by this misinformation.

And following on Ms. DeGette's questioning, how many posts did you actually take down that contained abortion misinformation?

Mr. CHEW. Contents and views on both sides of the—on abortion is allowed on our platform. It is just freedom of expression. If it is dangerous misinformation, we rely on third-party experts to help us identify and remove them. I can get back to you on specifics.

Ms. BLUNT ROCHESTER. Yes, please get back with us——

Mr. CHEW. Yes.

Ms. BLUNT ROCHESTER [continuing]. On the specifics.

Mr. Chew, in your testimony you indicated TikTok has taken several steps to implement Project Texas. You have said you have spent—in your testimony—$1.5 billion, you have hired 1,500 full-time employees. Can I ask for some specifics about the implementation? This $1.5 billion, what was it used for? The employees, were they people that you already had that you just transferred over? And what types of roles will they have?

Mr. CHEW. Oh, OK. This billion and a half U.S. dollars is spread across many things, including the infrastructure we have to build,

the migration of the data to a new cloud infrastructure, and all the third-party security partners that we are hiring, and, of course, the new employees.

Now, this team will now be run by a gentleman who used to be the—who has spent his career as a chief security officer in other companies, and another gentleman who used to work, I believe, in——

Ms. BLUNT ROCHESTER. If you could just follow up——

Mr. CHEW. Yes.

Ms. BLUNT ROCHESTER [continuing]. With us, that would be very helpful.

Mr. CHEW. I will, I will.

Ms. BLUNT ROCHESTER. Because we would really like to understand the details. Where is the money going? How many people are—and what will they be doing?

Mr. CHEW. OK.

Ms. BLUNT ROCHESTER. You know, as I put just kind of a finer point on this, one of my concerns is that we came here hoping to hear some actions that would alleviate some of our concerns and our fears. We have got family members, we have a lot of folks here that are constituents, that are content creators. And for us, we were looking for action. We wanted to see—make us feel like we really can trust, as you use the word.

What I leave here with is thinking about the fact that your company is—I learned that you are—you have personalized data advertising for kids as young as 13. And we have heard until Project Texas is supposedly stood up, engineers in China still have access to personal data, and that—that means engineers in China have access to personal data of 13-year-olds in the United States. And I think that really summarizes why you see so much bipartisan consensus and concern about your company. And I imagine that it is not going away any time soon.

Thank you, Madam Chair, and I yield back.

Mrs. RODGERS. The gentlelady yields back. I yield to the lady from Arizona, Mrs. Lesko, for 5 minutes.

Mrs. LESKO. Thank you, Madam Chair.

Mr. Chew, do you agree that the Chinese Government has persecuted the Uyghur population?

Mr. CHEW. Congresswoman, you—if you use our app and you open it, you will find our users who give all sorts of content——

Mrs. LESKO. That is not my question. My question is, do you agree that the Chinese Government has persecuted the Uyghur population?

Mr. CHEW. Well, it is deeply concerning to hear about all accounts of human rights abuse. My role here is to explain——

Mrs. LESKO. I think you are being pretty evasive.

Mr. CHEW [continuing]. What our platform does on this.

Mrs. LESKO. It is a pretty easy question. Do you agree that the Chinese Government has persecuted the Uyghur population?

Mr. CHEW. Congresswoman, I am here to describe TikTok, and what we do as a platform. And as a platform——

Mrs. LESKO. All right.

Mr. CHEW [continuing]. We allow our users to freely express their views——

Mrs. LESKO. All right. Earlier today——

Mr. CHEW [continuing]. On this issue and any other issue that matters to them.

Mrs. LESKO. Well, you didn't answer the question.

Earlier today Chairman Rodgers asked you, and I quote, "Have any moderation tools been used to remove content associated with the Uyghur genocide, yes or no?" Your answer, "We do not remove that kind of content." Yet in 2019 TikTok suspended the account of Feroza Aziz, an American 17-year-old, after she put out a video about the Uyghur genocide. So your answer, sir, does not align with history.

Mr. CHEW. That particular case was a mismoderation. I believe that video had a picture of Osama bin Laden, so we thought it was——

Mrs. LESKO. No, I——

Mr. CHEW [continuing]. Content that was inappropriate.

Mrs. LESKO. Yes, I looked it up. That was a different post that they banned, TikTok banned.

Mr. CHEW. I can get back on the specifics, yes.

Mrs. LESKO. My next question. India banned the use of TikTok in their country in 2020. New Zealand has banned the installation of TikTok on devices connected to the country's parliamentary network. Canada banned the installation of TikTok on government devices. The United Kingdom has banned the TikTok app from government-owned devices. Belgium banned the TikTok from government phones. The European Union banned the installation of TikTok on government devices. All cited security risks with the company's data collection and connection to the Chinese Communist Party.

Recently, our U.S. FBI Director, Christopher Wray, said about TikTok, "This is a tool that is ultimately within the control of the Chinese Government. And it—to me, it screams out with national security concerns."

Mr. Chew, how can all of these countries and our own FBI Director have been wrong?

Mr. CHEW. I think a lot of risks that I pointed out are hypothetical and theoretical risks. I have not seen any evidence. I am, you know, eagerly awaiting discussions where we can talk about evidence, and we then can address the concerns that are being raised.

Mrs. LESKO. Yes. My next question revolves around an article, "India Banned TikTok in 2020." A March 21st Forbes article revealed how troves of personal data of Indian citizens who once used TikTok remain widely accessible to employees at the company and its Beijing-based parent, ByteDance.

A current TikTok employee told Forbes that nearly anyone with basic access to company tools, including employees in China, can easily look up the closest contacts and other sensitive information about any user. This current TikTok employee also said, "If you want to start a movement, if you want to divide people, if you want to do any of the operation to influence the public on the app, you can just use that information to target those groups."

Why would a—Mr. Chew, why would a current TikTok employee say this if it wasn't true?

Mr. CHEW. This is a recent article. I have asked my team to look into it. As far as I know, there is—we have rigorous data access protocols. There is really no such thing where anybody can get access to tools.

Mrs. LESKO. All right.

Mr. CHEW. So I disagree with a lot of the conclusions of that.

Mrs. LESKO. Madam Chair, I request unanimous consent that the Forbes March 21st, 2023 article be added to the record.

Mrs. RODGERS. Without objection.

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

Mrs. LESKO. And I have—would like to turn over the rest of my time to Mr. Obernolte.

Mr. OBERNOLTE. Thank you, Madam Chair.

Mr. Chew, I would like to continue asking the question that we were—ran out of time last time.

So, as part of Project Texas, you are going to have engineers at Oracle review the algorithms, the machine learning algorithms that TikTok uses to ensure that they are free from foreign influence. But as you and I were discussing, reviewing the algorithms doesn't do anything. The algorithms are simple. That is not where the secret sauce is. The secret sauce is in the data used to train them and the outcomes that you are asking them to predict. Would you agree with that?

Mr. CHEW. I actually believe that, with third-party monitoring, you can identify a lot of the motivation of the code. And with enough third-party experts, you can identify a lot of what the code is designed to do.

Mr. OBERNOLTE. But how would——

Mr. CHEW. So I——

Mr. OBERNOLTE. How would you verify that you couldn't ask the algorithm for a different outcome than the one that the rest of the source code is asking for?

Mr. CHEW. The algorithm will be trained with this—it gets very technical, but it will be trained based on weights, for example. And those are things that we can verify. You know, what weights are you putting on——

Mr. OBERNOLTE. Well, if you could give us a written response to that, I would appreciate it, because I am interested.

Thank you, Madam Chair. I yield back.

Mrs. RODGERS. The lady yields back. The gentleman—gentlelady yields back. The Chair recognizes for 5 minutes the gentleman from Florida, Mr. Soto.

Mr. SOTO. Thank you, Madam Chair. The genie is really out of the bottle on this now, so to speak.

A hundred and fifty million Americans are now on TikTok. That is almost half of America. They are expressing themselves in art and music, poetry, short film, comedy, among other creative expressions. And many of them are inspiring, talented young people. But we also on the committee recognize there is a darker side to it, right? Violence, adult themes, drug and alcohol, sexualization, suicide, all major issues on TikTok, but also Twitter, Facebook, YouTube, and other social media platforms.

So the solution, as I see it, is to regulate TikTok and other social media platforms. And that job, Mr. Chew, as you know, really falls

to us. There are real concerns, bipartisan common ground we have already had. We had a Federal device ban that was voted on bipartisan in the omnibus. And I cointroduced a bill with my dear friend, Representative Cammack, about notices of that Federal ban.

Madam Chair, I think the first key is privacy. We have to pass the comprehensive legislation that got out of this committee but eluded us in the last Congress. I am really hoping we can get that done, and I am really excited about hearing that from folks.

The other thing is that TikTok needs to be an American company with American values and end its ties to the Chinese Communist Party. This is something that will be critical as we look and go forward.

And then three, we all agree we have to protect our kids. The committee should consider banning the use for children under 13 of not just TikTok but all social media platforms, or at least empower parents.

In addition, have rules of the road for teens that are 13 to 17, so that families can do what is right for their families.

So for privacy, that is on us. Internet privacy is on us.

As far as being an American company, Mr. Chew, as you know, the Committee on Foreign Investment in the United States at the Department of Treasury reviews foreign investment that affects national security. Right now they have negotiated with your company about this Oracle setup that you have talked about, servers in an American company in America, in Texas, and then Oracle would monitor the algorithms. But pressure is mounting.

So, Mr. Chew, would TikTok be prepared to divest from ByteDance and Chinese Communist Party ties if the Department of Treasury instructed you all to do so?

Mr. CHEW. Congressman, I said in my opening statement I think we are—need to address the problem of privacy. I agree with you. I don't think ownership is the issue here. With a lot of respect, American social companies don't have a good track record with data privacy and user security. I mean, look at Facebook and Cambridge Analytica, just one example.

So I do think that, you know, it is not about the ownership. It is a lot about making sure we have Project Texas, making sure that we are protecting and firewalling U.S. user data from unwanted foreign access, giving third parties to come in to have a look at this, and making sure that everybody is comfortable. We are giving transparency and third-party monitoring, and that is what we are doing for Project Texas.

Mr. SOTO. Well, I would at least encourage you all to start having the dialogue, should that be where the President and the Congress ends up going.

The third thing is on parents. I had a constituent of mine, Brandy of Lake Nona, say, "I am a parent of 2 teenagers, 14 and 18 years old, both of whom have been harmed by social media. TikTok's algorithms supply my 14-year-old son with a continuous stream of inappropriate content, and has negatively influenced his perception of all females. I noticed the attention span of both of my teens has changed or decreased dramatically, and social media has made my daughter insecure, leading to an eating disorder, and ultimately depression."

What safeguards do you have, and what should we tell Brandy of Lake Nona on—about how we can help her protect her children?

Mr. CHEW. We have a differentiated experience. I mentioned just now about the experience if you are below 13, very, very restricted. If you are below—13 to 17, Congressman, we actually have a whole series of things. The first—the content that you see, you know, we make sure that we remove things that could be mature themes from your—from your feed. We also, by default, do not allow under-16s to use direct messaging. We do not allow under-16s to—we set their accounts to private, by default. They can't go viral. If you are below 18, we shut off some features for you. Like, for example, you are not allowed to post live streams. Neither are you allowed to send virtual gifts.

So we take this very seriously, and we want to continue to build to ensure that we are giving our under-18 teenagers on our platform—although they—today they are only a minority of our user base today, but we still take it very seriously.

Mr. SOTO. Mr. Chew, I would encourage you to continue thinking about how to get the word out to parents across the Nation on some of these tools, as well, as we here craft a privacy law that will help provide well-needed regulation to social media companies across the Nation.

Thank you, and I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentleman from Indiana, Mr. Pence, for 5 minutes.

Mr. PENCE. Thank you, Chairwoman Rodgers and Ranking Member Pallone, for holding this hearing. I love both of your opening remarks.

Like my colleagues have discussed today, our increasingly digital world leaves Hoosiers and all Americans in the dark about who has access to their information. For TikTok users, that could be third-party data brokers, advertisers, or the Chinese Communist Party. TikTok aggressively feeds addictive content to users to glean massive amounts of personal data that is worth a fortune. For Hoosiers watching at home, this isn't just data about your favorite sports team.

You know, if there really are 150 million users in the U.S., this suggests to me that the CCP has a finger on the pulse of almost half our Nation's population. I find that hard to believe. But this week I decided I would ask my constituents in southern Indiana to share their stories with me. I went out Monday night, and we got 800 responses in less than 12 hours, OK? Let me share a couple of those with you.

One of my constituents shared, I quote: "I am a mental health counselor. Most of my teenage clients are on TikTok. They spend hours online being negatively influenced by others. I have seen kids experience self-harm, gender dysphoria, and many mental illnesses they have picked up from TikTok. I will not allow my children to have TikTok. The creators know the algorithms are addicting our children. They know that children are suffering more anxiety and depression from screen time, but they do not care. They will not change their algorithms because it is financially lucrative for them to keep their kids addicted."

Another parent said, "We let our child, our daughter, try it out. The feed was continuously suggesting sexually explicit, stupid, and vulgar videos. We discontinued it within a week." And there has been many more, many more. Like I said, 800, OK?

In your testimony, Mr. Chew, you walked through a number of supposed actions taken by your company to create a safe environment, empower parents to oversee content shown to their children. But virtually everything we have heard reflects the opposite. And some of your answers are a little confusing.

You know, all of those sitting here and maybe watching on C–SPAN, this is the 32d hearing we have held about privacy and Big Tech. Each hearing I have been part of, we have heard the same stories about our constituents' experience and the same promises for Big Tech to do better. The truth of the matter is, this disgusting and dangerous content littered across your platform is not justifiable, and it is uncontrollable. Americans' data is not safe, and Big Tech is doing nothing to protect it.

Putting aside the dangers of the CCP involvement and after these 32 hearings, I believe it is actually time to change the narrative, change the focus, and change the outcome by talking about the money you are making at TikTok. Mr. Chew, I have a question. How much revenue is generated per user?

Mr. CHEW. Congressman, we——

Mr. PENCE. It is a private company, and you are not going to tell me.

Mr. CHEW. A private company, yes.

Mr. PENCE. Does each user receive a comparable benefit for the amount of profit their data brings to your company?

Mr. CHEW. We do share some revenue with some creators who produce, say, 1-minute-plus informative content.

Mr. PENCE. Thanks. When am I going to get paid for the data that you are selling or your—or you are getting revenue from advertisers—when am I going to get paid for the data you are getting from my children, my grandchildren, my neighbors? I think that is the only way to get your attention, is talk about the money you are making, and maybe that will get you all to do what you are supposed to do.

Mr. CHEW. I respect and understand your opinion. The vast majority of our users have a great experience. I sent a video recently, as well. I got hundreds of thousands of comments.

Mr. PENCE. But what am I getting? It is a great experience? What about these 800 bad experiences that people in the Indiana 6th district have been getting?

Mr. CHEW. We will look into them, and a lot of the issues——

Mr. PENCE. You are going to look into it? But this is my—this is the 32d Big Tech hearing, and you are always going to look at it. Frankly, I think you are all stalling, is what you are doing. You are just trying to buy time while you are making the 18 billion, perhaps, whatever you are making.

Mr. CHEW. I—the majority of our users have a great experience on our platform. It is our duty to keep it safe. I agree with you. That is why our commitment is to make sure that safety——

Mr. PENCE. I think it is——

Mr. CHEW [continuing]. Is a priority for——

Mr. PENCE. I think it is your duty to pay attention to what you are doing, and maybe you paying people for the information that you are getting from it is a way to get that done.

Thank you, I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentlelady from Washington, Ms. Schrier, for 5 minutes.

Ms. SCHRIER. Thank you for being here, Mr. Chew. I am really concerned about everything that we are hearing in this conversation today, and I appreciate your good intentions, but the actions are really falling short.

As a pediatrician and the parent of a teenager, I am particularly concerned about how social media generally and TikTok specifically is affecting our kids and teens. We just heard a lot about this from testimony from a psychologist.

Last year the American Academy of Pediatrics sounded the alarm about our children's mental health crisis. And as a pediatrician, I know this has been going on for more than a decade. In fact, it tracks perfectly with social media engagement. And during the pandemic, teens who are missing out on in-person interactions turned even more to social media to connect with friends.

Social media is designed to be addicting. That is the business model. And your platform is the most addictive of all. And this endless, mindless scrolling takes teens away from human relationships. And here is what is important: It keeps teens awake all night, well past their bedtime at a time in their lives when sleep is critical for brain and physical development. In fact, sleep deprivation alone—ignoring even content—alone can cause depression, anxiety, social withdrawal, inattention, poor coping skills, and academic failure.

So, Mr. Chew, I just want to follow up a little bit on what my colleague Mr. Sarbanes was discussing. It is your business model to keep eyes on the app, to keep it addictive. I know you likely have experts who have advised you on how to design this to keep those eyes on your platform for the longest possible time. So I want to know if you have psychologists or other health experts on staff looking at screen time, hours of use, and sleep.

Mr. CHEW. We worked with the Digital Wellness Lab, Congresswoman, and—at the Boston Children's Hospital, and we came up with a 60-minute default limit for any users under 18.

Ms. SCHRIER. OK, so that is a——

Mr. CHEW. We were the first to do it in our industry.

Ms. SCHRIER. That is an opt out, and I can tell you they are going to immediately opt out. It is addictive.

Mr. CHEW. We also give tools——

Ms. SCHRIER. It is like asking a chain smoker not to take the next cigarette. It is not going to happen.

And by the way, so—first I have a question, then I will go back to Boston Children's. Mr. Sarbanes asked earlier, what is the percentage of teens who actually adhere to the 60-minute limit?

Mr. CHEW. I would need to check on those numbers and get back to you on specifics.

Ms. SCHRIER. I would appreciate those numbers.

Mr. CHEW. Yes.

Ms. SCHRIER. I am guessing it is an incredibly low percentage who actually heed that.

Now, as far as Boston Children's goes, I know you are referring to them as a source for these ideas about, you know, go outside, get some air, take some time out. But I can tell you, as a pediatrician, I am guessing their suggestions were a little stronger than that. And so I am wondering, what is the next step? What are you doing when you find out that almost nobody is really opting out after 60 minutes, to take this burden off of the kids and off of the parents and change your algorithms to make them not so hooked?

Mr. CHEW. We give our parents, as you pointed out, the family—the family pairing tool. And in that tool, if you pair it with your teenager's phone, you can actually set a restriction, how many minutes. And we believe it is very important for parents to have these conversations with their teenagers, so—to decide what is best for their family.

I also—Congresswoman, a lot of people come to our platform to have a really informative experience. Like I said, there were 116 billion pieces of content on STEM, and we are creating a feed dedicated to that. Book Talk has 115 billion——

Ms. SCHRIER. We also—we have also heard today that well over 20 percent of the information is misinformation. We heard that about medical remedies that are not really remedies. We have heard it about mental health topics.

I mean, this becomes very dangerous, especially when people who are not trained to think very critically are being given information and thinking that it is true. And you have said many times that the destructive information isn't available to kids, but it is. Like, we keep seeing examples here.

And so I am just wondering, what are you going to do with the algorithms? I mean, just because you are removing something that says "anorexia," "bulimia," or "eating disorder," that doesn't do it. If you show girls repeatedly skinny bodies and advice on how to cook meals that are less than 300 calories, that is dangerous.

Mr. CHEW. We have worked with—first of all, all—anything that glorifies eating disorders, we remove that from our platform as violative. We are working with experts now. It is a challenging problem for our industry, but we are actually identify—identifying some of these themes that you are talking about, and trying to build models where that kind of content is not up for the younger users. So it is something we take very seriously too.

Ms. SCHRIER. We are seeing eating disorders in elementary-age kids now, and I need you to expedite that process as much as possible, because parents out there are worried, and I am worried as a pediatrician. Parents can't take themselves off of these platforms. Kids, there is no way they are going to take themselves off. And we need you to do your part. It may affect your bottom line, but it could save this generation.

Mr. CHEW. I share your concerns, and I commit to doing more.

Ms. SCHRIER. I yield back.

Mrs. RODGERS. The gentlelady yields back. The Chair recognizes the gentleman from Pennsylvania, Mr. Joyce.

Mr. JOYCE. Thank you, Chair Rodgers and Ranking Member Pallone, for holding this hearing.

According to an August 2022 article in the New York Times, TikTok's in-app web browser can track every individual keystroke made by a user. We have heard today about the various ways in which the app's code could be used to monitor or track users. And likewise, we have heard concerns that this data may not be fully isolated from access by the Chinese Communist Party.

That said, I would like to know more about the historical nonpublic U.S. personal data that your company has already amassed. Mr. Chew, you have publicly stated that the nonpublic information of TikTok users in the United States is being transferred to an Oracle-based cloud infrastructure because of safety concerns. Will that be completed by the end of this week, by the end of this month?

What is the outline for dealing with that data that you have already amassed?

Mr. CHEW. All new data is already stored by default in this Oracle Cloud infrastructure, with the——

Mr. JOYCE. No, I am talking about the data that you have already amassed.

Mr. CHEW. We are in the process of deleting.

Mr. JOYCE. What timeline will that data be able to be stored?

Mr. CHEW. We will—I believe we will be able to get it done this year. I am hiring——

Mr. JOYCE. This year. Thank you. It is not going to occur any time soon.

To be clear, until that data transfer happens, user data remains accessible to the Chinese Communist Party.

On March 1st of this year, the committee asked you when you plan to delete nonpublic historical U.S. user data. Are you aware of this?

Mr. CHEW. Congressman, I disagree with this assessment that the Chinese Government can get access to the data. It is really for—look, this is a private company. This is what—Chinese employees——

Mr. JOYCE. You responded in writing to this committee. I have the response that we got back from you on March 7th, just 6 days later. Your attorneys wrote, "The company"—I am quoting—"The company plans to begin the process of deleting nonpublic historic U.S. user data this month, and anticipates that the process will be completed this year."

You came up with a supposed plan in the summer of 2022, specifically based on our concerns that the communist Chinese Government was spying on U.S. users. But you only just came up with the idea to delete historic nonpublic U.S. data just 2 weeks ago?

Let me read it again: On March 7th, your attorneys wrote—and I quote—"The company plans to begin the process of deleting nonpublic historical U.S. data this month, and anticipates that the process will be completed this year."

Mr. Chew, did you just come up with this plan only because we asked about it on March 1st?

Mr. CHEW. No, we started deleting this——

Mr. JOYCE. Because that is what it looks like to me.

Mr. CHEW. We hired a third-party auditor——

Mr. JOYCE. This is incredibly disappointing.

Mr. CHEW [continuing]. To help us with this.

Mr. JOYCE. Wouldn't you agree that awaiting even minutes for this personal privacy protection is absolutely wrong, and it is not in the best interest of your users?

Mr. CHEW. Congressman, respectfully, there are many companies that use a global workforce. We are not the only one. We are just taking action after hearing——

Mr. JOYCE. Given the delay——

Mr. CHEW. Many other companies have not.

Mr. JOYCE [continuing]. In reading this data, and what we have already established about the ability of the Chinese Communist Party to access personal user data, would you agree that no U.S. Government electronic devices should have access to TikTok platform, as your lackluster security currently stands?

Mr. CHEW. I disagree with that characterization. Like I said, the U.S.——

Mr. JOYCE. Do you think that any individual should be utilizing that on any Government platform?

Mr. CHEW. I think the Government devices should have no social media apps, to be honest, but——

Mr. JOYCE. And particularly TikTok.

Mr. CHEW [continuing]. Targeted to us.

Mr. JOYCE. Mr. Chew, during this hearing you have mentioned several times that there is a "different experience," your words, for children under the age of 13.

Mr. CHEW. That is correct.

Mr. JOYCE. A different experience. Mr. Chew, do you allow your children under the age of 13 to participate in TikTok? Yes or no.

Mr. CHEW. I did just explain this in detail. This experience doesn't exist in Singapore, where my children live. If my children lived here, then yes.

Mr. JOYCE. Based on what we have heard today, it is clear to me that TikTok, as a company, cannot be trusted, and that Americans remain significantly at risk because of the TikTok app. I still contend that TikTok is the spy in Americans' pockets.

I want to acknowledge that TikTok does have the ability to make those changes. But unfortunately, we have not heard that from you today. We have not heard a commitment to be able to protect the personal privacy that Americans expect and that Americans deserve.

Thank you, Madam Chair, and I yield the remainder of my time.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes Mrs. Trahan for 5 minutes.

Mrs. TRAHAN. Thank you, Madam Chair.

Mr. Chew, many Big Tech CEOs have sat where you are sitted—seated today and tried to run out the clock during a hearing like this one. They were trained not to answer questions and just wait for the news cycle to pass so that they could get on with business as usual. Those same executives want this moment, TikTok's moment under the microscope, to distract Congress and the American people from the very real issues that exist on their platforms.

You have an opportunity to turn the tables on them. While U.S.-based social media giants have regressed on protections for children and teens, on protecting our data privacy, and on embracing

transparency, you can lead, and you should lead. Last month you announced that TikTok would expand access to its researcher API. But I am concerned that your new policy could be more bark than bite, that it won't actually lead to the rigorous research that we, as lawmakers, and that parents and everyday TikTok users need.

In fact, your terms of service demand that researchers delete their data at TikTok's unilateral direction. It puts onerous restrictions on how researchers' findings can be published, and it only allows access to public data, which researchers already have access to within the app.

In order to actually address the content moderation and algorithmic amplification concerns that my colleagues have raised here today and that I have heard about directly from parents in my home State of Massachusetts, independent researchers, not just other tech companies like Oracle, need to be able to evaluate how TikTok's algorithm is making decisions to promote content.

Mr. Chew, will you commit to expanding your API to include data that would let researchers investigate how your algorithm is pushing content to users, whether it is showing up on your For You page, the hashtag page, or somewhere else?

Mr. CHEW. We are—one of the commitments I gave in the opening statement is a commitment to transparency and third-party monitoring. So Congresswoman, I will look into the details of that and get back to you.

Mrs. TRAHAN. And as well as the algorithm, including data on what types of users were targeted by the algorithm so that researchers can fully understand what content is being prioritized and who it is being pushed to.

Mr. CHEW. Again, we have a commitment to transparency. These are very important questions, and I will get back to you on the specifics.

Mrs. TRAHAN. Under this same proposal, you require that researchers give TikTok, quote, "worldwide, free, nonexclusive, and perpetual," end quote, rights to their papers. This threatens to clash directly with well-established practices of exclusive publication rights in research journals.

Mr. Chew, why does TikTok need those rights?

Mr. CHEW. I would need to get back to you on the specifics, if that is OK.

Mrs. TRAHAN. Yes. I don't see how we can expect researchers to do their work under these terms and then tout transparency.

I am going to shift gears with the time that I have remaining, Mr. Chew. I would like to talk about TikTok's efforts to protect children and young users. In 2021 the UK's age-appropriate design code went into effect, mandating 15 standards that companies like you need to follow to protect children on your platform. You still operate in the United Kingdom, which means you should be in compliance with this code.

So my question is simple: Will you commit to extending the protections currently afforded children in the UK to the millions of kids and teens who use your app here in the United States?

Mr. CHEW. We take the safety of the younger users on our platform very seriously. Every——

Mrs. TRAHAN. This is a good way to prove it.

Mr. CHEW. Every country is a little bit different in context, and in—so let me look at the specifics, and bring some of the best practices across the world. But——

Mrs. TRAHAN. Well, those best practices are in—they are being executed around the world. We just want the same for our kids here in the United States.

I mean, Mr. Chew, when we spoke a couple of weeks ago you indicated interest in taking steps to earn trust, our trust. And to me, it hasn't happened today so far. But rather, you have ducked behind industry standards and comparables to your competitors, which we know are woefully insufficient.

I strongly urge you to consider these terms, these commitments. Make the case for why you are different from your American competitors, and do better on—than them on transparency, which you have mentioned countless times today, but which we don't really have anything tangible to point to.

Mr. CHEW. Yes, I don't want to make excuses for our industry or ourselves. I think there is a lot of work that needs to be done. We take this very seriously. Nothing is—it is not perfect. We need to keep investing to stay ahead of our growth.

So I agree that, you know, we need to prioritize safety and continue to do that as part of our company. And——

Mrs. TRAHAN. Well, I look forward to getting back your comments and your commitments and those updated terms of service when you write back to the committee.

Thank you, Madam Chair.

Mr. CHEW. Thank you.

Mrs. TRAHAN. I yield back.

Mrs. RODGERS. The gentlelady yields back. The Chair recognizes the gentleman from North Dakota, Mr. Armstrong, for 5 minutes.

Mr. ARMSTRONG. Thank you, Madam Chair. You know, we have heard a lot today about the procedural safeguards, independent code review, server locations, and the corporate independence between ByteDance and the CCP. But I think there is something else a little more telling.

You know, when you were asked about Chinese censorship, you pivoted immediately to drug use in Singapore. You have absolutely tied yourself in knots to avoid criticizing the CCP's treatment of the Uyghur population. And I think it begs the first question: Before we ever get to Project Texas, which I will get to in a second, if the CCP demanded that ByteDance hand over all of the data that they had on user—on U.S. users in their possession and ByteDance refused, I wonder what would happen. I wonder if Jack Ma might have an opinion on that, and I wonder if he would be allowed to give it.

But let's talk about Project Texas for a second. Project Texas envisions a new U.S.-based TikTok subsidiary. You have stated that this arrangement is unprecedented. I would argue the reason it is unprecedented is because it requires continual oversight and monitoring by the U.S. of a private business because it poses a national security threat.

The new subsidiary's board would report to and be approved by CFIUS. CFIUS will also specify hiring requirements, as well as interact with Oracle as it performs its data role. That is an extraor-

dinary corporate governance structure. I have questioned whether it complies with corporate law and fiduciary duty to shareholders.

Yet the core concern is that the—proposes unparalleled integration with the U.S. Government with a private company, which will require significant Government resources, all of that to allow a continued operation of a social media platform that has serious national security implications. And CFIUs' workload has already dramatically increased in recent years, with a 30 percent increase in declarations and a 45 percent increase in joint voluntary notices. And there is bipartisan consensus that CFIUS needs to be expanded as we speak.

The only—Mr. Chew, can you identify any similar corporate arrangement that requires Federal Government to expand such resources to monitor an alleged data privacy and national security risk?

Mr. CHEW. Congressman, I am not an expert on this matter. I believe that there are certain similar arrangements, but I am not the expert on this matter.

Mr. ARMSTRONG. Well, the only one I could find was the UK created the Huawei Cyber Security Evaluation Center in 2010 to assess Huawei's tech and to detect malicious activity and guard UK's networks. That has worked so well that the United Kingdom is now planning on kicking Huawei out of Great Britain.

You have stated that TikTok has invested $1.5 billion in Project Texas. Are you aware of any discussions or proposals that entail TikTok funding or offsetting the costs of CFIUs' role?

Mr. CHEW. Those discussions are—I need to get back on you—on the specifics. But I can tell you, yes, we did spend approximately 1.5 billion U.S. dollars on our side.

Mr. ARMSTRONG. You spent $1.5 billion on Project Texas. But do you have any—I mean, you agree that, if CFIUS takes on this role, they are going to need a massive influx of dollars in human resources, right?

Mr. CHEW. I cannot speak on behalf of CFIUS, Congressman.

Mr. ARMSTRONG. Should the U.S. Government expend such resources to create this extraordinary arrangement for TikTok, especially considering alleged data privacy and national security risks?

Mr. CHEW. Congressman, I cannot speak on behalf of the United States——

Mr. ARMSTRONG. Well, the Project Texas doesn't work without CFIUS, right? And Project Texas, as you guys have proposed it, does not work without CFIUS involvement.

Mr. CHEW. The idea behind Project Texas is the firewall of U.S. user data, make sure it is stored by an American company overseen by American personnel, and we will invite third-party monitors to monitor this. So that, in essence, at least as far as I know, is the majority of the cost, because it will rely on not just us building the infrastructure, but us, you know, finding and hiring these third-party monitors who are vetted to come in and monitor this structure.

Mr. ARMSTRONG. You talked earlier about the shareholder's ownership of TikTok, and you said 60 percent global investors, 20 percent is employees, and 20 percent is original founders. Are all those voting shares the same?

Mr. CHEW. No, the founder has weighted voting rights, as is common in our industry.

Mr. ARMSTRONG. So do—as far as a voting block of shares owned in ByteDance, do you know if the Chinese Communist Party—not Chinese Communist Party officials, the Chinese Communist Party—do you know what their percentage of the actual voting block share of ByteDance is?

Mr. CHEW. The Chinese Communist Party doesn't have voting rights in ByteDance.

Mr. ARMSTRONG. Chinese Communist Party members is a different question. Do the founders control the voting block of ByteDance's shares?

Mr. CHEW. I do know that the founder himself is not a member of the Communist Party, but we don't know the political affiliation of our employees, because that is not something we ask.

Mr. ARMSTRONG. Does the Chinese Government know the political affiliation of their Chinese citizens?

Mr. CHEW. I cannot answer that question on their behalf.

Mr. ARMSTRONG. I yield back.

Mr. CHEW. The gentleman yields back. I yield to the lady from—the gentlelady from New Hampshire, Ms. Kuster, 5 minutes.

Ms. KUSTER. Thank you, Madam Chair.

Mr. Chew, I just want to say I agree with all of the comments of many of my colleagues today that we need to take a close look at whether TikTok poses a national security risk. For today I am going to focus my limited time on how TikTok can better protect its youngest users. And I think a number of us have identified as parents today and have serious concerns, as we relayed to you.

Just this week I heard from a parent in my district in Nashua, New Hampshire, whose child was served harmful content on TikTok and has needed counseling as a result. This experience is not unique to this family, and it underscores the need for better child protections on your app.

I would like to dig further into TikTok's current safety and privacy controls for children. I understand that TikTok restricts certain app capabilities for users under age 18 and has additional restrictions for users under age 16 or 13, such as limiting who can interact with them on the platform. However, these protections are worthless if any savvy child can easily bypass these age restrictions by deleting their own account and creating a new one with a different age. And by "easily," I mean you can literally go in and open another account using the same email address.

So I have been made aware by child safety groups, including Fair Play for Kids and Common Sense, that it is that simple for young users to bypass the age restrictions on TikTok. Yes or no, are you aware of this issue?

Mr. CHEW. I apologize. I think that is a great issue—question that you raised. If a user inputs an age and is blocked, my understanding is that if the user tries to do it again within a short period of time—and I won't disclose publicly——

Ms. KUSTER. We did it in our office yesterday. You can go right back in, use the exact same email address, and open a new account. So can I get your commitment that you will at least fix that bug?

Mr. CHEW. I will go and have a look at it, yes.

Ms. KUSTER. Thank you. If—we are here today to talk TikTok and not other platforms, but I am happy to look at legislative solutions.

In the interim, TikTok has a responsibility to do more to protect its young users, and I will accept your commitment to take a look at fixing that issue. Will you—let's see—sorry. I recognize that TikTok has made efforts to provide parents and guardians—increase options to monitor and limit their child's activity on the app, including family pairing and time limit features. But I still have concerns.

In order to access family pairing, parents then must download the app onto their phone, and this sounds like a design to lure more users onto the app rather than a practical safety feature. Furthermore, downloading the app may not be a viable option for many patients—parents.

Mr. Chew, will TikTok commit to developing other methods for parents to monitor their child's use of the app without having to download the TikTok app on their phone?

Mr. CHEW. I can look into that specifically, and get back to you.

Ms. KUSTER. OK.

Mr. CHEW. But the family pairing that you mentioned is a very good tool that we developed. I encourage parents with teenagers to——

Ms. KUSTER. But it is not a perfect——

Mr. CHEW [continuing]. To use it.

Ms. KUSTER [continuing]. Tool, and let me just say one of my concerns is that the minimum time limit TikTok lets parents set for their children is 40 minutes, which, for a young child, is a very long period of time. Actually giving parents control would mean providing them the freedom to set the screen time that makes sense for their family.

Now, I have got a copy of the app page that shows just the four options. Would you commit to adding an "other" option, so that the parent can easily set their own screen time limit?

Mr. CHEW. I can take a look at that.

Ms. KUSTER. I think it is important. I think parents are looking for control. They are looking to allow their family to use these apps without TikTok taking over their child's media use.

I have heard use reports—I have heard reports of users struggling to access the feature. And so I will look forward to hearing back from you on adding an "other" so that a parent can add a custom limit.

So finally, I ask that you commit to report back to this committee and the American public on how TikTok addresses these safety issues and the steps that you are taking to default children's accounts to the most protective possible settings.

And with that, Madam Chair, I yield back.

Mrs. RODGERS. The gentlelady yields back. I yield to—the Chair yields to the gentleman from Ohio.

Five minutes, Mr. Balderson.

Mr. BALDERSON. Thank you, Madam Chair.

Thank you, Mr. Chew, for being here today.

I would like to start by inserting into the record a report entitled "TikTok, ByteDance and Their Ties to the Chinese Communist Party," which was published by the Australian Parliament just over a week ago. If I could add that to the record, please.

Mrs. RODGERS. Without objection, so ordered. 1A[1]

Mr. BALDERSON. Thank you, Madam Chair.

Mr. Chew, we know that your company's algorithm has been exposed for delivering videos to China that encourages them to develop eating disorders, promotes challenges that have caused children to accidentally commit suicide, glorifies the use of drugs and pornography. Despite the constant media coverage of this issue, your company continues to feed our children this dangerous and harmful content.

Can you explain to parents back in my congressional district why it should be their burden and not TikTok's to set up the guardian parental controls for their children so that they do not view content which encourages eating disorders or committing suicide?

Mr. CHEW. Congressman, I take these issues very seriously. If the user is between—is a teenage user on our platform, we actually have a differentiated experience, including certain models that we are building with experts to help identify certain content that is not inherently harmful but could lead people to eating disorders. Anything that glorifies eating disorders is violative of our platform, and we remove that. And I want to assure you that I take this very, very seriously, this commitment.

Mr. BALDERSON. OK. Mr. Curtis, my colleague, mentioned the use of a heating tool on your platform to make specific videos go viral or get more views. Does TikTok use a cooling tool, where employees can manually limit the amplification of content that TikTok should hide, like content that promotes eating disorders, drug use, or suicide among children?

Mr. CHEW. The only promotion tool that we have is approved by the local teams—so in the U.S. by the U.S. team—and it is for commercial purposes. Like Taylor Swift, you know, I think when she onboarded we, you know, heated——

Mr. BALDERSON. So would that be a yes or no?

Mr. CHEW. My—I just want to make sure that I am answering your question with specifics.

Mr. BALDERSON. If this tool exists, why isn't it being used to cool then the spread of dangerous content? I mean, why is it still happening?

Mr. CHEW. Dangerous content has—that violates, we remove them. When we see them, we actually remove them from the platform.

Mr. BALDERSON. OK. The fact of the matter here is that, despite whatever action you take, that TikTok is taking to protect teens, your algorithm continues to promote harmful content. Wouldn't you agree that indicates there is something inherently wrong with the algorithm your platform employs?

Mr. CHEW. I do respectfully disagree with that. The algorithm drives a great user experience for many, many users. Well, I talked

[1] The information has been retained in committee files and is included in the Documents for the Record at https://docs.house.gov/meetings/IF/IF00/20230323/115519/HHRG-118-IF00-20230323-SD030.pdf.

about STEM content. That has 116 billion views on our platform. One more example: Book Talk is a trend that happened on our platform. It is to encourage people to read. And globally, it has 115 billion views, and it is fantastic. I have heard people telling me that they are reading more because of Book Talk. So there is a lot of good, and joy, and positive that can be derived from the TikTok experience. Yes, there are some bad actors who come in and post violative content, and it is our job to remove them. But the overwhelming experience is a very positive one for our community.

Mr. BALDERSON. But if it is your job to remove them, it has been said many times here today about the 41 days that that video stood up with addressing Mrs.—the chairwoman.

Mr. CHEW. After this I am going to go and look into the specifics of that.

Mr. BALDERSON. All right, thank you.

Mr. CHEW. Yes.

Mr. BALDERSON. Madam Chair, I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the lady from Texas, Mrs. Fletcher, for 5 minutes.

Mrs. FLETCHER. Thank you, Chairwoman McMorris Rodgers, and thanks to Ranking Member Pallone for holding today's hearing. And thank you, Mr. Chew, for appearing today.

It has been a long day, but we are here to learn about a complex set of issues that relate to TikTok and how to address them. And I think that is what we are hearing from colleagues on both sides of the aisle today, is a real effort to grapple with the challenges that we see for national security, and for the safety and protection of American citizens, especially our children and young adults.

And we have already covered today a lot of the information about the extensive use of the app, the number of users who are children and young adults. But I think it bears repeating, as Mr. Veasey mentioned, that TikTok is the preferred platform of young Americans, and they use it for all kinds of creative and important things. And we have seen that. But there are also some dangerous things that we know it has and continues to be used for, and that—also that the data that is collected is posing additional dangers. And that is—that is what we are here for.

Most people using TikTok do not realize that TikTok is collecting data about their keystrokes or about their browsing history on other sites, and so much more. And I agree with my colleagues that we need a comprehensive set of data privacy laws here in the country, and we have heard some very good ideas today.

Mr. Chew, you have mentioned several times today that these are industrywide issues, and I agree with you that there are industrywide challenges here. But there are also some specific things relating to TikTok that I want to focus my questions on, and really want to understand where there is a difference and how we can craft legislation that addresses the very real challenges that we have been hearing about today.

As you know, States across the country have joined an ongoing investigation into possible violations of consumer protection laws by TikTok as they pertain to TikTok's effect on the mental health of American children and teenagers. As part of this investigation, States have requested to review internal TikTok communications

that takes place on Lark. That is TikTok's primary instant messaging system. Is that right?

Mr. CHEW. Yes.

Mrs. FLETCHER. OK. And does every TikTok employee have a Lark account?

Mr. CHEW. It is very similar to companies that use Slack or any other instant messaging tool.

Mrs. FLETCHER. But Lark is a proprietary instant messaging tool. It is not Slack.

Mr. CHEW. It is something that was developed, yes, by ByteDance.

Mrs. FLETCHER. And it was developed by TikTok?

Mr. CHEW. No, it was developed by ByteDance.

Mrs. FLETCHER. It is developed by ByteDance. OK. And so a couple of questions stemming from that.

Is it true that Lark videoconferencing has a translation feature in which Chinese is translated to English text and vice versa?

Mr. CHEW. That is correct. It helps with global cooperation.

Mrs. FLETCHER. OK, and those translated conversations are somehow saved into the Lark system?

Mr. CHEW. I would need to get back to you on the specifics. There is a—you know, I will get back to you on the specifics.

Mrs. FLETCHER. OK. That would be great to know. And I neglected to ask, but does every TikTok employee have a Lark account?

Mr. CHEW. Yes, I believe so. Yes.

Mrs. FLETCHER. Including you, do you have one?

Mr. CHEW. Yes, I believe so, yes.

Mrs. FLETCHER. And then do you have a—there is some kind of profile for your instant messaging system so every employee identifies their manager and their department, who they work for, what they do. Is that all included in their Lark profile, do you know?

Mr. CHEW. It is very common for companies to have enterprise messaging tools that——

Mrs. FLETCHER. Sure.

Mr. CHEW [continuing]. Companies use.

Mrs. FLETCHER. It does. And I guess I am asking specifically about Lark, since it is specific to TikTok, whether it includes information like identifying who, for example, your manager is. Do you know whether that is something that is identified in Lark?

Mr. CHEW. Yes. Again, some of these HR features are built into a lot of enterprise tools that we use. And—yes.

Mrs. FLETCHER. So, like, for your own profile, does it identify who your manager is?

Mr. CHEW. Yes, it does.

Mrs. FLETCHER. And who does it identify as your manager?

Mr. CHEW. I report to the CEO of ByteDance.

Mrs. FLETCHER. OK. And so that is Zhang Yiming. Is that identified as your manager? That is the former CEO.

Mr. CHEW. He has stepped down from the board. And——

Mrs. FLETCHER. OK, so——

Mr. CHEW. That is the CEO, yes.

Mrs. FLETCHER. OK. So Mr. Rubo is identified now as your manager on——

Mr. CHEW. Yes.

Mrs. FLETCHER [continuing]. The system? OK. And as you mentioned, it was developed by ByteDance. So it is not just used by TikTok employees, it is also used by ByteDance employees, is that right?

Mr. CHEW. Also by other companies now. I think Lark is selling it, and it is a good tool for instant messaging.

Mrs. FLETCHER. So Lark is available to third parties outside of the ByteDance system, as well, like Slack?

Mr. CHEW. Yes.

Mrs. FLETCHER. And do you personally ever use Lark to communicate with ByteDance?

Mr. CHEW. With employees at ByteDance? Yes, I do.

Mrs. FLETCHER. You do? OK. Well, I am running out of time, and I am sorry to say, because this is really interesting. I do think it underscores some of the concerns that have been raised in this hearing. So I think it is clear we have work we need to continue to do here in the Congress to address data protection and privacy.

And with that, Madam Chairwoman, I thank you, and I will yield back.

Mrs. RODGERS. The gentlelady yields back. The committee stands in recess, and we will reconvene immediately following the third vote being called.

[Recess.]

Mrs. RODGERS. The gentleman from Texas, Mr. Weber, is recognized for 5 minutes.

Mr. WEBER. Thank you, Madam Chair and, Mr. Chew, thanks for being here.

Mr. Chew, I am one of six Texans on this committee. I am over here. So when you invoke the name of Texas, you get my attention.

Mr. Chew, when you were the CFO of ByteDance, did the Chinese Government instruct you on how content was to be moderated on Douyin or TikTok, yes or no?

Mr. CHEW. Sorry, Congressman, would you mind repeating that question?

Mr. WEBER. When you were the CFO of ByteDance, did the Chinese Government instruct you on how content to be moderated—was to be moderated on Douyin or TikTok?

Mr. CHEW. I was not in charge of that. That is the CFO of——

Mr. WEBER. You were not?

Mr. CHEW [continuing]. Of ByteDance.

Mr. WEBER. OK, we have a discrepancy there.

Reports have shown that TikTok accounts managed by media links to be a propaganda arm of the CCP, pushed divisive content before the recent midterm election. Mr. Chew, yes or no, has—to your knowledge, has the CCP coordinated or utilized TikTok to influence users through algorithms, state-paid content creation, or in any other capacity?

Mr. CHEW. No, they do not do that. We do not promote or remove any content on behalf of the Chinese Government.

Mr. WEBER. You don't, but did the Chinese Government? Do you have any knowledge of that?

Mr. CHEW. We do not do—Congressman, we have only one process of removing content on our platform——

Mr. WEBER. OK.

Mr. CHEW [continuing]. And the process is done by our content moderation team headquartered in Ireland, in Dublin—sorry—Ireland and the U.S. And we will only remove content if it violates our guidelines. And that is something that we audit, you know, or if there is a valid legal order. So——

Mr. WEBER. OK. Several reports, hearings, and leaked internal documents have indicated that TikTok has repeatedly censored or deamplified content that is critical of the Chinese Communist Party's party policies in the U.S. and abroad. Are you aware of those reports?

Mr. CHEW. I don't think that is accurate, Congressman. I do not——

Mr. WEBER. Are you aware of those reports?

Mr. CHEW. There could be some reports that say that, but that action itself is not something——

Mr. WEBER. But your testimony here today is that you can keep up with stuff and make it as "clean as possible." Are you aware of those reports?

Mr. CHEW. I want to make it very clear that we—there is content on TikTok that is great and fun, there is content that is critical of China, and——

Mr. WEBER. That is not what I am saying. Are you aware of the reports citing that fact?

Mr. CHEW. Again, like I said, the fact is if you go onto our platform, you will find content that is critical of China.

Mr. WEBER. Well, we are going to talk about that. Now, this committee is looking at reforming section 230 of the Communications Decency Act, which has already been mentioned here today. Do you think that censoring history and—historical facts and current events should be protected by section 230's good faith requirement?

Mr. CHEW. Congressman, that is a more complex topic. I would need to speak to my team and get back to you on the specifics.

Mr. WEBER. Is your team behind you?

Mr. CHEW. It is my broader team. I will speak to them and I will get back to you.

Mr. WEBER. It is always good to have folks behind you, isn't it?

Mr. CHEW. Not them.

Mr. WEBER. Oh, no? OK, I got you.

Here are my concerns with TikTok. Your claims are hard to believe. It is no secret to us that TikTok is still under the thumb of CCP influence. And let's be honest, TikTok is indoctrinating our children with divisive, woke, and pro-CCP propaganda, all while threatening our national security with Chinese spyware.

In fact—let me look at my notes here—you had an exchange with Anna Eshoo. In your exchange with Congresswoman Eshoo you said that "extreme fitness videos shouldn't be viewed too much," do you remember that exchange here today?

Mr. CHEW. What extremist videos?

Mr. WEBER. With Anna Eshoo out of California.

Mr. CHEW. I—any content that is—has extremist content——

Mr. WEBER. OK.

Mr. CHEW [continuing]. Is not allowed on our platform. It will be—we identify them, and we——

Mr. WEBER. Was that also true about the gun video that you saw today? Was that extreme content that should have been taken down?

Mr. CHEW. I would need to look at the specifics of the whole video. There was a bit of lag just now. We couldn't see the whole video.

Mr. WEBER. OK. You know it threatened our committee chair here?

Mr. CHEW. That is unacceptable.

Mr. WEBER. OK.

Mr. CHEW. And, you know——

Mr. WEBER. So you are aware of that extreme video. And why did it take 40-plus days to get it down? Does it take literally an act of Congress? Should we plan to have a committee hearing every time, every day, every time there is something brought up, so that we can limit the content on TikTok? Should Congress plan to do that, Mr. Chew?

Mr. CHEW. Congressman, we work very hard to remove violative content on our platform.

Mr. WEBER. OK. Well, let me move on. With Congressman Hudson, he asked you about your wages and your stocks, and you said you would prefer to keep that information private. Now you know how we feel about American public's information. We prefer to keep it private, as well, and we don't think TikTok does that.

So, Madam Chair, my time is up. And if this committee gets its way, TikTok's time is up.

Mr. CHEW. Madam Chair, if I may——

Mrs. RODGERS. The gentleman——

Mr. CHEW [continuing]. In my response to an earlier question——

Mrs. RODGERS. The gentleman—I am sorry, the gentleman's time has expired, or—yes, I—the Chair recognizes Mr. Ruiz from California for 5 minutes.

Mr. RUIZ. Thank you, Chair Rodgers. I echo my colleagues' concerns about TikTok's impacts on the health and well-being of the American public.

As a doctor and the ranking member of the Select Subcommittee on the Coronavirus Pandemic, I am troubled that TikTok is rife with medically inaccurate information, including dangerous misinformation and the intentional disinformation about COVID–19 and vaccines. TikTok's community guidelines state that the company will remove content or accounts that involve, quote, "misleading information that causes significant harm." However, since the early stages of the pandemic, TikTok has been used as a platform for people pushing misinformation, disinformation, including by those casting doubt on the safety and efficacy of lifesaving vaccines.

And despite TikTok's pledge to address harmful misinformation, these videos are being viewed millions of times. For example, the Institute for Strategic Dialogue found that a sample of 124 TikTok videos containing vaccine misinformation were viewed 20 million times. And Media Matters found that a sample of 18 videos with COVID–19 misinformation were viewed over 57 million times.

Here is another shocking study: The Journal of American Medical Informatics Association found that, when searching

"#coronavirus" on TikTok, almost 30 percent of the videos that came up contained misinformation. Videos in that sample containing a high level of misinformation were viewed a median of 9.4 million times.

Mr. Chew, what are these—why are these dangerous videos falling through the cracks of your company's efforts to enforce its own community guidelines and remove harmful misinformation?

Mr. CHEW. Before I answer that, in my response to an earlier——

Mr. RUIZ. No, no, you are——

Mr. CHEW [continuing]. Question from Representative Dunn——

Mr. RUIZ. You are in my—Mr. Chew you are in my time. Answer my question.

Mr. CHEW. I understand. But if—I would like to clarify something.

Mr. RUIZ. Clarify, I have 5 minutes.

Mr. CHEW. OK.

Mr. RUIZ. In my time. You are in my time now. Answer my question.

Mr. CHEW. Yes. Any dangerous misinformation is—we partner with third-party experts to be able to identify and help us with subject domain expertise, and with the expertise that we recognize we rely on those to develop policies that recognize and remove content that could be——

Mr. RUIZ. Well, your efforts are—have failed, and they are dangerous. OK? It's public health risks that—you are putting millions of people's lives at risk for not being able to do a better job.

And I am concerned that TikTok's features make it—users uniquely vulnerable to the spread of this misinformation. For example, TikTok makes it extremely easy to reuse audio and videos to create content, which allows misinformation to quickly spread through the platform and TikTok's algorithm. To recommend videos means that a user viewing one video containing misinformation can easily result in their quote-unquote "For You page" becoming filled with videos containing similar misinformation. This is a dangerous feedback loop.

So is TikTok taking any action to modify these features so that they no longer facilitate the spread of this misinformation or this misinformation feedback loop?

Mr. CHEW. Congressman, again, like I said, any dangerous mis- or disinformation we work with third parties to recognize that, and it is proactively removed from our platform.

Mr. RUIZ. OK, so——

Mr. CHEW. So it doesn't get into those loops at all.

Mr. RUIZ. So I can—I can go back and read you the data and the Journal of American Medical Informatics: 30 percent of videos after searching for #coronavirus had misinformation. Like, almost one out of three. Your third party and your company are missing one—almost one out of three misinformed videos. So you are telling me what you are doing; I am telling you the data shows that you are grossly failing at that effort.

The other thing, the other question I have for you is that TikTok is also in Spanish, and Spanish-speaking populations have been specifically targeted to misinformation when it comes to many as-

pects, especially medical misinformation. And as chair of the Congressional Hispanic Caucus, we reached out to you last Congress on this issue.

So what is your intent, or how does your team look like to address Spanish versus English?

How many staff do you have focusing on Spanish versus how many staff do you have focusing on English misinformation?

Mr. CHEW. Congressman, I was—like I had explained just now, the Spanish-speaking population is very important to our platform. We do have a lot of Spanish-speaking moderators, and we will continue to——

Mr. RUIZ. So how many Spanish-speaking staff versus English-speaking staff for misinformation do you have?

Mr. CHEW. I can get back to you on the specifics, but dangerous misinformation is moderated, regardless of language.

Mr. RUIZ. Not to the degree that it needs to be.

Mr. CHEW. We are—we can continue to work hard to——

Mr. RUIZ. And when there is misinformation, people base their decisions that oftentimes put them at risk and exposures, and their families at risk. And with the coronavirus, especially prior to the vaccines, they—the risk was their life.

Thank you, I yield back.

Mr. CHEW. Madam Chair, I would like to clarify something. In the followup question to Representative Dunn's question just now, I misunderstood the followup about ByteDance buying on behalf of the Chinese Government. My answer to that question should be a no, because it came very rapidly. I just want to clarify that.

Mrs. RODGERS. The gentleman's time has expired. The gentleman—or the Chair, the Chair recognizes the gentleman from Idaho, Mr. Fulcher, for 5 minutes.

Mr. FULCHER. Thank you, Madam Chairman.

Mr. Chew, we have been going a long time here by now, and a lot of questions have been answered, and a lot of them have not been answered. And the primary thing I want to do is just share some thoughts of what I have seen, learned today, been exposed to.

First of all, I have got to compliment you on having a product that is impressive. It is a very influential tool. It is addictive. And that is what you want users to be exposed to, something addictive. And it is a data-gathering masterpiece. So clearly, it has got the potential to sell products, connect like-minded people with that artificial intelligence capability in a viral, viral fashion, and perhaps spread information quicker, better than anything else that has been developed out there.

Now, I am just going to tell you, I am not a subscriber, at least a willing subscriber. But probably in that database somewhere is my preferences with colors or foods or who I have spoken to or what I have said, my favorite newspapers, I don't know. But that is available to be sold or given to whomever or whatever. And the whatever is what bothers me.

And I will use myself as an example again. If for whatever reason I became a target in this, I became somebody you didn't like—and I know that would be hard to believe, because you have got to like me—but let's say you didn't, or your company didn't. Or for whatever reason, I became an app target. That artificial intel-

ligence algorithm could be shared or spread selectively to a targeted audience that—with negative information that maybe they—has been paired up with that knowledge and that app to make me look really, really bad. Or to the converse, the same thing could be done to make me look really, really good.

Here is the problem. It is someone else or some artificial intelligence algorithm that has inordinate power to subjectively combine strategic data with strategic audiences to shape whatever thoughts and news they want. And I have equipped it, not even knowing it. And that process could apply to anyone or anything. There is the danger. It could be the President of the United States, it could be their kids, it could be a company, it could be a political party, it could be a news outlet. Anything could be targeted for that selective viral spread of just some information.

Mr. Chew, this may be genius, but that doesn't make it fair, it doesn't make it good, and it doesn't make it accountable. I wouldn't want my government to have that ability. I wouldn't want a company or a political party or my friend August here or my mother to have that capability. And I certainly don't want that to be accessible to anyone in China.

Now, there is no question it has got immense value. And as proof that, you are here, because this hasn't been a fun day. I know that. It hasn't been a fun day for us, either.

Artificial intelligence is difficult to manage once it is on autocruise control. And it is, as we have talked about, nearly impossible to wall off data. I know the idea, I know a little bit about databases, I know a little bit about corruption of those databases. It is very difficult to wall things off.

And unfortunately, there is this thing called human nature, where there's some dark components from time to time. There is always a temptation to monetize things or perhaps use some of these tools for nefarious purposes, and they can have absolutely devastating consequences.

So, Mr. Chew, I am going to wrap up my comments and just say that this is so attractive. TikTok poses as a Mr. Rogers' Neighborhood, but it acts like Big Brother. And that has got to stop.

Madam Chair, I yield back.

Mr. GRIFFITH. Will the gentleman yield?

Mrs. RODGERS. The gentleman yields back. Oh——

Mr. GRIFFITH. Will the gentleman yield?

Mr. FULCHER. The gentleman yields.

Mrs. RODGERS. Yield to Mr. Morgan Griffith.

Mr. GRIFFITH. I thank the gentleman for yielding.

Mr. Chew, earlier we had submitted into evidence the TikTok, ByteDance, and their ties to the Chinese Communist Party report that was filed as an exhibit last week with the Senate in Australia.

If you have any comment, I would like to get it on this paragraph out of their summary: "Our research confirms beyond any plausible doubt that TikTok is owned by ByteDance. ByteDance is a PRC company, and ByteDance is subject to all the influence, guidance, and de facto control to which the Chinese Communist Party now subjects all PRC technology companies. We show"—in this report—"how the CCP and the PRC state agencies together"—the party state—"have extended their ties into ByteDance to the point that

the company can no longer be accurately described as a private enterprise.‘‘

You keep calling it a private enterprise, but all the countries in the world are saying it is not a private enterprise, it is part of the Chinese Communist Party. What say you, sir? Yes or no, is it part of the Chinese Communist Party, as everybody thinks, or are you still living in some mystical world?

Mr. CHEW. I disagree with many conclusions——

Mr. GRIFFITH. So you are living in the mystical world.

I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes Ms.—the lady—gentlelady from Minnesota, Ms. Craig, for 5 minutes.

Ms. CRAIG. Well, thank you so much, Madam Chair, for yielding.

Mr. Chew, I am probably like a lot of parents who are also Members of Congress out here. I know a number of us—when you testified earlier today, you mentioned that the over-35 segment was a growing group of potential users, as if over 35 is old. And I realize that my own children think that I am ancient, our four boys.

But like a lot of us up here, we understand that there is some potential good. And of course, many of your influencers are doing what they are doing for all the right reasons. But one thing in your testimony you said a lot was ‘‘safety.‘‘ But as a mother and as a Member of Congress and as someone who is very concerned about drug use in our country, I was surprised that that didn't come up once in your testimony. No real reference to it here today. You know, I have raised my concerns in general about social media platforms serving as an illegal marketplace for drugs in prior Big Tech hearings. And I plan to continue that focus during today's hearing.

Mr. Chew, a March 8th, 2023 article in the Washington Post detailed the fact that TikTok has made little progress in combating the sale of illegal drugs on your platform. In fact, Colorado Attorney General Phil Weiser said that getting drugs on platforms like yours was nearly as convenient as using a phone to order a pizza or call an Uber. That same article mentions that law enforcement agencies have been frustrated by TikTok's lack of competition in the form of data sharing.

In my view, TikTok has taken little action in response to this crisis. According to a May 2022 blog post from TikTok, you donated $125,000 or 0.001 percent of your 2022 revenue to an antidrug effort on your platform in the form of ad credits. You also redirected #drugs, #fentanyl, and other obvious hashtags away from posts selling drugs to a community resources page, as if a teenager looking for drugs is going to look for them at #drugs.

Drug dealers have easily worked their way around this, using emojis and slang to communicate that they have drugs for sale. To this day it is possible for anyone to log into your platform and acquire drugs, and the consequences of that can be fatal.

What are you doing to move past these token efforts to prevent teenagers from accessing drugs on your platform?

Look, as parents up here today we not—we may not understand everything about your platform. I am not a tech guru. Many of us up here may not use exactly the right language, but we know when

our kids are at risk. And our kids are at risk on your platform. So what are you going to do to move past these previous token efforts?

Mr. CHEW. Congresswoman, we do take illegal drugs content on our platform very seriously. It violates our guidelines. We proactively identify and remove them. And as you pointed out, if anybody searches for any drugs on our platform, we do point them to resources to help them with that.

At the same time, we have also taken product changes. Like, for example, we don't allow our under-16 users to use the right messaging. And the reason is because, you know, we wanted to—that was a trade-off here. And we believe that, you know, it will protect these younger users better from getting contacts from people trying to push illegal activity.

So we will continue to work on it. Again, no company can be perfect at this. We are not saying we are——

Ms. CRAIG. Mr. Chew, I—with all due respect, the "no company can be perfect" line has been used way too much today.

I am going to reclaim my time. You know, clearly, in the 3-plus hours you have been before us today, what you are saying about Project Texas just doesn't pass the smell test. My constituents are concerned that TikTok and the Chinese Communist Party are controlling their data and seeing our own vulnerabilities.

If you are an American company, we could look at your 10–K, we could see who your shareholders are. The answer you provided earlier today, you would rather not tell us what your compensation is or how it is derived? Well, no American CEO would like to tell us that, but they have to because they are an American company. So what you are doing down in Texas, it is all well and good, but it is not enough for us to be convinced that our privacy is not at risk.

So how can you say that you are protecting American users' privacy with the CCP being so heavily involved with ByteDance? It is not possible. China won't even carry your product. How is it that you can convince us that our privacy is not at risk and, more than that, our kids' privacy is not at risk in this country?

Mr. CHEW. In my opening statement——

Mrs. RODGERS. The gentlelady's time has expired.

Ms. CRAIG. Thank you, Madam Chair.

Mrs. RODGERS. The gentlelady's time has expired. We are going to have to continue on. The gentleman from Georgia, Mr. Allen, is recognized for 5 minutes.

Mr. ALLEN. Thank you, Madam Chair, and thank you, Mr. Chew, for being here today.

In September 2021 the Wall Street Journal published an article titled "How TikTok Serves Up Sex and Drug Videos to Minors." This article gives a chilling depiction of the types of content that TikTok's algorithm is curating for our children. This article claims that your application served an account that was registered as a 13-year-old "videos about drug use" referenced—it referenced to cocaine and meth addiction and promotional videos for online sales of drugs.

The algorithm was also found to have delivered countless videos depicting "pornography and other adult content" to the device of an account that was registered as a 13-year-old.

Could you please explain to the members of this committee and parents across the country why your company deems it acceptable for such inappropriate content to be prominently featured on a child's For You page?

Mr. CHEW. The—a lot of the content that you mentioned, Congressman, are violative of our own policies. And we don't think they are acceptable, and we remove them when we identify them. We take this very seriously. I mentioned this.

This is an industrywide challenge. We are investing as much as we can. We don't think it represents the majority of the users' experience on TikTok, but it does happen. Some bad actors try and come in and post some of this content, and we are doing our best to invest as much as we can to remove them.

Mr. ALLEN. Well, I would say you are not doing enough.

I have 14 grandchildren, Mr. Chew. Do you personally believe that such content is appropriate for minor children to consume?

Mr. CHEW. A lot of the content that you mentioned, like porn, for example, is not allowed on our platform. So no, I do not think they are acceptable for young people to consume.

Mr. ALLEN. Earlier this week, the Wall Street Journal published an article titled "TikTok's Chinese Partner Has Another Wildly Popular App in the U.S." This app is called CapCut. It is a video editing tool to help users go viral on TikTok. While for obvious reasons most of our attention is focused on TikTok and ByteDance, other companies and their applications are also continuing to exploit the privacy of Americans. TikTok, CapCut, Lark, FaceU, all of these apps are also controlled by ByteDance and pose serious privacy concerns.

In 2022, it was reported that TopBuzz, an international version of ByteDance-censored Chinese news app was used to spread pro-China messages to Americans. When it comes to the data privacy of Americans, we must have a clear set of guidelines to ensure Americans' data is protected and not passed along to unknown third-party actors who could pose a threat to our security.

I urge my colleagues to continue to work together to pass a national data privacy bill, not just one out of the House Energy and Commerce Committee but also through the House of this Congress. It is the only systematic way we can address privacy concerns. Unfortunately, I have been given no reason to believe that TikTok does not pose a threat, and cannot be trusted to follow our laws when they conflict with the desires of the Chinese Communist Party.

Your firewall that you are talking about, if you had a bad actor in your—what you call your Texas initiative—could get through that firewall and send any information that they wanted to send anywhere direct to the—into—directly to the Chinese Communist Party, would you deny that?

Mr. CHEW. Congressman, this risk that you talk about exists for every company. Bad actors——

Mr. ALLEN. I am talking about TikTok, sir.

Mr. CHEW. In fact, the risk is lower for us, because these——

Mr. ALLEN. It is a risk, correct?

Mr. CHEW. The personnel will be vetted.

Mr. ALLEN. Yes.

Mr. CHEW. So the risk is actually lower than most companies in the industry.

Mr. ALLEN. Well, that is why we have to deal with your company.

And with that, Madam Chair, I yield back.

Mrs. RODGERS. The gentleman yields back. The Chair recognizes the gentleman from California, Mr. Peters, for 5 minutes.

Mr. PETERS. Thank you, Madam Chair.

Mr. Chew, thanks for being here today. You know, your testimony discusses an effort your company has named Project Texas and the investments your company has made in creating a firewall between the United States user data and entities in China susceptible to influence by China's government.

And with your company's recent announcement by CFIUS—that CFIUS has instructed TikTok to separate itself from ByteDance or face a ban—TikTok's commitment to retaining this firewall is at a crossroads. So I want to ask you some questions about your company's long-term plans to ensure the safety and security of American data. And this, for me, is the crux of the concern for me about TikTok.

First of all, does the Chinese Government need to approve Project Texas for TikTok to agree to it?

Mr. CHEW. Congressman, we have designed Project Texas to move forward in the United States. This is something that we have described at length in the written testimony and in my opening statement: the firewall of American data stored on American soil by an American company overseen by American personnel. This is designed to move forward in the United States.

Mr. PETERS. But does the Chinese Government need to approve Project Texas for you to agree to it?

Mr. CHEW. We do not believe so.

Mr. PETERS. How is TikTok considering the future of Project Texas in the event of a sale or other ownership changes?

Are there elements of the Project Texas that TikTok would change prior to, or——

Mr. CHEW. I cannot speak on this hypothetical or on, you know, on potential, you know, owners who would—I cannot represent.

Mr. PETERS. OK. You don't know.

Mr. CHEW. I don't know, yes.

Mr. PETERS. Despite Project Texas' planned positive changes, it does include several broad exceptions that would allow large amounts of U.S. user data to routinely leave the country. I want to know a little bit more about these exceptions so I can understand whether Project Texas can live to—up to its promise of protecting Americans' user data.

I understand that, under Project Texas, business data and public data will be permitted to regularly leave the United States. Is that correct?

Mr. CHEW. Almost all the data is under the—that is not public is under the definition of protected data. This excepted data that you mentioned—I can get back to your team on this—is really for interoperability purposes, to make sure that the business can still operate and American users are still getting the benefit——

Mr. PETERS. Can you tell us what data—what date—where the data goes, and how it is used by the company?

Mr. CHEW. It will travel outside of the United States, but I can get back to you on the specifics.

Mr. PETERS. OK.

Mr. CHEW. It is data that doesn't—it cannot be used to identify users, you know, so it really is data that ensures the interoperability of the platform.

Mr. PETERS. And I understand that. I think we would want to have some understanding of how we would distinguish that by definition, and then also how it would be enforced.

Mr. CHEW. I can get back to you on those specifics.

Mr. PETERS. How is the U.S. data used to promote certain content back in the United States market, for instance?

Mr. CHEW. I am sorry?

Mr. PETERS. So what—you have—U.S. data feed the—all right.

How—can you discuss—when you discuss where the data goes and how it is used by the company, how and at what points of data transfer does the U.S. data feed the PRC-developed algorithm used by TikTok?

How would the data that you are talking about——

Mr. CHEW. We—TikTok does not—is not available in mainland China.

Mr. PETERS. The PRC-developed algorithm used by TikTok, how does U.S. data get fed by that?

Mr. CHEW. The U.S.—the algorithm that leads to the U.S. app is in the Oracle Cloud infrastructure, and is trained by U.S. and global data. Again, TikTok does not—is not available in mainland China.

Mr. PETERS. How can we trust that these exceptions for Project Texas won't be used abused by China's government or by foreign adversaries?

Mr. CHEW. We can—we—this is the fourth commitment, transparency, third-party monitors, including the definitions of these exceptions. And, you know, we can be very transparent on how they are used.

Mr. PETERS. OK. I guess—I guess my question will be, then—and if you want to get back to me in writing, that is fine, but how we would distinguish between the data for interoperability that you suggest needs to be shared with what data wouldn't be shared?

Mr. CHEW. It is—again, you know, it is—first of all, public data is not part of the protected data definition, because public data is what users want to share globally. So if you post a video and you want someone in France to see it, just by definition it has to leave the United States. Otherwise, the world cannot see it.

Now, there are certain aggregated and anonymized data sets that's useful for interoperability, for advertising, for example.

Mr. PETERS. Right.

Mr. CHEW. And that is part of what we are talking about.

Mr. PETERS. Right.

Mr. CHEW. I can get back to you on the specifics, but——

Mr. PETERS. I think we would also want to know how it is anonymized, and how—what oversight and enforcement we can count on.

Mr. CHEW. OK, I can get back to you on specifics.

Mr. PETERS. Thank you.

I yield back.

Mrs. RODGERS. The gentleman yields back. The gentleman from Texas, Mr. Pfluger, is recognized for 5 minutes.

Mr. PFLUGER. Thank you, Madam Chair.

Mr. Chew, I got to hand it to you. You have actually done something that in the last 3 to 4 years has not happened, except for the exception of maybe Vladimir Putin: you have unified Republicans and Democrats. And if only for a day, we are actually unified because we have serious concerns.

Do you—does TikTok support good? I mean, is TikTok a platform for good? Just yes or no.

Mr. CHEW. I believe, yes.

Mr. PFLUGER. OK. Does TikTok support freedom of speech?

Mr. CHEW. Yes. It is one of the commitments I have given this committee.

Mr. PFLUGER. Do you personally support the First Amendment?

Mr. CHEW. Congressman, I am here to talk about——

Mr. PFLUGER. As the CEO of TikTok.

Mr. CHEW. I am here to talk about TikTok.

Mr. PFLUGER. As the CEO of TikTok, do you support the——

Mr. CHEW. TikTok supports freedom of——

Mr. PFLUGER. Thank you. Does TikTok support genocide?

Mr. CHEW. Again, Congressman, I am here to talk about TikTok.

Mr. PFLUGER. Does TikTok support genocide? Does TikTok——

Mr. CHEW. No, but——

Mr. PFLUGER. OK.

Mr. CHEW. But——

Mr. PFLUGER. So—reclaiming my time, I am going to go to a video now, and it is from Enes Kanter Freedom. And I would like you to see Enes Kanter Freedom, who has spent his entire career post-NBA fighting against human rights violations within the Chinese Communist Party.

Go ahead and play this video, which highlights a situation that allegedly shows some human rights violations inside China. Please play.

[Video shown.]

Mr. PFLUGER. Mr. Chew, this was a video that was posted on TikTok by Enes Kanter Freedom. Are you familiar with this basketball player?

Mr. CHEW. I am not familiar with the specifics of this——

Mr. PFLUGER. Are you——

Mr. CHEW [continuing]. But I can tell you that——

Mr. PFLUGER. Are you familiar with the player Enes Kanter Freedom?

Mr. CHEW. Congressman, I am not——

Mr. PFLUGER. OK.

Mr. CHEW [continuing]. Familiar with this. You have—you just have to open TikTok and just search for this kind of content.

Mr. PFLUGER. OK.

Mr. CHEW. It really exists.

Mr. PFLUGER. I have read the moderation policy. Let me just quote what—you have talked about content moderation. TikTok has a moderation policy. Yes?

Mr. CHEW. We do have community guidelines that——

Mr. PFLUGER. One of the guidelines says, "material that in the sole judgment of TikTok is objectionable." Is this an example, banning Enes Kanter Freedom? Is that an example of objectionable material inside the Chinese Communist Party in mainland China?

Mr. CHEW. We do not take down content simply because it is critical of China.

Mr. PFLUGER. He was banned 1 week after this video.

Mr. CHEW. We do not do that. And I can check about the specific——

Mr. PFLUGER. If you need a note, go ahead.

Mr. CHEW. The note says he is not banned.

Mr. PFLUGER. His account was taken off 1 week after.

Mr. CHEW. Well, we can check on the specifics.

Mr. PFLUGER. We can check.

Mr. CHEW. Yes.

Mr. PFLUGER. So let's get to some other questions. Thank you for the slide.

Your privacy policy states that you collect a great array of data: keystroke patterns, app file names and types, sometimes approximate location, GPS location. Are keystroke patterns and rhythms part of TikTok gathering—the data that is gathered by TikTok?

Mr. CHEW. If you are talking, Congressman, specifically about keystrokes, you know, keystrokes, we do not engage in keystroke logging to monitor what the users say. It is to identify bots.

Mr. PFLUGER. OK.

Mr. CHEW. It is for security purposes. And this is a standard industry practice.

Mr. PFLUGER. You gather a lot of data, it is safe to say.

Mr. CHEW. We don't gather—we don't believe we gather more than any other social media company.

Mr. PFLUGER. TikTok gathers a lot of data, because your value proposition, as you sat in my office and told me, was to connect people to each other around the world. You told me this in my office. So you gather data on what they like and what they don't like, and then you show them things that they don't know they like, but eventually they may. You told me this.

Mr. CHEW. I think that is—I don't think that is what I said. What I said is that we connect people together, yes.

Mr. PFLUGER. Reclaiming——

Mr. CHEW. And that doesn't mean that we collect more data——

Mr. PFLUGER. Are you aware of any instances of TikTok distributing content from Chinese state media?

Mr. CHEW. I am sorry?

Mr. PFLUGER. Are you aware of any instances of TikTok distributing content from Chinese state media on the platform?

Mr. CHEW. We will label them clearly to—for our users to understand that.

Mr. PFLUGER. Do you disagree with FBI Director Wray and NSA Director Nakasone when they said that the CCP could have the ca-

pability to manipulate data and send it to the United States? Do you disagree with their statement?

Mr. CHEW. Their statement says "could."

Mr. PFLUGER. So do you disagree with that?

Mr. CHEW. No, I don't disagree with that.

Mr. PFLUGER. OK. So it is possible that the CCP, under the auspices of ByteDance, which is your parent company, which you get paid from, has the ability to manipulate content that is being shared with 130 million Americans. Yes?

Mr. CHEW. Congressman, I just want to make sure I am understanding all these questions.

I don't disagree with them, that there are data risks in general. That is what I meant.

Mr. PFLUGER. There is a big data risk, because——

Mr. CHEW. But on us, specifically——

Mr. PFLUGER. Are there engineers located inside mainland China that work on TikTok? Not Douyin, but TikTok.

Mr. CHEW. We are not the only company that has that.

Mr. PFLUGER. Are there engineers inside mainland China currently working on the algorithm for TikTok——

Mr. CHEW. Congressman, like I said——

Mr. PFLUGER [continuing]. As you told me in my office.

Mr. CHEW. There are other companies that—as I told you in your office, there are other companies that——

Mr. PFLUGER. I am going to reclaim my time.

Please rename your project. Texas is not the appropriate name. We stand for freedom and transparency, and we don't want your project.

I yield back.

Mrs. RODGERS. The gentleman yields back. The gentlelady from Tennessee is recognized for 5 minutes, Mrs. Harshbarger.

Mrs. HARSHBARGER. Thank you, Madam Chair, and thank you, Mr. Chew, for being here today.

Both President Trump and now President Biden have backed forcing TikTok to sell to an American company. However, the Chinese Communist Party has put export controls on algorithms ByteDance owns that power TikTok. And of course, this has created a gauntlet of regulatory hurdles in China and the U.S. that prevented the sale of TikTok.

Now, as a longtime business owner, I want to tell you, Mr. Chew, that waiting until your hands are forced will only drive down the price of your app. And right now, both your hands are tied, and you are going to have to make a decision about whether you choose freedom from the CCP or you continue to be an agent of the CCP.

And I will tell you why I say it that way. As a former member of Homeland Security, I point blank asked FBI Director Wray, "Is TikTok a national security threat?"

And without hesitation, sir, he looked at me and said, "Yes, Congresswoman, it is."

Now, how much data is ByteDance collecting through TikTok that is worth continuing to fight this regulatory gauntlet? You know, why not take the money and run, like any other company would do?

Mr. CHEW. Congresswoman, we built Project Texas in order to safeguard, and we listened to the concerns that have been raised, and we are building something that is unprecedented, that no other company is offering to protect U.S. user interests. And we believe it is rigorous and robust. And, you know, we are even offering third-party transparency and monitors to come in to verify this.

Frankly, I haven't heard any good reason why this doesn't work. I have heard a lot of rhetoric around this, but I haven't heard a good reason why it doesn't work.

Mrs. HARSHBARGER. Well——

Mr. CHEW. I look forward to these conversations, by the way, with you.

Mrs. HARSHBARGER. Absolutely. Well, let me go down this road.

When TikTok was unveiled to the public, its business model was solely based on generating revenue from advertising. Of course, ByteDance operated a separate app called Douyin for the Chinese marketplace. TikTok is embarking on becoming a so-called super app. In other words, it is a one-stop shop with everything you do, as Representative Fulcher said.

It is reported that TikTok's algorithms are so powerful that owner ByteDance has begun to license it to other companies. TikTok's recommendation engine drives usage on the platform, and this leads to promises of quick exposure and fame that leads to even more people joining. And when you sign up, TikTok starts collecting data about you, your location, your gender, your age, your facial data. The user never gets to the end of the content. And that is by design. And obviously, that makes you a lot of money.

Now, I know that the Chinese Communist Party is preventing ByteDance from selling TikTok due to export restrictions on the technology. And this causes me to question how are you going to power TikTok with your Oracle servers located in the U.S. with that Texas Project with ByteDance technology, if it can't leave China? How is that going to happen? I just want you to explain how it is going to happen.

Mr. CHEW. Congresswoman, the way that we design this is so that any piece of software that is impactful to the code, that enters, you know, that—some technical details around this will be reviewed by a third party or a few third-party monitors, just to make sure that we are all comfortable with the code.

I want to say this again: I don't know of any other company in my industry who is offering this level of transparency.

Mrs. HARSHBARGER. Well, why are there two different versions of apps, one in China and one in the United States?

Mr. CHEW. It is just a different business.

Mrs. HARSHBARGER. Well, I think we all know the reason that the Chinese get a different version, because ByteDance puts China first and America last.

And, you know, TikTok has—with everything we have heard today, sir, when you see 13-year-olds, 16-year-olds, you see the degradation that is happening to our youth and our society, you know, it is deceptive, and it is destructive comment, and it is comments, and the worst thing is that it is deliberate, sir. And that is not acceptable.

And with that, Chairwoman, I yield back.

Mrs. RODGERS. The gentlelady yields back. The gentlelady from Iowa, Mrs. Miller-Meeks, is recognized for 5 minutes.

Mrs. MILLER-MEEKS. Thank you, Madam Chair, and I would just like to thank our witness, Mr. Chew. Having been in the hot seat, so to speak, before, when I was in State Senate, I know how challenging this can be.

And thank you for your demeanor throughout all of this. But certainly, as you can see, in a bipartisan way we have concerns, and those concerns are valid.

And this is a yes-or-no question: Does TikTok track users' individual keystrokes?

Mr. CHEW. Only for security purposes, for—like, for example, like detecting bots. But we don't monitor what users say.

Mrs. MILLER-MEEKS. So the only purpose that you would monitor keystrokes is for security purposes.

Mr. CHEW. I can get back to you on more specifics, but this is not unlike what many other companies in the industry does.

Mrs. MILLER-MEEKS. So the keystroke monitoring does not go beyond what common industry practice in comparison to platforms like Facebook or Instagram use.

Mr. CHEW. Yes, I believe so.

Mrs. MILLER-MEEKS. OK. And does TikTok keep records of users' credit cards and passwords?

Mr. CHEW. I am not aware of that. You don't need that to log in. Of course, I can get back to you on specifics if you make a transaction on an e-commerce platform.

But regardless, all that U.S. data will be stored within the Project Texas firewall, you know, within the Oracle Cloud infrastructure, and overseen by American personnel.

Mrs. MILLER-MEEKS. So you would store credit card and password information?

Mr. CHEW. I need to check on the specifics. We are launching a pilot e-commerce plan, and we are making sure that the data is very secure within the Oracle Cloud infrastructure.

Mrs. MILLER-MEEKS. I think you have made a point of saying that your platform is not different than other platforms on social media and therefore are no more responsible than Facebook or Instagram or Twitter or the other social media platforms.

The concern, however, comes with where the technology is generated and whom it is owned by. And in the case of other companies, it is generated in the U.S., under U.S. guidelines, under U.S. privacy laws with certain parameters, versus generated through a parent company, ByteDance, which, as we know, is susceptible to the laws of the Chinese Communist Party, which has access to all of that data and information.

And I understand that TikTok has just reinstated Enes Kanter's account recently.

So our concern, and the question I have for you, is why would China or the Chinese Communist Party be opposed to a forced sale of TikTok?

Mr. CHEW. I cannot speak on behalf of the Chinese Government.

I can say that we designed Project Texas to take it forward here in the United States. And again, I believe it offers unprecedented protection for U.S. user data.

Mrs. HARSHBARGER. Yes, I think the problem is when there is a lack of transparency, then that leads people to believe that there is something more nefarious, and that there is in fact data that is captured, is stored, and poses a risk not only to children in the United States, but also poses a risk to national security.

With that, I yield the rest of my time to my colleague, Jay Obernolte.

Mr. OBERNOLTE. I thank the gentlelady from Iowa for yielding.

Mr. Chew, I would like to continue our discussion about Project Texas and the technical details about what you are proposing to do. So you are migrating all storage of U.S. user data to the Oracle Cloud infrastructure, and you think that that will be done by the end of the year. Was that right?

Mr. CHEW. Again, I can get back to you on the technical parts of it, the migration. Today, by default, all U.S.—new U.S. data is stored, by default——

Mr. OBERNOLTE. Sir, I am just using what you have said in your testimony in your opening here. So——

Mr. CHEW. It is stored there by default. What I said in my testimony is I am deleting legacy data.

Mr. OBERNOLTE. I see, OK.

Mr. CHEW. This is Virginia and Singapore. That is the difference.

Mr. OBERNOLTE. So who—when this migration is complete, who will have access to that data?

Mr. CHEW. Right now a team called TikTok U.S. Data Security, led by American personnel, they have access to that. We have begun these operations already.

Mr. OBERNOLTE. OK, but the app itself has access to the data, correct?

Mr. CHEW. Only through them. Any employees that have the data——

Mr. OBERNOLTE. Oh, no. What I mean is, like, if I lose my iPhone and I reinstall the app, and I put in my username and password, my app will reconnect to the mothership and download some of that data, my settings——

Mr. CHEW. That is not the way it works, no.

Mr. OBERNOLTE. It is not?

Mr. CHEW. That is not the way it works. It will go through the Oracle Cloud infrastructure, and that team——

Mr. OBERNOLTE. No, no. Yes, I realize that. So let me ask you this: What would prevent them, someone with detailed technical knowledge of the way the app is constructed, from creating an almost identical version of the app that could also access that data?

Mr. CHEW. That is—we are giving you third-party monitors and transparency——

Mr. OBERNOLTE. Yes, but they are monitoring the source code for your app. I mean, ByteDance, these engineers, have been working on this app for years. What would prevent them from making an app that could also access that data?

Mr. CHEW. Congressman, I think we are going into the area where, you know, what if there is a hacker, what if there is this.

Mr. OBERNOLTE. OK.

Mr. CHEW. You know, this is a common industry problem, as you know.

Mr. OBERNOLTE. Yes. But, well, I mean, it is just—I see my time is expired. It illustrates the point——

Mrs. RODGERS. OK——

Mr. OBERNOLTE [continuing]. I am just skeptical that you are technically able to do——

Mrs. RODGERS. The gentleman's time has expired.

Mr. OBERNOLTE [continuing]. What you promised.

Mrs. RODGERS. The gentlelady's time has expired.

Mr. Chew, I recognize that we have run over. I appreciate your time. We have just a few Members left and would appreciate the chance for them to get to answer—or ask their 5 minutes' worth of questions.

The gentleman from Virginia, Mr. Griffith, is recognized for 5 minutes.

Mr. GRIFFITH. Thank you very much, Madam Chair.

Mr. Chew, you share legal counsel lawyers with ByteDance, yes or no?

Mr. CHEW. Yes, we do.

Mr. GRIFFITH. And you testified that you prepared extensively with your legal team for this hearing, yes or no?

Mr. CHEW. With my team in DC, including the——

Mr. GRIFFITH. Including some of your legal counsel.

Mr. CHEW. Yes.

Mr. GRIFFITH. Right. And did they tell you about the report to the Australian Senate of March 14th that I referenced earlier? Did they tell you that that report was out there? Yes or no.

Mr. CHEW. I cannot recall how I found out about the report.

Mr. GRIFFITH. But you know about the report. OK.

Mr. CHEW. I can check, and—yes.

Mr. GRIFFITH. And did they tell you to favorably cite the Citizens Lab in your written testimony today, yes or no?

Mr. CHEW. Congressman, I need to get back to you on specifics——

Mr. GRIFFITH. They helped you with the preparation of your written statement, though, didn't they?

Mr. CHEW. A team prepares, yes.

Mr. GRIFFITH. Yes. And did they tell you that the director of Citizen Labs says he has called out your company for misrepresenting their report repeatedly, and has—and did so as late as yesterday? Did they tell you about that? Yes or no.

Mr. CHEW. Congressman, the Citizen Lab is saying they cannot prove a negative, which is what I have been trying to do for the last 4 hours.

Mr. GRIFFITH. All right. But you cited it favorably as saying that it did positive things for you.

That being said, let me ask you this. You keep talking about transparency, but you haven't been transparent with us here today. You were asked earlier by Mr. Hudson if you own stock in ByteDance. You said you didn't want to reveal that. Well, we are trying to figure out what the ties are between ByteDance and TikTok. I am not going to ask you how many shares you own, but do you own shares in ByteDance, sir?

Mr. CHEW. Yes, I do.

Mr. GRIFFITH. All right. There you go. How about in TikTok?

Mr. CHEW. Right now all employees own shares in one——

Mr. GRIFFITH. Yes, sure. I expected that. I just don't understand why you didn't tell Mr. Hudson that, and were transparent earlier. Instead, you made us drag it out of you.

All right. Now let's talk about the kids. You told several of our folks that there was a 60-minute deadline. You also told us that, if you were under the age of 18, you couldn't access the live section, the live option. So I texted my 17-year-old and my 15-year-old, and I basically got scoffs back—scoffs—when I said, "Are you all limited to 60 minutes?"

My older son said, "Well, there is a notice I get from time to time that says I shouldn't be on more than 60 minutes, but it never has kicked me off."

And my younger son said, "Oh, I am on as long as I want to be."

So I am just informing you whoever told you, particularly if it was your legal team, that that is not accurate, that they are on for more than 60 minutes, and they can access the live section. I believe it was Mr. Carter that you said they couldn't, under 18, access the live—you know, being on the live section. He has done it. So whatever it is you think you are doing, it ain't getting done.

Now, let's talk about the law for a minute. You share a legal team, but you keep talking about how you got a firewall between you and ByteDance. You can't have an effective firewall under the United States interpretation of such if you are sharing legal counsel, because anything that you say to your legal counsel, they can share internally. If you have got the same lawyers—now, maybe you have two different teams of lawyers in the law firm, but that is not what you said to us today. You said you share lawyers. There is no firewall, legally. I am just telling you.

So if you want to clean it up and be transparent, you need to do something about that. Wouldn't you agree, yes or no——

Mr. CHEW. Congressman——

Mr. GRIFFITH [continuing]. That you need to do something about that?

Mr. CHEW. Congressman, I——

Mr. GRIFFITH. You will look into it.

Mr. CHEW. Yes.

Mr. GRIFFITH. You will look into it. You have been looking into it all the time.

All right. You told Dr. Burgess, when asked if your employees—if your employees who were members of the Chinese Communist Party had access to TikTok data from the U.S., you said you didn't know who was a member of the Communist Party. But then Congressman—to Congressman Walberg you said that the CEO of TikTok was not a member of the Communist—the Chinese Communist Party. And to Congressman Kelly you said the founder of TikTok was not a member of the Communist Chinese Party.

Sir, either you know who is and isn't a member of the Chinese Communist Party or you don't. Which one is it? I submit that you know, and you just aren't giving us the straight story. Clearly you know, but you denied that to Dr. Burgess.

Mr. CHEW. Congressman, I can ask one or two people, but we have no policy to ask all the employees. I can ask one or two people, but I—you know, who are in——

Mr. GRIFFITH. But it is reasonable to assume that, with a significant number of members of the country of China being members of the Chinese Communist Party, logic would tell us—you are a logical man, I assume—logic would tell us that there are a fair number of your employees who are members of the Chinese Communist Party, at least a dozen or so, who have access to this data. Isn't that so?

Mr. CHEW. Again, like I said, I can ask one or two people. We don't have a policy to ask everybody.

Mr. GRIFFITH. I said earlier you are living in some kind of a cloud world, because either you know or you don't know.

I yield back. Thank you, ma'am.

Mrs. RODGERS. The gentleman from South Carolina the Chair recognizes for 5 minutes, Mr. Duncan.

Mr. DUNCAN. Thank you, Madam Chair. I think it has been revealed today there is not a degree of separation between ByteDance and TikTok.

I would like to enter in the record a Heritage Foundation document, "TikTok Generation: a CCP Official in Every Pocket."

Mrs. RODGERS. Without objection, so ordered.

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

Mr. DUNCAN. And I would like to yield the balance of my time to Kelly Armstrong from North Dakota.

Mr. ARMSTRONG. Thank you, Madam Chair.

Mr. Chew, the TikTok Privacy Policy details extensive data collection on users. One line states that "we may collect information about you from other publicly available sources." What publicly available data is TikTok collecting and adding to the profiles of users?

Mr. CHEW. It will be publicly available, but I can get back to you on specifics.

Mr. ARMSTRONG. OK. What is the purpose of obtaining even more data on your users beyond the data collected from the platform?

Mr. CHEW. We collect data—we want to give our users, by the way, a lot of transparency on what data we collect. We give them choices on the controls of their own privacy settings, and it really is to serve them a better experience. This is the reason why so many people love the app. It is a great experience.

Mr. ARMSTRONG. So how does the non-TikTok-related data service relate to the service provided?

Mr. CHEW. I need to check the specifics and understand the question, and get back to you.

Mr. ARMSTRONG. OK. Do you think the average TikTok user knows that you are—and understands that TikTok's data collection extends to information outside the use of the app?

Mr. CHEW. We do give transparent information on this. And like I said, we—I—we don't—I don't believe we collect more information than most other social media platforms out there.

Mr. ARMSTRONG. Well, and the reason I ask this—because I am going to go back into the corporate structure. You described that TikTok is a subsidiary of ByteDance. Mr. Griffith just said that you guys share the same lawyers. You have stated that your direct report is the CEO of ByteDance. But you have also stated that, at

certain levels, TikTok operates without direct daily control from ByteDance. You have used content moderation as an example for that.

TikTok's privacy policy states that you may share user data within your corporate group. Does that corporate group include ByteDance?

Mr. CHEW. If you are talking about that one entity that has the share for the—for Chinese media licensing purposes, I think it is called Beijing Douyin Services. If you are talking about that entity, of the government share, the answer is, you know, we have cut off, you know, all access of U.S. data sets to that.

Mr. ARMSTRONG. So——

Mr. CHEW. Employees of the entity.

Mr. ARMSTRONG. But your user privacy—so your corporate—ByteDance is part of your corporate group.

Mr. CHEW. ByteDance is the top company.

Mr. ARMSTRONG. So——

Mr. CHEW. So, yes, you are talking about the other entities within the group.

Mr. ARMSTRONG. So you just testified that you firewalled this. Does that statement—so you are saying the TikTok's executives you—that operate independently of ByteDance, but does that statement not hold for sharing of access to data?

Mr. CHEW. Well, I was talking about that one entity that has—that many of you have raised some concerns, you know. That is the entity that I am talking about, the entity with the Chinese Government's investment that has—that is for the purpose of Chinese Internet licensing for the Chinese business——

Mr. ARMSTRONG. Let me ask it a different way: What other entities have access to TikTok user data?

Mr. CHEW. Well, after Project Texas, we are going to move it so that only TikTok user data security has controlled access of that data.

Mr. ARMSTRONG. OK. So—and we could bring you back either—and after Project Texas is done. But right now, what other entities have access to TikTok's user data today?

Mr. CHEW. Only by requirement. It is really only by requirement. Certain employees may use—may need—require some access of data to help build the product.

But for U.S., you know, we have moved it from Project Texas, and by the end of this year it will be firewalled away.

Mr. ARMSTRONG. But this is your privacy policy today. Like, I understand what you are telling us, what is potentially going to happen in the future. I have concerns again about CFIUS and government involvement, private organization, all of that. I am just saying this is your user agreement today.

So your user agreement says that you share access with your corporate group.

Mr. CHEW. You know——

Mr. ARMSTRONG. You are telling me what is going to happen whenever Project Texas gets done. I am asking you today. Who has access to TikTok's user data?

Mr. CHEW. In our user agreement, Congressman, in our privacy policy, we also added a link so that our users in the U.S. can be informed about Project Texas. The link is there.

Mr. ARMSTRONG. So the link is there to private—but—I understand what you are trying to do moving forward. I have my own concerns about that. But we are sitting here today in a hearing, and your privacy policy is different than your testimony. Your privacy policy specifically says that you can share user data within your corporate group.

So you are saying, even though your privacy policy says that, you are not doing it?

Mr. CHEW. Like I said, no, I don't think there is any contradiction here. Like I said, Project Texas, when it is done, we firewall off that data. We still have some legacy data in Virginia and Singapore that we started deleting, and we will be done by the end of this year.

Mr. ARMSTRONG. So at the end of this year, then you won't share it. Does that mean you are sharing it today?

Mr. CHEW. I don't believe so, but there is some——

Mr. ARMSTRONG. Then why haven't you changed your privacy policy? Why haven't you updated it?

Mr. CHEW. We did update it, and we gave our users more information on Project Texas. We did update it.

[Pause.]

Mrs. RODGERS. The gentleman yields back. The gentleman from Texas the Chair recognizes for 5 minutes, Mr. Crenshaw.

Mr. CRENSHAW. Thank you, Madam Chair.

Thank you, Mr. Chew, for bringing Republicans and Democrats together. I appreciate that.

I want to get right to the critical point of concern. So TikTok is able to collect massive amounts of personal data. We all know that. That means it could, if it desired to, use this data to influence narratives and trends, create misinformation campaigns, encourage self-destructive behavior, purposefully allow drug cartels to communicate freely and organize human and drug trafficking.

Now, to be fair, all social media companies could do that. But here is the difference. It is only TikTok that is controlled by the Chinese Communist Party. All these other social media companies are not. Mr. Chew, do you agree that TikTok is controlled by the CCP?

Mr. CHEW. No.

Mr. CRENSHAW. OK, I thought you would say that. I disagree, as you thought I might say.

Here is why I disagree: Your parent company is ByteDance, right?

Mr. CHEW. That is correct.

Mr. CRENSHAW. It is correct. So, many of the workers who work at ByteDance are Communist Party members, right?

Mr. CHEW. I wouldn't know.

Mr. CRENSHAW. Well, I think, for example, the chief editor at ByteDance, Zhang Fuping, is the Communist Party's secretary. Correct?

Mr. CHEW. He works on the Chinese business, not on TikTok.

Mr. CRENSHAW. Right. He works for ByteDance, the parent company.

Mr. CHEW. He works on the Chinese business.

Mr. CRENSHAW. Right, the parent company of TikTok.

Mr. CHEW. The Chinese business is called Douyin.

Mr. CRENSHAW. Yes, but it is all associated with ByteDance, right?

Mr. CHEW. So ByteDance owns a number of businesses.

Mr. CRENSHAW. Right. You all report to ByteDance. Everybody is part of ByteDance. OK? And do you know of any other employees that work for ByteDance that are part of the Chinese Communist Party?

Mr. CHEW. Like I said, you know, there are—ByteDance has—owns Chinese businesses, and they operate in China.

Mr. CRENSHAW. You don't know how many, but you acknowledge many must be card-carrying members of the CCP, right?

Mr. CHEW. In the Chinese business, yes.

Mr. CRENSHAW. Yes. I mean, the CCP holds a—what is called a golden share in ByteDance that allows the CCP to control one board seat in ByteDance. That is public——

Mr. CHEW. That is not correct.

Mr. CRENSHAW. It is not correct?

Mr. CHEW. No, it is——

Mr. CRENSHAW. It is publicly reported. They admitted to it.

Mr. CHEW. It is—on our website we have updated it, so we have—can give people more transparent information on this.

They have a share in a subsidiary that is only for the Chinese business. It has nothing to do with TikTok, and it is for the purposes of content licensing in China.

Mr. CRENSHAW. So there is not an internal CCP committee, which is a regular thing that happens in China, they have a CCP committee internally inside the company.

Mr. CHEW. I run TikTok. I cannot represent the Chinese business.

Mr. CRENSHAW. ByteDance, I am talking about ByteDance. No arrangement in ByteDance?

Mr. CHEW. Again——

Mr. CRENSHAW. Here is the main point of concern. China's 2017 national intelligence law states very clearly that "any organization or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work."

In other words, ByteDance, and also your TikTok employees that live in China, they must cooperate with Chinese intelligence whenever they are called upon. And if they are called upon, they are bound to secrecy. That would include you. So, Mr. Chew, if the CCP tells ByteDance to turn over all data that TikTok has collected inside the U.S., even within Project Texas, do they have to do so, according to Chinese law?

Mr. CHEW. Congressman, first, I am Singaporean.

Mr. CRENSHAW. That is fine. But there are employees of yours, and ByteDance is in China.

Mr. CHEW. We understand this concern. In my opening statement we said we hear these concerns. We didn't try to avoid them

or, you know, trivialize them. We built something where we take that data and put it out of reach. This is what we did. We put it out of reach.

Mr. CRENSHAW. Out of reach. But they own you.

Mr. CHEW. No, we put it out of reach by storing them——

Mr. CRENSHAW. ByteDance owns TikTok. If ByteDance is—and the CCP owns ByteDance, because the CCP owns everybody in China.

Mr. CHEW. Well——

Mr. CRENSHAW. And so, by law, they can make them do whatever they want, and they say that, by law, you can't tell anyone about it. So they can make you hand over that data. Is that correct?

Mr. CHEW. That data is stored here, in American soil, by an American company——

Mr. CRENSHAW. Well, you say that. We——

Mr. CHEW [continuing]. Overseen by American——

Mr. CRENSHAW. We thought that, but leaked audio from 80 internal TikTok meetings shows that U.S. user data has been repeatedly accessed from China when you said it hasn't been.

And here is the other thing. Following back on my colleague's line of questioning, in your own privacy policy it says that you may share information within your so-called corporate group. Is ByteDance part of that corporate group?

Mr. CHEW. If you are talking about the share of the entity with the share, like I shared with the previous——

Mr. CRENSHAW. Is ByteDance part of the corporate group?

Mr. CHEW. ByteDance is a holding company. It is part of the corporate group, yes.

Mr. CRENSHAW. It is part of the corporate group.

Mr. CHEW. Yes.

Mr. CRENSHAW. OK. So your own privacy policy says you have to share data with ByteDance. And if the CCP says, "Hey, ByteDance, you are going to do what we say, and you can't tell anyone about it" because by law, according to that 2017 national intelligence law, they have to do it, that is our concern.

Mr. CHEW. This——

Mr. CRENSHAW. Maybe you haven't done it yet, but my point is that you might have to. And that is where our concerns come from.

I mean, over 300 TikTok employees have worked for China's state-run propaganda media. That is just from looking at their LinkedIn profiles. OK?

So here—and my last point is this. I want to say this to all the teenagers out there and TikTok influencers who think we are just old and out of touch and don't know what we are talking about, trying to take away your favorite app. You may not care that your data is being accessed now, but it will be one day when you do care about it.

And here is the real problem: With data comes power. They can choose what you see and how you see it. They can make you believe things that are not true. They can encourage you to engage in behavior that will destroy your life. Even if it is not happening yet, it could in the future.

The long-term goal of the Chinese Communist Party is the demise of the American power, and that starts with our youth. At any

moment they could demand that all of TikTok's data be used to design an AI algorithm with the sole purpose of promoting Chinese interests and destroying our society from within. You want to know why that is Democrat—why that is—why Democrats and Republicans have come together on this? That is why we are so concerned.

Thank you, and I yield back.

Mrs. RODGERS. The gentleman yields back.

I remind the Members they have 10 business days to submit questions for the record, and I ask our witness to respond to the questions promptly.

Pursuant to committee rules, I ask unanimous consent to enter the documents from the staff list into the record.

Without objection, so ordered.

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

Mrs. RODGERS. Members should submit their questions by the close of business on April 6th.

Without objection, the committee is adjourned.

[Whereupon, at 3:23 p.m., the hearing was adjourned.]

[Material submitted for inclusion in the record follows:]

The Washington Post
Democracy Dies in Darkness

EXCLUSIVE

A former TikTok employee tells Congress the app is lying about Chinese spying

His claims of data-security flaws, which the company disputes, underscore how seriously Congress has begun taking the wildly popular short-video app with more than 100 million users nationwide.

By Drew Harwell

Updated March 10, 2023 at 11:33 a.m. EST | Published March 10, 2023 at 6:30 a.m. EST

A former risk manager at TikTok has met with congressional investigators to share his concerns that the company's plan for protecting United States user data is deeply flawed, pointing to evidence that could inflame lawmakers' suspicion of the app at a moment when many are considering a nationwide ban.

In an exclusive interview with The Washington Post, the former employee, who worked for six months in the company's Trust and Safety division ending in early 2022, said the issues could leave data from TikTok's more than 100 million U.S. users exposed to China-based employees of its parent company ByteDance, even as the company races to implement new safety rules walling off domestic user information.

His allegations threaten to undermine this $1.5 billion restructuring plan, known as Project Texas, which TikTok has promoted widely in Washington as a way to neutralize the risk of data theft or misuse by the Chinese government.

They could also fuel speculation that the wildly popular short-video app remains vulnerable to having its video-recommendation algorithm and user data distorted for propaganda or espionage. Authorities in the United States have not shared evidence that the Chinese government has accessed TikTok's data or code.

TikTok and ByteDance officials have since 2019 been negotiating with a group of federal officials, known as the Committee on Foreign Investment in the United States, about which privacy standards and technical safeguards they'd need to adopt to satisfy U.S. national-security concerns. The company finalized its proposal in August and presented it to CFIUS, but it has yet to be approved, and CFIUS officials have declined to explain why.

The former employee, who spoke on the condition of anonymity because of fear of retaliation, has told congressional investigators that Project Texas does not go far enough and that a truly leakproof arrangement for Americans' data would require a "complete re-engineering" of how TikTok is run.

As one piece of evidence, he shared with The Post a snippet of code he said showed that TikTok could connect with systems linked to Toutiao, a popular Chinese news app run by ByteDance. That connection, he said, could allow for surreptitious interference in the flow of U.S. data.

TikTok officials said the former employee has misconstrued the plan and that his termination, months before it was finalized, means he "would have no knowledge of the current status of Project Texas and the many significant milestones the initiative has reached over the last year."

His Toutiao allegation was "unfounded," they said, and the code snippet he shared did not indicate any correlation or connectivity between the two apps. The Toutiao code, they said, does not link back to China and is "nothing more than a naming convention and technical relic" harking back to ByteDance's first successful app.

Officials also said they have already adopted one key pledge of Project Texas by moving U.S. user data and other critical code to servers run by the American tech giant Oracle — a move, they said, that would further undermine the claim that Toutiao officials could have any influence on TikTok's U.S. content or operations.

The former employee's ability to secure meetings with key senators' staff reinforces the expansiveness of Washington's interest in a youth-beloved app best known for its viral dances and challenges. TikTok's chief executive Shou Zi Chew probably will be grilled on Project Texas and the possibility of Chinese influence during a congressional hearing later this month.

His visits in Washington are also timed to accelerating concern about TikTok, including two recent legislative pushes that could lead to an unprecedented nationwide app ban. The former employee said he had met with staff in the offices of Sens. Charles E. Grassley (R-Iowa) and Mark R. Warner (D-Va.). Representatives from both offices confirmed the meetings but declined further comment.

Sen. Warner and a bipartisan group of senators on Tuesday proposed a bill that would give the Commerce Department a direct path to banning TikTok and other apps with foreign owners following a "risk-based" assessment. Another bill advanced by the House Foreign Affairs Committee last week would let President Biden ban TikTok outright.

The White House said Wednesday it supported Warner's bill but was also waiting for the CFIUS negotiations to conclude. More than two dozen states have passed measures banning TikTok on government-owned devices, but a 2020 federal court ruling — and a growing group of civil-liberties activists and congressional Democrats — have argued that a nationwide ban would violate Americans' First Amendment protections against any government law limiting freedom of speech.

The former employee worked as head of a unit within TikTok's Safety Operations team, which oversaw technical risk management and compliance issues, including which employees had access to company tools and user data, according to documents he shared with The Post.

He argues that a nationwide ban would be unnecessary to resolve the technical concerns, which he said could be fixed with "doable and feasible" solutions that would go beyond Project Texas's protocols. He said he worked to address the data-privacy issues internally but was fired after raising his concerns.

In a December letter to TikTok's CEO, Chew, which he shared with The Post, the former employee wrote that senior managers were "responsible for the internal fraud pertaining to implementation of Project Texas," which he said involved them "intentionally lying" to U.S. government officials about how its controls had been tested and verified.

"Various TikTok executives were unduly pressuring me to sign off on Project Texas as if it was something accomplished [a] long time ago," he wrote. He demanded a "rapid internal investigation to ensure true risk management and my reinstatement."

ByteDance's head of global legal compliance acknowledged receiving his letter of concerns and said the company would "review them with expediency," according to a copy of the email reviewed by The Post. The company, he said, has not offered any updates since.

The former employee said he has not yet filed an official whistleblower complaint with the SEC, and his claims have not been corroborated by an official investigation.

He said he is also separate from an alleged whistleblower referenced in a Tuesday letter that Sen. Josh Hawley (R-Mo.) sent to the Treasury Department, first reported by Axios. That person said TikTok's data-access controls were "superficial" and that China-based engineers could use tools to access U.S. data with "the click of a button," wrote Hawley, one of TikTok's biggest critics in Congress. Those claims have also not been verified.

TikTok officials said in a statement Wednesday that the "analytic tools" did not grant direct access to data and that protected U.S. information is now stored on Oracle servers where it can be accessed only in "limited, monitored circumstances."

Project Texas would wall off TikTok's U.S. operations into a new subsidiary, TikTok U.S. Data Security, whose leaders would be vetted by the U.S. government and report to CFIUS, according to briefings the company has given to researchers, journalists and members of Congress.

All U.S. user data would be siloed in a system with monitored gateways for authorized use, according to the plan, and TikTok's code and recommendation algorithms would be reviewed by engineers from Oracle, who could alert U.S. regulators to possible concerns.

Some briefed on the plan have commended its rigor, including Samm Sacks, a senior fellow at Yale Law School's Paul Tsai China Center, who said it reflected a serious effort that would give the U.S. government an unprecedented level of supervision and control into how the company works.

"If it's not working, if there's data leakage or content that's problematic, TikTok would be subject to more oversight than any social media company operating in the U.S.," she said.

But skeptics have argued that no technical safeguard can protect from ByteDance's ownership, which they say could pressure TikTok managers to censor inconvenient topics, boost pro-government messages or introduce vulnerabilities through lines of code. TikTok employees told The Post last year that ByteDance teams in Beijing worked on design, engineering and software tools that they relied on for daily operations.

If Project Texas is rejected, some members of Congress have argued that the only solution would be to force ByteDance to sell TikTok to an American buyer — an idea, first floated by the Trump administration, that TikTok's supporters have compared to hostage-taking. Government authorities in Beijing used export laws to block the Trump proposal in 2020 and could do so again.

TikTok can collect a large range of user data, including video viewing histories, email addresses and contacts, though American tech giants such as Facebook and Google gather even more, including precise GPS locations, extensive biographical details and web-browsing histories, according to a Post review last month.

Chinese government authorities can, by law, compel tech companies to hand over user data to support "national intelligence" work. TikTok has argued that Americans' information would not be subject to that law because it is stored in servers in the U.S. and Singapore.

Critics of a ban have argued it would violate Americans' free-speech rights and fail to address the bigger need for a national law restricting how personal data is collected by all apps, not just TikTok. The digital rights group Fight for the Future said in a statement last month that the ban proposal amounted to "xenophobic showboating that does exactly nothing to protect anyone."

The former employee's claims match those from a source who shared hours of internal meeting recordings, first reported by BuzzFeed last year, in which company employees said they were working to close up ways in which U.S. data could be accessed by employees in China, in line with their CFIUS proposal.

Following that report, an internal ByteDance team used TikTok data such as users' IP addresses, which offer a general estimate of their location, in an attempt to identify how company information had been leaked. The attempt failed, according to ByteDance officials, who announced the attempt in December and said the four employees involved in the effort had been fired.

Chew, who met with The Post last month during a cross-Washington charm offensive, said the company was restructuring its internal-audit team and working to explain its safety controls to skeptical lawmakers and regulators. The scandal, he said, threatened to "erode all the work that we have done."

The Heritage Foundation

BACKGROUNDER
No. 3757 | MARCH 22, 2023
TECHNOLOGY POLICY CENTER

TikTok Generation: A CCP Official in Every Pocket

Kara Frederick

KEY TAKEAWAYS

TikTok's data exploitation practices, privacy abuses, influence operations, and promotion of social contagions leave Americans vulnerable to the CCP.

Given the current threat environment, a wholesale ban of TikTok's operations in the U.S. is the only viable option to protect the United States and Americans.

A systemic, risk framework applied to foreign-owned platforms will prevent another TikTok from infiltrating America.

Three hundred billion dollars, three billion downloads, and at least 90 minutes of attention per user every day—TikTok and its China-based parent company have captured much of the world in more ways than one.[1] Yet today's most popular social media app poses a distinct threat to American citizens. From logging keystrokes to laundering pro–Chinese Communist Party (CCP) narratives to U.S. audiences, TikTok—via its Beijing-based parent company ByteDance—exposes Americans to a host of abuses by the Chinese government.

TikTok's data-collection and exploitation practices, abuses of privacy, propagation of influence operations, and promotion of social contagions that rend America's social fabric require immediate attention from policymakers. If America is to preserve her

self-governing republic, especially in the psyches of the next generation, dealing with TikTok and successor platforms is both a strategic and moral imperative.

TikTok and the CCP

TikTok's parent company, ByteDance, is subject to the People's Republic of China's (PRC) laws and policies that permit the CCP's access to the data ByteDance collects. One such policy is China's 2017 National Intelligence Law, which compels private entities and individuals to cooperate with "state intelligence work."[2] Specifically, Article 7 of this law declares that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to the law."[3]

Beyond this, Chinese officials—former and current—are embedded in TikTok's parent company and involved in the company's inner workings.[4] In April 2021, the Chinese government acquired a 1 percent stake in ByteDance's main domestic subsidiary and the board seat that came along with it. This action makes at least one of the three board members, Wu Shugang, a card-carrying official of the Chinese government.[5] Further, a U.S. Department of Justice filing against TikTok assessed in September 2020 that "ByteDance contains an internal corporate CCP committee through which the CCP exercises influence at the company."[6] At lower levels, an August 2022 *Forbes* review found more than 300 LinkedIn profiles of current TikTok and ByteDance employees with ties to the Chinese state media apparatus.[7] Fifteen of these profiles indicate that these professionals are both employed by ByteDance and official Chinese propaganda arms at the same time.[8]

In fact, TikTok's ties to the CCP via ByteDance are so deep that TikTok's public relations strategy from leaked documents published by *Gizmodo* in July 2022 in a document titled, "TikTok Master Messaging," include imperatives to "[d]ownplay the parent company ByteDance, downplay the China association," as two of the first four exhortations on the list.[9]

TikTok's Data Privacy and Collection Methods

While a number of private American platforms engage in controversial data-collection and tracking practices, TikTok's CCP links intensify debates over privacy invasion. Given its influence over the app, the CCP would likely encourage more collection, not less. And while the commercial surveillance practices of many American

companies are exploitative, direct comparisons do not account for the differences in corporate governance between American and Chinese companies as well as the stark contrasts between U.S. and Chinese political systems. America—though under internal pressure—retains a relatively open society, free press, engaged citizenry, and independent judiciary to hold both the U.S. government and private companies accountable for their data-collection practices.[10] China does not have a remotely comparable approach.

As of today, TikTok's invasive data-collection practices include gathering users' Global Positioning System (GPS) locations, Internet protocol (IP) addresses, content, contacts, images, microphone access (for "voiceprints"), and other biometric, personally identifiable, or device information.[11] Its 2023 Privacy Policy also includes admissions that TikTok collects the mobile carriers, time zone settings, models, networks, device identifiers, screen resolution, operating systems, app and file names and types, along with keystroke patterns or rhythms of its users.[12]

In terms of comparative data-collection practices to other platforms, a February 2023 report by cybersecurity company Internet 2.0 alleges that TikTok's data-collection behaviors are among the worst in the industry.[13] For example, TikTok's Malcore (malware analysis tool) score was 63.1 out of 100, the highest and worst score of the more than 20 digital applications it tested. The average application's score was 28.8, with no other app ranking as poorly in terms of data privacy and security as TikTok. According to the report, TikTok's performance was due, in part, to the security vulnerabilities in TikTok's code and the abundance of data trackers riddling the platform.[14]

Particularly troubling is the extent to which TikTok conceals atypical elements of its collection practices. In August 2020, *The Wall Street Journal* revealed that TikTok exploited a loophole in Google's Android operating system that allowed it to track the media access control (MAC) addresses (the unique device identifiers) of its users for at least 15 months. When TikTok was first installed on a new device over that time period, the company reportedly bundled these identifiers and other device data to send to parent company ByteDance.[15] During the 15-month period, TikTok reportedly took steps to cover its tracks and conceal its exploitation of this loophole via a layer of encryption.[16] TikTok also reportedly accessed user clipboards on Apple's mobile operating system for a time, reading the clipboard in every instance the app was opened, potentially exposing sensitive information, such as passwords and banking information, to TikTok.[17]

Whose Data? Everyone's Data

Hard security concerns, such as vulnerability to intrusion and hacking through lax security measures, backdoors, and even bugdoors (security flaws hidden in a programming vulnerability—wittingly or unwittingly) are present whenever a device connects to the Internet. Yet TikTok appears to have deliberately engineered access to non-public datasets for certain individuals. Leaked audio of 80 internal TikTok meetings obtained by *Buzzfeed* captured an external auditor as he mused: "I feel like with these tools, there's some backdoor to access user data in almost all of them."[18] If not backdoors, bugdoors can be introduced later via a software update that can provide access to certain systems. Additionally, TikTok could serve as a potential entry point to access the data of other people using the same Wi-Fi network.[19]

This matters because China-based engineers employed by ByteDance reportedly accessed U.S. user data multiple times over the course of at least four months from 2021 to 2022.[20] In June 2022, the same *Buzzfeed*-obtained leaked audio from TikTok's internal company meetings confirmed that China-based engineers accessed U.S. user information that was not public, to include birthdays and phone numbers.[21] Before that, TikTok's former chief information security officer tacitly admitted that employees in China had access to U.S. user data in a blog post in 2020.[22]

Separate whistleblower leaks point to access of U.S. user data by China-based employees as a pervasive practice among ByteDance employees. In a March 2023 letter to Committee on Foreign Investment in the United States (CFIUS) chair Janet Yellen, Senator Josh Hawley (R–MO) wrote that a former ByteDance employee with direct knowledge of TikTok's operations admitted that his colleagues could "switch between Chinese and U.S. data with nothing more than the click of a button using a proprietary tool...just like a light switch."[23] In this case, extensive safeguards to shield U.S. user data likely did not exist and it was not difficult for ByteDance employees to access the data of Americans at will. In 2022, ByteDance conceded that it built an entire initiative centered around using TikTok to monitor the locations of at least two U.S. journalists.[24] Known as Project Raven internally, this effort to track the physical locations of Americans was approved by ByteDance employees in China, likely as an attempt to ferret out the employees that leaked to *Buzzfeed* in the summer of 2022.[25]

Beyond access to data, the CCP's likely control over TikTok's algorithm—originally designed using ByteDance's algorithms and artificial intelligence (AI) models—raises questions about the app's potential

to be actively manipulated by CCP-linked actors.[26] During divestment talks with Oracle in 2020, ByteDance representatives reportedly indicated that they would not surrender TikTok's source code to the U.S. company and would instead retain it in China.[27] After all, the CCP would have much to lose if ByteDance transferred the algorithm to an American company. FBI Director Christopher Wray appeared to explain why in a public speech more than two years later, asserting that the Chinese government both controls ByteDance and has the "ability to control the recommendation algorithm."[28] In a later hearing in front of the Senate Intelligence Committee in 2023, Director Wray testified that the Chinese government could control the software and data of millions of users who have TikTok on their devices, as well as spread propaganda within America.[29] Given the CCP's authoritarian track record, it is naive to believe that it has not taken advantage of these capabilities.

Manipulating the Information Environment

Concerns over data security do not scratch the surface of TikTok's ability to manipulate the information environment. ByteDance and TikTok have already pushed pro-CCP narratives to the U.S. public, censored content of which the party-state disapproves, and gathered the necessary information to conduct tailored influence campaigns. In two years, the percentage of adults who get their news from TikTok on a regular basis rose from only 3 percent in 2020 to 10 percent of American adults in 2022—roughly tripling this audience.[30] Now, nearly a quarter of adults in the United States under the age of 30 claim to regularly get their news from TikTok, according to the same survey.[31] This creates yet another vector for the CCP through which to expand its influence over the cognitive landscape of the American body politic.

In one example of these soft influence operations against U.S. users, former ByteDance employees alleged in 2022 that TikTok's parent company deliberately served pro-China content to a U.S. audience through its old news app, TopBuzz, in addition to censoring stories unfavorable to the Chinese government.[32] In 2020, TikTok confirmed that the Chinese government asked its employees to set up an account, under the radar, that "[showcases] the best side of China (some sort of propaganda)," according to a TikTok employee.[33] Leaked documents revealed that TikTok censors content that exposes the CCP's genocide against its Uyghur community in the Xinjiang region and videos about Tiananmen Square, Tibetan independence, and Hong Kong protests.[34] Concurrently, TikTok accounts linked to Chinese

state media pushed divisive content to users during the 2022 U.S. midterm elections focusing on cultural flashpoints, such as the abortion debate, and mostly criticizing Republican candidates while favoring Democrats.[35]

TikTok's algorithm and unique technical features, such as "heating," or artificially picking stories to go viral, also facilitate its manipulation of the information environment.[36] Since the algorithm trains on data drawn from individual user preferences and engagement versus connections and "friend" networks, it amounts to a more bespoke vector for propaganda delivery. When information is tailored to individuals based on their unique digital profiles, it could supercharge, at scale, custom CCP influence operations against U.S. citizens.[37] It is not hard to envision how these techniques could be deployed for the next U.S. presidential election in 2024.

The Long Game: Integrating TikTok Data with Stolen Datasets to Map U.S. Networks and Life Patterns

Americans should be concerned about the integration of TikTok data with China's growing trove of stolen datasets from hacks conducted at least as far back as 2014. Seemingly disparate datasets, once integrated, can help foreign adversaries to create profiles of American citizens that are ripe for blackmail, espionage, and more.

TikTok data, if fused with other information, could paint comprehensive intelligence pictures of American users. This type of data integration involves bringing together distinct data sources and synthesizing them into something new and more useful than the constituent sources. Such integration can also be as simple as cross-referencing data to make inferences and assessments.

Relatedly, China's strides in AI development indicate that the Chinese party-state can and will apply emerging technologies to such datasets to expeditiously exploit its collection. Leveraging applications of AI, such as machine learning, and analytics can transform data into insights. These technologies can parse through raw data at machine speed and make it useful, such as by identifying patterns and anomalies or predicting and mapping trends. Big data analytics can help to process and analyze large volumes of data and extract meaning or flag items of interest. With the advent of these technologies, data that was previously discarded or ignored now has value. What TikTok collects is thus even more useful to the PRC.

China is no stranger to employing these techniques. In fact, CCP officials are already using analytics and data integration to enforce internal control in places like the Xinjiang Uyghur Autonomous Region using an "Integrated

Joint Operations Platform."[38] Through this and other systems, Chinese authorities aggregate behavioral and biometric data, such as whether its inhabitants use an abnormal amount of electricity, display religious enthusiasm, or fail to show up to the local CCP activity of the day.[39] Authorities collect iris scans, cheek swabs, eyelash and voice samples, and even 360 degree captures of an individual's gait, all with the intent of integrating these pieces of data to create a multimodal profile of individuals and identify potential threats to the regime.[40] TikTok—given the depth and scope of data it collects—could be used by the Chinese government to build digital profiles, determine patterns of life, and even map out the social networks of Americans.

The CCP can easily construct digital profiles of Americans using the surveillance footholds it has already gained in the United States and other parts of the West. China reportedly created dossiers on prominent Americans and those hailing from allied countries like Australia, Canada, and Great Britain as recently as 2020 with both stolen and publicly available datasets.[41] This is just the tip of the iceberg. The CCP could add TikTok and other "open-source" data to cross-reference data from the Chinese hack of the Office of Personnel Management detected in 2014, which exposed the Social Security numbers, addresses, and family contacts of thousands of U.S. government employees, among other sensitive information.[42] This data can be added to that from other hacks linked to the Chinese state, such as the hack of the Marriott hotel system in 2018, the Anthem health care system hack from 2015 and the Equifax financial services hack in 2017 to enable the CCP to track where U.S. citizens stay, who they travel with, and any vulnerabilities in their health, medical, or financial lives.[43] Patterns of life from digital platforms like TikTok, with real-time GPS and biometric data-collection capabilities, can fill in many gaps. As former Google CEO Eric Schmidt warns in a 2023 *Foreign Affairs* essay:

> [T]he warfare of the future will target individuals in completely new ways: authoritarian states such as China and Russia may be able to collect individual data on Americans' shopping habits, location, and even DNA profiles, allowing for tailor-made disinformation campaigns and even targeted biological attacks and assassinations.[44]

The Chinese party-state has already unleashed an advanced surveillance state on its own people. All efforts by the CCP to apply its surveillance apparatus to Americans must be actively repudiated.

Recommendations for the United States

Given the current threat environment, The Heritage Foundation recommends a wholesale ban of TikTok's operations in the United States (and, eventually, all U.S. allied countries). After implementing a U.S. ban, the federal government should craft, publicize, and enforce a risk framework for foreign-owned platforms and applications seeking entry into the U.S. market.[45] A systemic approach is required to prevent another TikTok from infiltrating America in the future.[46]

To achieve this outcome, Congress, along with the executive branch and relevant agencies, should:

Ban TikTok from Operating in the U.S. Market. Congress should eliminate the loophole that prevents the President from enforcing sanctions against TikTok. To do so, U.S. legislators should update the International Emergency Economic Powers Act's (IEEPA's) Berman Amendment. IEEPA generally grants the President broad authority to contend with unusual or extraordinary foreign threats through measures like economic sanctions or embargoes.[47] A 2020 executive order by President Trump attempted to use IEEPA authorities to ban TikTok as a national security threat.[48] TikTok sued the Trump Administration that same year and a federal judge sided with TikTok by relying in part on a loophole for "informational materials" in the Berman Amendment, which is a set of amendments to IEEPA originally meant to protect the free flow of legitimate communication, such as films and photographs, to the United States from hostile nations like Cuba.[49]

Congress should update the statute to account for today's information environment and data exploitation practices by foreign-owned digital platforms and their proxies.[50] Specifically, the informational materials exemption could be qualified with language to indicate that these materials should be reasonably free from malign state actor links and influence. TikTok, by virtue of its parent company ByteDance, would not meet this criterion for exemption.[51]

- Congress can make clear, for example, that under such an update to the Berman Amendment, the President can deem these foreign-owned digital platforms (1) a national security threat, and (2) under the influence of a malign state actor. Alternatively, Congress can find that TikTok already qualifies as a national security threat under malign state actor influence.

- Legislators can also engineer a ban through other avenues that eliminate the Berman Amendment loophole or otherwise allow the use of IEEPA authorities to ban TikTok. Such efforts include Senator Marco Rubio's (R–FL) draft bill Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party (ANTI-SOCIAL CCP) Act, a bipartisan companion bill in the House sponsored by Representatives Mike Gallagher (R–WI) and Raja Krishnamoorthi (D–IL), and Representative Mike McCaul's (R–TX) Deterring America's Technological Adversaries (DATA) Act.[52]

Institute a Risk-Based Framework that Triggers Specific Policies for Foreign-Owned Digital Platforms that Want to Operate in the United States. A solution to the next TikTok exists in a country-neutral risk framework applied to foreign-owned platforms.[53] When met, these criteria would trigger an if–then ruleset for more focused policy prescriptions. *If* a particular criterion or set of criteria is met, *then* a particular policy action should be enacted.[54] The Treasury Department, Commerce Department, State Department, and the National Institute of Standards and Technology can contribute to the development of this framework. Essential elements of risk-based criteria that, when met, should trigger specific policy action include:[55]

- **The digital platform's target audience and monthly active users** (such as the size of the digital platform's American userbase and scale of growth). Meeting high-risk criteria under this description would not trigger a specific policy action but would help to inform the next three criteria.

- **The platform's overall security** (such as vulnerability to hard security problems like hacking and intrusion). Meeting high-risk criteria under this description would likely trigger a CFIUS review.

- **The platform's collection and information-control practices** (such as features of its algorithms, content moderation, and censorship policies). Meeting high-risk criteria under this description would likely trigger the use of IEEPA sanctions.

- **The platform's home jurisdiction.** This last element should encompass a foreign government's data practices (that is, asking: Does the

foreign government use AI-driven systems for surveillance that data collection from a U.S. market will help to improve?), the foreign government's human rights record, and the foreign government's governance atmosphere.[56] Platforms emanating from adversary nations like Iran, North Korea, or Russia would effectively trigger specific policy action.[57] Meeting specific high-risk criteria in this description would likely trigger a combination of CFIUS review and Leahy Law restrictions.

Pass a National Data-Protection Framework to Address Third-Party Data Collection and Sharing Mechanisms for U.S. Users. Congress should prohibit digital applications from sending U.S. user data to TikTok/ByteDance and similar foreign-owned digital platforms that represent legitimate national security threats to the United States.

- A TikTok ban is not sufficient to protect U.S. data because myriad apps and trackers can send U.S. data to TikTok even if a user has not downloaded the TikTok app.[58] In the future, *if* a company like TikTok/ByteDance meets specific high-risk criteria under the risk-based framework proposed in this *Backgrounder*, *then* these apps should be prevented from sending U.S. data to these designated companies.

- Congress can take steps to prevent applications from providing TikTok, and therefore ByteDance, with U.S. data via a data-protection framework with appropriate standards and oversight for how commercial entities collect, store, and share U.S. user data.[59]

Private companies should:

Remove TikTok from Their App Stores While Congress Negotiates a Solution to the TikTok Problem. Pending congressional action on TikTok, U.S. tech companies, including Google and Apple, should remove TikTok from their app stores due to its relationship to the CCP and legitimate threat to national security.[60]

Conclusion

Every day that TikTok is allowed to operate in the United States is another day that China can collect information about U.S. citizens and sharpen its ability to exploit Americans—especially the young. The more that TikTok becomes embedded in the United States, the harder it will be to uproot.

Even so, there will be another TikTok. Without implementing a systemic, risk-based framework to proactively address the next TikTok now, the U.S. will have ceded yet another critical digital battlespace to its adversaries. More so, U.S. policymakers have a duty to safeguard America's social fabric and protect young citizens from the whims of an adversary nation. Failing to deliver means that the next generation of Americans will pay the price for Washington's lassitude.

Kara Frederick is Director of the Technology Policy Center at The Heritage Foundation.

Endnotes

1. "TikTok Owner ByteDance Increases Price of Stock Option Buyback," Reuters, October 12, 2022, https://www.reuters.com/technology/TikTok-owner-ByteDance-increases-price-share-buyback-staff-sources-2022-10-12/ (accessed March 11, 2023); "TikTok Hits 3 Billion Downloads," CNET, July 14, 2021, https://www.cnet.com/tech/services-and-software/TikTok-hits-3-billion-downloads/ (accessed March 11, 2023); Sarah Perez, "Kids and Teens Now Spend More Time Watching TikTok than YouTube, New Data Shows," TechCrunch, July 13, 2022, https://techcrunch.com/2022/07/13/kids-and-teens-watch-more-TikTok-than-youtube-TikTok-91-minutes-in-2021-youtube-56/ (accessed March 11, 2023); "BTN Newsbreak," Australian Broadcast Corporation, March 2, 2023, https://www.abc.net.au/btn/newsbreak/btn-newsbreak-20230302/102045772 (accessed March 14, 2023); Drew Harwell, "How TikTok Ate the Internet," *The Washington Post*, October 14, 2022, https://www.washingtonpost.com/technology/interactive/2022/TikTok-popularity/ (accessed March 10, 2023); and "Watch Live: Sen. Warner Holds Press Briefing on TikTok," *The Hill*, March 7, 2023, video, https://thehill.com/homenews/3388161-watch-live-sen-warner-holds-press-briefing-on-TikTok/ (accessed March 10, 2023).
2. Murray Scot Tanner, "National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense (accessed March 10, 2023). See also the following excerpt from the author's 2019 white paper for the U.S. Cybersecurity Solarium Commission, with language from the author's 2019 testimony in front of the U.S. Senate Judiciary Subcommittee on Crime and Terrorism: Another similar policy is China's 2017 Cybersecurity Law, which is broadly written and provides a low threshold for access to data by the state. "[T]he CAC [Cyberspace Administration of China] updated the law in May 2019 to include a 'Data Security Management Measures' document, complete with 'personal information protection' and provisions for AI-driven content. Previous versions of the law invoke 'critical information infrastructure' and define 'network operators' in broad terms that extend beyond internet service providers to any entity using information and communication technologies (ICTs). As public policy researchers teased out for American media, these laws '[entail] strict provisions requiring data to be housed inside China, as well as spot inspections and even black-box security audits.' Finally, China's full 'internet security plan,' encompassing a soon-to-be-implemented 2020 Foreign Investment Law, will no longer render foreign-owned companies in China exempt from the Cybersecurity Law. Effectively, any data on communications networks in China will soon be subject to the Chinese Cybersecurity Bureau's scrutiny, without requiring an official request. This ability to access more data from more sources lays the groundwork for its exploitation." Kara Frederick, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors," testimony before the Subcommittee on Crime and Terrorism, Judiciary Committee, U.S. Senate, November 5, 2019, https://www.judiciary.senate.gov/imo/media/doc/Frederick%20Tesitmony1.pdf (accessed March 20, 2023).
3. Tanner, "National Intelligence Law: From Defense to Offense."
4. Ryan McMorrow, Qianer Liu, and Cheng Leng, "China Mes to Take 'Golden Shares' in Alibaba and Tencent Units," *Financial Times*, January 12, 2023, https://www.ft.com/content/65e60815-c5a0-4c4a-bcec-4af0f76462de (accessed March 20, 2023).
5. Coco Feng, "Chinese Government Takes Minority Stake, Board Seat in TikTok Owner ByteDance's Main Domestic Subsidiary," *South China Morning Post*, August 17, 2021, https://www.scmp.com/tech/big-tech/article/3145362/chinese-government-takes-minority-stake-board-seat-tiktok-owner (accessed March 14, 2023), and "Exclusive: Fretting About Data Security, China's Government Expands Its Use of 'Golden Shares,'" Reuters, December 16, 2021, https://www.reuters.com/markets/deals/exclusive-fretting-about-data-security-chinas-government-expands-its-use-golden-2021-12-15/ (accessed March 14, 2023).
6. U.S. Department of Justice, "Defendants' Memorandum in Opposition to Plaintiffs' Motion for a Preliminary Injunction," September 25, 2020, https://www.documentcloud.org/documents/7218230-DOJ-s-MEMORANDUM-in-OPPOSITION-to-TIKTOK.html (accessed March 10, 2023).
7. Emily Baker-White, "LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State Media—and Some Still Do," *Forbes*, August 11, 2022, https://www.forbes.com/sites/emilybaker-white/2022/08/10/ByteDance-TikTok-china-state-media-propaganda/?sh=68359903322f (accessed March 10, 2023).
8. Ibid.
9. Chris Stokel-Walker, "Inside TikTok's Attempts to 'Downplay the China Association,'" *Gizmodo*, July 27, 2022, https://gizmodo.com/TikTok-master-messaging-pr-playbook-china-music-1849334736 (accessed March 10, 2023).
10. Kara Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," Center for a New American Security, September 3, 2020, https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem (accessed March 12, 2023).
11. TikTok, "Privacy Policy," January 1, 2023, https://www.tiktok.com/legal/page/us/privacy-policy/en (accessed March 20, 2023).
12. TikTok, "Privacy Policy," and Paul Mozur, Ryan Mac, and Chang Che, "TikTok Browser Can Track Users' Keystrokes, According to New Research," *The New York Times*, August 29, 2022, https://www.nytimes.com/2022/08/19/technology/TikTok-browser-tracking.html (accessed March 10, 2023).
13. David Robinson, "TikTok Scores 63.1—Designed to Collect Data with Highest Malcore Score in Industry," Malcore, February 13, 2023, https://blog.malcore.io/p/TikTok-scores-631-designed-to-collect (accessed March 10, 2023).
14. Ibid.
15. Kevin Poulsen and Robert McMillan, "TikTok Tracked User Data Using Tactic Banned by Google," *The Wall Street Journal*, August 11, 2020, https://www.wsj.com/articles/TikTok-tracked-user-data-using-tactic-banned-by-google-11597176738 (accessed March 10, 2023).

16. Ibid.
17. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat: Curtailing and Controlling Global Information Flows," Australian Strategic Policy Institute, 2020, p. 40, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHlmPVE_6KKcBP1JRD5fRnAVTZ= (accessed March 10, 2023).
18. Emily Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China," *BuzzFeed News*, June 17, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/TikTok-tapes-us-user-data-china-ByteDance-access (accessed March 10, 2023).
19. Kurt Zindulka, "Former MI6 Chief: TikTok Gives CCP a Backdoor into Politicians' Data," *Breitbart*, August 12, 2020, https://www.breitbart.com/europe/2020/08/11/former-mi6-chief-TikTok-gives-ccp-a-backdoor-into-politicians-data-through-their-kids-smartphone/ (accessed March 10, 2023).
20. Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China."
21. Ibid.
22. Roland Cloutier, "Our Approach to Security," TikTok, April 28, 2020, https://newsroom.TikTok.com/en-us/our-approach-to-security (accessed March 10, 2023).
23. Josh Hawley, letter to Janet Yellen, March 7, 2023, https://www.documentcloud.org/documents/23698254-2023-03-07-hawley-letter-to-yellen-TikTok (accessed March 10, 2023).
24. Emily Baker-White, "Exclusive: TikTok Spied on Forbes Journalists," *Forbes*, December 2, 2022, https://www.forbes.com/sites/emilybaker-white/2022/12/22/TikTok-tracks-forbes-journalists-ByteDance/?sh=55bb707e7da5 (accessed March 10, 2023).
25. Ibid.
26. Liza Lin and Raffaele Huang, "TikTok's Talks with U.S. Have an Unofficial Player: China," *The Wall Street Journal*, February 14, 2023, https://www.wsj.com/articles/TikToks-talks-with-u-s-have-an-unofficial-player-china-f5fec4ec (accessed March 10, 2023).
27. Aaron Tilley, "TikTok Says All Data for U.S. Users Now Routed to Oracle Cloud," *The Wall Street Journal*, June 17, 2022, https://www.wsj.com/articles/TikTok-says-all-data-for-u-s-users-now-routed-to-oracle-cloud-11655503707 (accessed March 12, 2023); Jonathan Cheng, "Chinese State Television: 'ByteDance Will Not Sell TikTok's U.S. Operations to Microsoft or Oracle, nor Will the Company Give the Source Code to Any U.S. Buyers, Sources Said,'" Twitter, September 14, 2020, https://twitter.com/jchengwsj/status/1305381978422812673 (accessed March 10, 2023), and Georgia Wells and Aaron Tilley, "Oracle Wins Bid for TikTok in U.S., Beating Microsoft," *The Wall Street Journal*, September 14, 2020, https://www.wsj.com/articles/microsoft-drops-out-of-bidding-for-TikToks-u-s-operations-11600039821 (accessed March 10, 2023).
28. Christopher Wray, "2022 Josh Rosenthal Memorial Talk," The Ford School at the University of Michigan, December 2, 2022, https://fordschool.umich.edu/video/2022/christopher-wray-2022-josh-rosenthal-memorial-talk (accessed March 10, 2023).
29. Ivana Saric, "China Could Use TikTok to Control Users' Devices, FBI Director Says," Axios, March 8, 2023, https://www.axios.com/2023/03/08/china-TikTok-fbi-director-congress (accessed March 10, 2023).
30. Katerina Eva Matsa, "More Americans Are Getting News on TikTok, Bucking the Trend on Other Social Media Sites," Pew Research Center, October 21, 2022, https://www.pewresearch.org/fact-tank/2022/10/21/more-americans-are-getting-news-on-TikTok-bucking-the-trend-on-other-social-media-sites/ (accessed March 10, 2023).
31. Ibid.
32. Emily Baker-White, "TikTok Owner ByteDance Used a News App on Millions of Phones to Push Pro-China Messages, Ex-Employees Say," *Buzzfeed News*, July 26, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/TikTok-ByteDance-topbuzz-pro-china-content (accessed March 10, 2023).
33. Olivia Solon, "Chinese Government Asked TikTok for Stealth Propaganda Account," Bloomberg, July 29, 2022, https://www.bloomberg.com/news/articles/2022-07-29/chinese-government-asked-TikTok-for-stealth-propaganda-account?leadSource=uverify%20wall (accessed March 12, 2023), and Drew Harwell and Tony Room, "TikTok's Beijing Roots Fuel Censorship Suspicion as it Builds a Huge U.S. Audience," *The Washington Post*, September 15, 2019, https://www.washingtonpost.com/technology/2019/09/15/TikToks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/ (accessed March 10, 2023).
34. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat: Curtailing and Controlling Global Information Flows," Australian Strategic Policy Institute, 2020, p. 15, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHlmPVE_6KKcBP1JRD5fRnAVTZ= (accessed March 10, 2023), and Alex Hern, "Revealed: How TikTok Censors Videos that Do Not Please Beijing," *The Guardian*, September 25, 2019, https://www.theguardian.com/technology/2019/sep/25/revealed-how-TikTok-censors-videos-that-do-not-please-beijing (accessed March 10, 2023).
35. Emily Baker-White and Iain Martin, "On TikTok, Chinese State Media Pushes Divisive Videos about U.S. Politicians," *Forbes*, December 1, 2022, https://www.forbes.com/sites/emilybaker-white/2022/11/30/TikTok-chinese-state-media-divisive-politics (accessed March 10, 2023).
36. Emily Baker-White, "TikTok's Secret 'Heating' Button Can Make Anyone Go Viral," *Forbes*, January 20, 2023, https://www.forbes.com/sites/emilybaker-white/2023/01/20/TikToks-secret-heating-button-can-make-anyone-go-viral (accessed March 10, 2023).

37. Michael Horowitz et al., "Artificial Intelligence and International Security," Center for a New American Security, July 10, 2018, https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security (accessed March 10, 2023); Jordan Schneider, "What to Do About TikTok and WeChat," *ChinaTalk*, July 20, 2020, https://chinatalk.substack.com/p/what-to-do-about-TikTok (accessed March 12, 2023); and Brit McCandless Farmer, "How TikTok Could Be Used for Disinformation and Espionage," CBS News, November 15, 2020, https://www.cbsnews.com/news/TikTok-disinformation-espionage-60-minutes-2020-11-15/ (accessed March 10, 2023).
38. Australian Strategic Policy Institute, "How Mass Surveillance Works in Xinjiang: Reverse Engineering the Police Mass Surveillance App," April 2019, https://xjdp.aspi.org.au/explainers/how-mass-surveillance-works-in-xinjiang/ (accessed March 16, 2023), and Human Rights Watch, "China's Algorithms of Repression," May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass (accessed March 12, 2023).
39. Human Rights Watch, "China's Algorithms of Repression," and Yael Grauer, "Revealed: Massive Chinese Police Database," The Intercept, January 29, 2021, https://theintercept.com/2021/01/29/china-uyghur-muslim-surveillance-police/ (accessed March 16, 2023).
40. Megan Rajagopalan, "They Thought They'd Left the Surveillance State Behind. They Were Wrong," BuzzFeed, July 9, 2018, https://www.buzzfeednews.com/article/meghara/china-uighur-spies-surveillance (accessed March 12, 2023).
41. Andrew Probyn and Matthew Doran, "China's 'Hybrid War': Beijing's Mass Surveillance of Australia and the World for Secrets and Scandal," Australian Broadcasting Corporation, September 13, 2020, https://www.abc.net.au/news/2020-09-14/chinese-data-leak-linked-to-military-names-australians/12656668 (accessed, March 10, 2023).
42. Evan Perez, "FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach," CNN, https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html (accessed March 10, 2023).
43. David E. Sanger et al., "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing," *The New York Times*, December 10, 2018, https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html (accessed March 10, 2023); Eric Geller, "Chinese Nationals Charged for Anthem Hack, 'One of the Worst Data Breaches in History,'" *Politico*, May 9, 2019, https://www.politico.com/story/2019/05/09/chinese-hackers-anthem-data-breach-1421341 (accessed March 10, 2023); and Federal Bureau of Investigation, "Chinese Military Hackers Charged in Equifax Breach," February 10, 2020, https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020 (accessed March 10, 2023).
44. Eric Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs*, February 28, 2023, https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics (accessed March 10, 2023).
45. Kara Frederick, Chris Estep, and Megan Lamberth, "Beyond TikTok: Preparing for Future Digital Threats," *War on the Rocks*, August 20, 2020, https://warontherocks.com/2020/08/beyond-TikTok-preparing-for-future-digital-threats/ (accessed March 3, 2023).
46. Kara Frederick, "Democracy by Design," Center for a New American Security, December 15, 2020, https://www.cnas.org/publications/reports/democracy-by-design (accessed March 3, 2023).
47. 50 U.S. Code § 1701-1702, International Emergency Economic Powers Act.
48. The White House, "Executive Order on Addressing the Threat Posed by TikTok," August 6, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-TikTok/ (accessed March 10, 2023).
49. John D. McKinnon, "TikTok Ban Faces Obscure Hurdle: The Berman Amendments," *The Wall Street Journal*, January 29, 2023, https://www.wsj.com/articles/tiktok-ban-faces-obscure-hurdle-the-berman-amendments-11674964611 (accessed March 14, 2023); *TikTok, Inc., et al., v. Donald J Trump*, Civil Action No. 1:20-cv-02658 [federal court], https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2020cv2658-30 (accessed March 20, 2023); 50 U.S. Code § 1701-1702, International Emergency Economic Powers Act; and Christopher A. Casey et al., "The International Emergency Economic Powers Act: Origins, Evolution, and Use," Congressional Research Service R45618, July 14, 2020, https://fas.org/sgp/crs/natsec/R45618.pdf (accessed March 17, 2023). As researchers at the Center for a New American Security highlighted in a 2021 report, any presidential Administration's "hands are effectively tied...when it comes to using IEEPA to address the national security concerns associated with social media applications and websites" due to the Berman Amendment's exemption for "informational materials."
50. John Costello, Martijn Rasser, and Megan Lamberth, "From Plan to Action: Operationalizing a U.S. National Technology Strategy," Center for a New American Security, July 29, 2021, https://www.cnas.org/publications/reports/from-plan-to-action (accessed March 10, 2023).
51. Other proposals, such as the Data and Algorithm Transparency Agreement (DATA) Act, suggest exempting "sensitive personal data" from Berman Amendment protections.
52. Marco Rubio and Mike Gallagher, "TikTok, Time's Up. The App Should Be Banned in America," *The Washington Post*, November 10, 2022, https://www.washingtonpost.com/opinions/2022/11/10/marco-rubio-ban-TikTok-america-china-mike-gallagher/ (accessed March 10, 2023); The White House "Executive Order on Addressing the Threat Posed by TikTok"; David Feith, "Opportunities and Challenges for Trade Policy in the Digital Economy," Center for a New American Security, November 30, 2022, https://www.cnas.org/publications/congressional-testimony/opportunities-and-challenges-for-trade-policy-in-the-digital-economy (accessed March 10, 2023); and Brendan Bordelon, "GOP Rams Through TikTok Ban Bill Over Dem Objections," *Politico*, March 1, 2023, https://www.politico.com/news/2023/03/01/house-republicans-TikTok-ban-00084951 (accessed March 2023).
53. This concept of systemic risk and a risk-based framework with a ruleset to contend with future challenges is derived from the author's previous publications and communications with Administration officials and journalists starting in 2019, including but not limited to: Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem"; Frederick, "Democracy by Design"; Frederick, Estep, and Lamberth, "Beyond TikTok: Preparing

for Future Digital Threats"; Kara Frederick, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors," testimony before the Subcommittee on Crime and Terrorism, Judiciary Committee, U.S. Senate, November 5, 2019, https://www.judiciary.senate.gov/imo/media/doc/Frederick%20Tesitmony1.pdf (accessed March 20, 2023); and David Wertime, "America's Problem Is Much Bigger than TikTok," *Politico*, September 3, 2020, https://www.politico.com/newsletters/politico-china-watcher/2020/09/03/beijing-washington-next-TikTok-data-rules-standards-490242 (accessed March 10, 2023).

54. These policy actions can be a combination of tools already in the U.S. government policy toolkit, such as IEEPA sanctions, Leahy Law restrictions, or CFIUS reviews.
55. Derived from the author's e-mailed responses to David Wertime in the fall of 2020 for *Politico* China Watcher. Wertime, "America's Problem Is Much Bigger than TikTok."
56. From the author's e-mailed responses to David Wertime in the fall of 2020 for *Politico* China Watcher: "A governance atmosphere encompasses the systemic risk a nation brings to the table through its political institutions and legal environment (e.g. China's national intelligence law, Hong Kong's national security law, etc). This would control for the lack of recourse against government demands for private data, information, and/or access, like an independent judiciary and free press." And from Frederick, "The Razor's Edge": "For instance, China lacks sufficient rule-of-law protections, specific corporate governance practices, and democratic features that would allow companies to resist arbitrary requests for information from the Chinese government." Also see Frederick, "Democracy by Design."
57. This concept is not unlike the U.S. State Department's annual International Religious Freedom report's "Countries of Particular Concern" designations that lead to specific policy action.
58. Thomas Germain, "How TikTok Tracks You Across the Web, Even If You Don't Use the App," *Consumer Reports*, September 29, 2022, https://www.consumerreports.org/electronics-computers/privacy/TikTok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/ (accessed March 10, 2023).
59. Kara Frederick, "Combating Big Tech's Totalitarianism: A Road Map," Heritage Foundation *Backgrounder* No. 3678, February 7, 2022, https://www.heritage.org/technology/report/combating-big-techs-totalitarianism-road-map.
60. Brendan Carr, Commissioner of the Federal Communications Commission, letter to Apple and Google, June 24, 2023, https://www.fcc.gov/sites/default/files/carr-letter-apple-and-google.pdf (accessed March 10, 2023).

BuzzFeed News SIGN IN

TECH • CORPORATE ACCOUNTABILITY

Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China

"I feel like with these tools, there's some backdoor to access user data in almost all of them," said an external auditor hired to help TikTok close off Chinese access to sensitive information, like Americans' birthdays and phone numbers.

Emily Baker-White
BuzzFeed News Reporter

Posted on June 17, 2022 at 12:31 pm

View 26 comments

Erik Carter for BuzzFeed News

For years, TikTok has responded to data privacy concerns by promising that information gathered about users in the United States is stored in the United States, rather than China, where ByteDance, the video platform's parent company, is located. But according to leaked audio from more than 80 internal TikTok meetings, China-based employees of ByteDance have repeatedly accessed nonpublic data about US TikTok users — exactly the type of behavior that inspired former president Donald Trump to threaten to ban the app in the United States.

The recordings, which were reviewed by BuzzFeed News, contain 14 statements from nine different TikTok employees indicating that engineers in China had access to US data between September 2021 and January 2022, at the very least. Despite a TikTok executive's sworn testimony in an October 2021 Senate hearing that a "world-renowned, US-based security team" decides who gets access to this data, nine statements by eight different employees describe situations where US employees had to turn to their colleagues in China to determine how US user data was flowing. US staff did not have permission or knowledge of how to access the data on their own, according to the tapes.

"Everything is seen in China," said a member of TikTok's Trust and Safety department in a September 2021 meeting. In another September meeting, a director referred to one Beijing-based engineer as a "Master Admin" who "has access to everything." (While many employees introduced themselves by name and title in the recordings, BuzzFeed News is not naming anyone to protect their privacy.)

The recordings range from small-group meetings with company leaders and consultants to policy all-hands presentations and are corroborated by screenshots and other documents, providing a vast amount of evidence to corroborate prior reports of China-based employees accessing US user data. Their contents show that data was accessed far more frequently and recently than previously reported, painting a rich picture of the challenges the world's most popular social media app has faced in attempting to disentangle its US operations from those of its parent company in Beijing. Ultimately, the tapes suggest that the company may have misled lawmakers, its users, and the public by downplaying that data stored in the US could still be accessed by employees in China.

In response to an exhaustive list of examples and questions about data access, TikTok spokesperson Maureen Shanahan responded with a short statement: "We know we're among the most scrutinized platforms from a security standpoint, and we aim to remove any doubt about the security of US user data. That's why we hire experts in their fields, continually work to validate our security standards, and bring in reputable, independent third parties to test our defenses." ByteDance did not provide additional comment.

"Everything is seen in China."

In 2019, the Committee on Foreign Investment in the United States began investigating the national security implications of TikTok's collection of American data. And in 2020, then-president Donald Trump threatened to ban the app entirely over concerns that the Chinese government could use ByteDance to amass dossiers of personal information about US TikTok users. TikTok's "data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information," Trump wrote in his executive order. TikTok has said it has never shared user data with the Chinese government and would not do so if asked.

Most of the recorded meetings focus on TikTok's response to these concerns. The company is currently attempting to redirect its pipes so that certain, "protected" data can no longer flow out of the United States and into China, an effort known internally as Project Texas. In the recordings, the vast majority of situations where China-based staff accessed US user data were in service of Project Texas's aim to halt this data access.

Project Texas is key to a contract that TikTok is currently negotiating with cloud services provider Oracle and CFIUS. Under the CFIUS agreement, TikTok would hold US users' protected private information, like phone numbers and birthdays, exclusively at a data center managed by Oracle in Texas (hence the project name). This data would only be accessible by specific US-based TikTok employees. What data counts as "protected" is still being negotiated, but the recordings indicate that all public data, including users' public profiles and everything they post, will not be

included. (Disclosure: In a previous life, I held policy positions at Facebook and Spotify.) Oracle did not respond to a request for comment. CFIUS declined to comment.

Shortly before publication of this story, TikTok published a blog post announcing that it has changed the "default storage location of US user data" and that today, "100% of US user traffic is being routed to Oracle Cloud Infrastructure. We still use our US and Singapore data centers for backup, but as we continue our work we expect to delete US users' private data from our own data centers and fully pivot to Oracle cloud servers located in the US."

Lawmakers' fear that the Chinese government will be able to get its hands on American data through ByteDance is rooted in the reality that Chinese companies are subject to the whims of the authoritarian Chinese Communist Party, which has been cracking down on its homegrown tech giants over the last year. The risk is that the government could force ByteDance to collect and turn over information as a form of "data espionage."

There is, however, another concern: that the soft power of the Chinese government could impact how ByteDance executives direct their American counterparts to adjust the levers of TikTok's powerful "For You" algorithm, which recommends videos to its more than 1 billion users. Sen. Ted Cruz, for instance, has called TikTok "a Trojan horse the Chinese Communist Party can use to influence what Americans see, hear, and ultimately think."

Project Texas's narrow focus on the security of a specific slice of US user data, much of which the Chinese government could simply buy from data brokers if it so chose, does not address fears that China, through ByteDance, could use TikTok to influence Americans' commercial, cultural, or political behavior.

The headquarters of ByteDance, the parent company of video-sharing app TikTok, in Beijing.
Greg Baker / AFP via Getty Images

TikTok has said in blog posts and public statements that it physically stores all data about its US users in the US, with backups in Singapore. This does mitigate some risks — the company says this data is not subject to Chinese law — but it does not address the fact that China-based employees can access the data, experts say.

"Physical location does not matter if the data can still be accessed from China," Adam Segal, director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, told BuzzFeed News in an email. He said the "concern would be that data would still end up in the hands of Chinese intelligence if people in China were still accessing."

TikTok itself acknowledged its access issue in a 2020 blog post. "Our goal is to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the EU and US," TikTok's Chief Information Security Officer Roland Cloutier wrote.

Project Texas, once completed, is supposed to close this loophole for a limited amount of data. But many of the audio recordings reveal the challenges employees have faced in finding and closing the channels allowing data to flow from the US to China.

"Physical location does not matter if the data can still be accessed from China."

Fourteen of the leaked recordings include conversations with or about a team of consultants from Booz Allen Hamilton. One of the consultants told TikTok employees that they were brought on in February 2021 to help manage the Project Texas data migration, and a TikTok director told other TikTok employees that the consultants reported to TikTok's chief of US data defense. In recordings, the consultants investigate how data flows through TikTok and ByteDance's internal tools, including those used for data visualization, content moderation, and monetization.

In September 2021, one consultant said to colleagues, "I feel like with these tools, there's some backdoor to access user data in almost all of them, which is exhausting."

When asked for comment, Booz Allen Hamilton spokesperson Jessica Klenk said something about the above information was incorrect, but refused to specify what it was. "[A]t this point I'm not in a position to further discuss or even confirm/deny our relationship with any client. But I can tell you that what you're asserting here is inaccurate."

Additionally, four of the recordings contain conversations in which employees responsible for certain internal tools could not figure out what parts of those tools did. In a November 2021 meeting, a data scientist explained that for many tools, "nobody has really documented, uh, like, a how-to. And there are items within the tools that nobody knows what they're for."

The complexity of the company's internal systems and how they enable data to flow between the US and China underscores the challenges facing the United States Technical Services team, a new dedicated engineering team TikTok has begun hiring as part of Project Texas.

"Chinese nationals are not actually allowed to join."

To demonstrate the USTS team's independence from Chinese-owned ByteDance, one team member told a colleague in January that "not everyone can join" the team. "Chinese nationals are not actually allowed to join," he said. (A former employee who spoke to BuzzFeed News on condition of anonymity for fear of retribution corroborated this account.) When asked for comment on this practice, TikTok did not respond.

But while the mandate of this team is to control and manage access to sensitive US data, the USTS team reports to ByteDance leadership in China, as BuzzFeed News reported in March. In a recorded January 2022 meeting, a data scientist told a colleague: "I get my instructions from the main office in Beijing."

TikTok headquarters in Culver City, California.
Aaronp / GC Images

TikTok's goal for Project Texas is that any data stored on the Oracle server will be secure and not accessible from China or elsewhere globally. However, according to seven recordings between September 2021 and January 2022, the lawyer leading TikTok's negotiations with CFIUS and others clarify that this only includes data that is not publicly available on the app, like content that is in draft form, set to private, or information like users' phone numbers and birthdays that is collected but not visible on their profiles. A Booz Allen Hamilton consultant told colleagues in September 2021 that what exactly will count as "protected data" that will be stored in the Oracle server was "still being ironed out from a legal perspective."

In a recorded January 2022 meeting, the company's head of product and user operations announced with a laugh that unique IDs (UIDs) will not be considered protected information under the CFIUS agreement: "The conversation continues to evolve," they said. "We recently found out that UIDs are things we can have access to, which changes the game a bit."

What the product and user operations head meant by "UID" in this circumstance is not clear — it could refer to an identifier for a specific TikTok account, or for a device. Device UIDs are typically used by ad tech companies like Google and Facebook to link your behavior across apps, making them nearly as important an identifier as your name.

As TikTok continues to negotiate over what data will be considered protected, the recordings make clear that a lot of US user data — including public videos, bios, and comments — will not be exclusively stored in the Oracle server. Instead, this data will be stored in the company's Virginia data center, which may remain accessible from ByteDance's Beijing offices even once Project Texas is complete. That means ByteDance's China-based employees could continue to have access to insights about what American TikTok users are interested in, from cat videos to political beliefs.

It also appears that Oracle is giving TikTok considerable flexibility in how its data center will be run. In a recorded conversation from late January, TikTok's head of global cyber and data defense made clear that while Oracle would be providing the physical data storage space for Project Texas, TikTok would control the software layer: "It's almost incorrect to call it Oracle Cloud, because they're just giving us bare metal, and then we're building our VMs [virtual machines] on top of it." Oracle did not respond to a request for comment.

Meanwhile, TikTok's national security lawyer hopes the negotiation will have ripple effects in the tech industry and beyond. "There is going to be national security law that comes down from the Commerce Department," they said, referencing the Biden administration's development of regulations to govern apps that could be exploited "by foreign adversaries to steal or otherwise obtain data."

"The question is whether the company will go far enough."

"The law will be promulgated and codified in probably the next 18 months, I would say — and that's how every Chinese company is going to be able to operate in the US," the lawyer said.

TikTok's efforts with Project Texas may ultimately pay off for the company. According to Graham Webster, a research scholar at Stanford's Cyber Policy Center, if TikTok commits to being "transparent and high-integrity, and China-based employees won't be able to access user data," then "from a data security perspective, it should be possible to convince good-faith skeptics they have done enough.

"The question is whether the company will go far enough and whether skeptical authorities are truly open to being convinced," he told BuzzFeed News.

The details of the arrangement between CFIUS, TikTok, and Oracle were still under discussion as of January 2022, when the recordings end. But even though Project Texas's goal is to cordon off access to the most sensitive details about Americans that exist on TikTok's servers, one policy employee had doubts that will actually prevent ByteDance's employees in China from accessing this data.

"It remains to be seen if at some point product and engineering can still figure out how to get access, because in the end of the day, it's their tools," they said in a September 2021 meeting. "They built them all in China." ●

Topics in this article

Corporate Accountability | Big Tech | TikTok

Emily Baker-White
BuzzFeed News Reporter

Contact Emily Baker-White at emily.bakerwhite@buzzfeed.com.

Got a confidential tip? 👉 Submit it here

INNOVATION DAILY COVER

A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns

ILLUSTRATION BY STEPHANIE JONES FOR FORBES

Emily Baker-White Forbes Staff

Follow

Oct 25, 2022, 12:32pm EDT

Roland Cloutier, a U.S. Air Force veteran and former law enforcement officer, stepped down as TikTok's Global Chief Security Officer in July 2022 as the Biden administration continued to evaluate the national security risks posed by TikTok's Chinese ownership.

China-based ByteDance team led multiple audits and investigations into TikTok's U.S.-based former Global

Chief Security Officer, who had been

TIKTOK'S CHINA PROBLEM

China-based employees' access to American user data, according to internal company materials reviewed by *Forbes*.

TikTok hired Roland Cloutier as its Global Chief Security Officer in March 2020, shortly after the Treasury Department's Committee on Foreign Investment in the U.S. (CFIUS) opened an investigation into TikTok's ties to China. In public statements, TikTok touted the work of Cloutier, a U.S. Air Force veteran and former veterans affairs police detective, as evidence that TikTok was taking cybersecurity and data concerns seriously.

But according to current and former employees, as well as internal materials reviewed by *Forbes*, Cloutier's efforts to build out a robust security team were hamstrung by ByteDance's Internal Audit and Risk Control department, which is led by Song Ye, an executive in Beijing.

The materials show that Internal Audit launched multiple audits and investigations into Cloutier, alleging that he had pushed contracts worth millions of dollars to U.S.-based security vendors who were his personal friends. *Forbes* did not view materials that conclusively substantiated or refuted the veracity of these allegations.

Some current and former employees, though, characterized the probes into Cloutier as pretextual fishing expeditions designed to find a reason to push him out of the company. They noted that TikTok's Chief Internal Auditor, Chris Lepitak, had argued that some

work managed by Cloutier's TikTok team should instead be owned by ByteDance's Internal Audit team. The sources said Lepitak indicated that Internal Audit should oversee areas like digital forensics and insider risk, which are key to ensuring the security of user data. Lepitak reports to Song Ye, who reports to ByteDance cofounder and CEO Liang Rubo. *(Disclosure: In a past life, I held policy positions at Facebook and Spotify.)*

TikTok and ByteDance did not answer questions about why Cloutier was investigated, whether he was fired or whether he was pushed out of the company because of his work on data access controls. ByteDance spokesperson Jennifer Banks said that "[a]ny internal investigation is done with the intent to maintain a safe and compliant workplace," but declined to comment on specific investigations.

One investigation into Cloutier focused specifically on the Global Security Organization's relationship with consulting giant Booz Allen Hamilton. Several former employees at Booz currently work on TikTok's security team. Among other things, Booz was helping TikTok manage China-based employees' access to U.S. user data. Previously, Booz declined comment on its relationship with TikTok, and did not immediately respond to a comment request.

TikTok is currently negotiating a national security contract with CFIUS which will govern the way the Chinese-owned social media app handles Americans' personal user data. Before he left his post at the company in July 2022, Cloutier had been working on reducing

China-based employees' access to data: In an April 2020 blog post, he wrote, "Our goal is to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the E.U. and U.S."

BuzzFeed News reported in June that U.S. user data had been repeatedly accessed by employees in China into at least January 2022. *Forbes* reported last week that ByteDance's Internal Audit department — the same one that investigated Cloutier — planned to monitor individual U.S. citizens' locations using the TikTok app.

"Our goal is to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the E.U. and U.S."

Cloutier did not respond to multiple requests for comment. TikTok announced that he was stepping down from his role as Chief Security Officer in July, and his LinkedIn profile says he left the company in September.

ByteDance spokesperson Banks said in a statement that the Internal Audit team is "responsible for objectively auditing and evaluating the company and our employees' adherence to our codes of conduct."

TikTok did not comment on a detailed list of points and questions from *Forbes* about the Cloutier investigations and other investigations conducted by ByteDance's Internal Audit team. However, in response to *Forbes*'s earlier report about the team, TikTok's communications department tweeted: "Our Internal Audit team follows set policies and processes to acquire information they need to conduct internal investigations of violations of the company codes of conduct[.]"

Despite TikTok's claim that Internal Audit is "our" team, internal materials indicate that the Internal Audit team does not report to any members of TikTok's executive team, and instead reports directly to ByteDance executives in China. TikTok did not answer a question about why it referred to the Internal Audit team in this way.

Materials also show that the probes conducted by Internal Audit have often been extensive, including contracts with outside security firms and reviews of many thousands of emails, employee correspondences and messages in Lark, ByteDance's internal workplace management software. Materials also show that some investigations have been kept confidential from employees' managers and from HR.

Cloutier is also not the only U.S. executive who was targeted by the Internal Audit department. Two sources

also said that at least one other executive, former TikTok Global Head of Marketing Nick Tran, was also pushed out over allegations of conflicts of interests due to personal relationships, which the sources characterized as an excuse to terminate the employee. Tran declined to comment.

Numerous senior employees felt "that themselves and their teams are just 'figureheads' or 'powerless ombudsmen'" who are "functionally subject to the control of CN-based teams."

Three current and former employees also described a list of TikTok employees — some of whom have now left the company — that ByteDance hoped to oust from their positions. Neither TikTok nor ByteDance commented on the existence of such a list. The Financial Times previously reported that TikTok had created a "kill list" for employees it wished to force out of the company. At the time, TikTok told FT that it was "unable to find any list that matched this description."

TikTok has not yet named its next Chief Global Security Officer, but documents show that the company's Global Security Organization is currently in the middle of a corporate restructuring, meant to address "pain points" including redundancy across teams. TikTok and ByteDance declined to answer questions about whether the restructuring would change the division of responsibilities between TikTok's Global Security Organization and ByteDance's Internal Audit team.

In the past, TikTok has struggled with retention of U.S.-based executives. In September, *Forbes* reported that at least five senior leaders at TikTok had left the company because they felt they could not contribute to key decision making. ByteDance's Internal Audit department apparently found the same thing: A risk assessment prepared by the department in late 2021 found that numerous senior employees felt "that themselves and their teams are just 'figureheads' or 'powerless ombudsmen'" who are "functionally subject to the control of CN-based teams."

Neither TikTok nor ByteDance commented on the risk assessment.

Last month, President Biden issued an executive order instructing CFIUS to more closely consider the risks posed by foreign companies' access to Americans' private data. Yesterday, the Department of Justice held a press conference to announce indictments into two Chinese government intelligence officials who allegedly sought to impede a federal investigation into alleged wrongdoing

by the China-based telecom giant Huawei. (Huawei did not immediately respond to a request for comment.)

At the press conference, Deputy Attorney General Lisa Monaco, who is reportedly among the officials reviewing the deal between TikTok and CFIUS, said about the Huawei case: "This case exposes the interconnection between PRC intelligence officers and Chinese companies. And it demonstrates once again why such companies, especially in the telecommunications industry, shouldn't be trusted to securely handle our sensitive personal data and communications."

Richard Nieva contributed reporting.

MORE ON TIKTOK AND BYTEDANCE

MORE FROM FORBES

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

By **Emily Baker-White**

MORE FROM FORBES

LinkedIn Profiles Indicate 300 Current TikTok And ByteDance Employees Used To Work For Chinese State Media—And Some Still Do

By **Emily Baker-White**

MORE FROM FORBES

TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say

By **Emily Baker-White**

MORE FROM FORBES

Senate Intelligence Committee Calls On FTC To Investigate TikTok For 'Deception'

By **Emily Baker-White**

MORE FROM FORBES

TikTok, Hospitals And Tutoring Apps: The Many Tentacles Of Chinese Tech Giant ByteDance

By **Alexandra S. Levine**

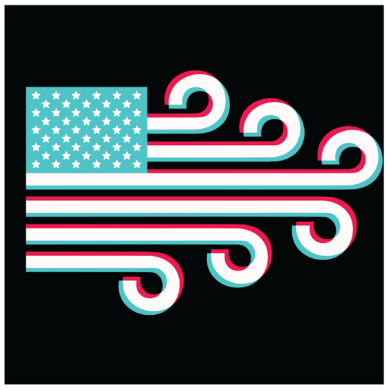
Follow me on Twitter. Send me a secure tip.

Emily Baker-White Follow

I'm a technology reporter and senior writer at Forbes based in San Francisco. Have a tip? Email me at ebakerwhite@forbes.com or emilybakerwhite@protonmail.com.

Editorial Standards Reprints & Permissions

TIKTOK'S CHINA PROBLEM



INNOVATION EDITORS' PICK

TikTok Couldn't Ensure Accurate Responses To Government Inquiries, A ByteDance Risk Assessment Said

ILLUSTRATION BY FERNANDO CAPETO FOR FORBES

Emily Baker-White Forbes Staff

Follow

Nov 28, 2022, 07:00am EST

The internal risk assessment, completed in late 2021, also warned of rampant self-dealing, embezzlement, and potential indictment of executives.

In **fall 2021**, members of ByteDance's internal audit and risk control team prepared an urgent message for executives: Change your approach to fraud prevention — soon — or you could end up in jail.

The message came in the form of a standard Fraud Risk Assessment, reviewed by *Forbes*, which was based on a

review of TikTok and ByteDance policies, and on approximately 90 interviews — some educational and others investigatory — with TikTok and ByteDance employees from at least 17 different teams.

In its executive summary, the document laid out the stakes: "Unless ByteDance makes substantial, sustained, and rapid investments in its anti-fraud programs, it will likely be too late to prevent immense future fraud-related losses and liabilities — potentially including multi-billion dollar fines ($USD), being forced to submit to the control of an external monitor, loss of the ability to operate in the U.S. and other major markets, and criminal indictments of ByteDance executives and managers (even if they did not actively participate in misconduct)."

Much of the risk assessment was devoted to discussion of basic risks present at any large company — things like embezzlement and conflicts of interest in vendor selection. But it also warned of additional risks caused by ByteDance's Chinese ownership. At one point, it said that according to an employee with knowledge of the company's data retention practices, it was "impossible" to avoid "sensitive and/or regulated data" from being "improperly" kept in servers in China. At others, it pointed to incomplete company policies, irregular document retention practices, and a "lack of formal clarity" about which executives and teams were in charge of various workstreams.

Because of that lack of formal clarity, the assessment said, "it is frequently difficult or impossible to verify the

correctness of information the Company reports to government agencies."

At the time the risk assessment was written, TikTok was engaged (as it is today) in negotiations with the U.S. government about potential national security risks posed by the app's ownership by Beijing-based ByteDance. Those risks intensified in June, after a report from BuzzFeed News showed that China-based ByteDance employees had repeatedly accessed U.S. TikTok users' personal information, and again in October, after a *Forbes* report showed that a Beijing-based ByteDance team had planned to use the TikTok app to monitor the location of specific U.S. citizens.

The assessment did not recognize TikTok as a separate business entity from ByteDance, but drew from numerous TikTok-specific sources of information, including documents referencing TikTok operations, TikTok content moderation, the TikTok verification process and TikTok revenue products. *(Disclosure: In a former life, I held policy positions at Facebook and Spotify.)*

"[I]t is frequently difficult or impossible to verify the correctness of information the Company reports to government agencies."

TikTok did not reply to a request for comment.

ByteDance spokesperson Jennifer Banks provided the following statement about the assessment: "ByteDance regularly conducts risk assessments to identify potential risks and improve compliance, but this report is not one of them. This document was created within one department nearly two years ago, never presented internally beyond that, and is largely inaccurate, with outdated details which are made irrelevant by regular updates to our practices in the years since." Banks did not answer a follow-up question about which, if any, of the specific points included in this reporting were inaccurate, and did not offer details on how the company has updated its practices since the assessment was done.

The assessment was primarily authored by an attorney with experience in state and federal government who no longer works for ByteDance. The author responded "no comment" to an interview request.

The assessment also identified risks related to TikTok and ByteDance's primary form of internal communication — a ByteDance messaging app called Lark — noting that Lark messages are stored in China. TikTok and ByteDance did not answer questions about whether the Lark messages of U.S.-based employees, including those in which employees discussed topics like the labeling of Chinese state media entities or the tracking of foreign influence operations, are viewable by ByteDance employees in China.

But the assessment's discussion of Lark did not stop at where messages were stored. It also said, "[t]he Company is currently incapable of extracting accurate, usable records of critically important internal communications, specifically, numerous information about and within internal Lark messages."

It then put that limitation into sharp relief, saying that as a result, "we lack the ability to assure even basic custodian-by-custodian preservation of communications that represent critically important investigative evidence and/or that the Company is responsible for maintaining and turning-over to outside parties in connection with government investigation and litigation subpoenas." In other words, ByteDance might not be able to turn over certain internal communications to the government, even in circumstances where it is legally required to do so.

"The Company is currently incapable of extracting accurate, usable records of critically important internal communications[.]"

Austin Hacker, press secretary for Republican Congressman James Comer, confirmed to *Forbes* that Comer's office has requested internal communications

from TikTok, including Lark messages. "At this time, TikTok has failed to provide the requested information, documents, and communications," he said in an email. TikTok spokesperson Maureen Shanahan confirmed that TikTok received Rep. Comer's request and said the company plans to respond.

Comer's office is just one of numerous government entities that might seek Lark records from TikTok and ByteDance — and encounter the irregular data retention practices described in the risk assessment, if they have not changed since it was written. In July, the Senate Intelligence Committee called on the FTC to investigate whether TikTok had misled lawmakers about foreign access to U.S. user data, and regulators from the EU and Australia have also launched investigations into the company's data practices. In a recent update to its European data policies, TikTok acknowledged that EU user data is accessible by China-based employees, "subject to a series of robust security controls and approval protocols."

In addition to its warnings about ByteDance's inability to comply with government requests, the assessment also pointed to problematic internal policies. One employee interviewed for the assessment said that for a set of new product launches, "nobody really confirm[ed] the product's features were compliant with the law before launch." Elsewhere, the assessment described a document called "Communications Guidelines," which many managers and employees understood to be mandatory despite warnings from company lawyers that it "could likely not be enforced consistent with U.S. labor

laws." TikTok and ByteDance declined to answer questions about why their lawyers gave this advice.

The assessment also described a vendor payments process that lacked even basic checks against self-dealing and embezzlement. "Based on expense data obtained for this FRA and verbal confirmations from system administrators," the assessment said, "it appears that ByteDance's data systems simply do not collect or retain data about multiple critically important matters related to company expense transactions."

Moreover, it said company transactions often happened without contracts in place (it referenced almost 35,000 payments of this type), or with poor recordkeeping about what the payments were for. Between September 2019 and May 2021, the report said, "ByteDance made over forty-six thousand payments (collectively totaling over $1.38 billion USD) for which the data field that is supposed to track which project a payment relates to says only 'NULL'." Also, because ByteDance tasks some employees with entering one another's payments, the assessment noted that over $1 billion in payments was attributable to just seven people.

The assessment cited various examples of alleged employee fraud at ByteDance, including embedded images of fraudulent invoices and a reference to 342 instances where "multiple different supplier names receiv[ed] payments at the same bank account number." It described one case where an employee "abused his access to Company systems to improperly verify TikTok user accounts/handles" and "orchestrated a substantial

fraud scheme involving embezzlement, bribery, kickbacks among fictitious vendors, family members, and friends."

"This FRA did not examine extensive high-risk related-party transactions involving potentially improper self-dealing between ByteDance and its own institutional investors[.]"

But it also noted the company's limited ability to investigate incidents of this kind, saying: "Employees responsible for investigating potential procurement fraud encounter a pervasive absence of evidence that accurately, completely, and specifically describes important decisions, thought processes, and actions by employees and managers related to high-risk transactions, such as vendor selections on rushed, high-value, procurements where no competitive bidding occurs."

Despite the assessment's considerable length and detail, its authors were also careful to explain its limited scope. "This FRA did not examine extensive high-risk related-party transactions involving potentially improper self-dealing between ByteDance and its own institutional

investors," it said. Moreover, because the assessment was conducted only by ByteDance employees, it noted that it lacked the independence and objectivity expected of fraud assessments at companies of ByteDance's size. (According to the Association of Certified Fraud Examiners, Fraud Risk Assessments are standard for large companies and should be conducted regularly.)

To underscore the stakes of ByteDance's lack of fraud protections, the document referenced the criminal proceedings against Theranos founder Elizabeth Holmes as an example of how privately held companies can be criminally liable for fraud. It noted that people uninvolved in fraud can be personally indicted "for failing to report suspicions to internal and external authorities."

MORE FROM FORBES

MORE FROM FORBES

A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns

By **Emily Baker-White**

MORE FROM FORBES

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

By **Emily Baker-White**

MORE FROM FORBES

TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say

By **Emily Baker-White**

MORE FROM FORBES

Senate Intelligence Committee Calls On FTC To Investigate TikTok For 'Deception'

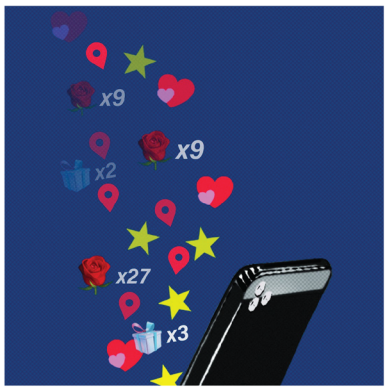
By **Emily Baker-White**

Follow me on Twitter. Send me a secure tip.

Emily Baker-White Follow

I'm a technology reporter and senior writer at Forbes based in San Francisco. Have a tip? Email me at ebakerwhite@forbes.com or emilybakerwhite@protonmail.com.

Editorial Standards Reprints & Permissions



INNOVATION DAILY COVER

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

ILLUSTRATION BY STEPHANIE JONES FOR FORBES; PHOTO BY GEORGE PETERS/GETTY IMAGES

Emily Baker-White Forbes Staff

Follow

Oct 20, 2022, 03:24pm EDT

The project, assigned to a Beijing-led team, would have involved accessing location data from some U.S. users' devices without their knowledge or consent.

A China-based team at TikTok's parent company, ByteDance, planned to use the TikTok app to monitor the personal location of

some specific American citizens, according to materials reviewed by *Forbes*.

The team behind the monitoring project — ByteDance's Internal Audit and Risk Control department — is led by Beijing-based executive Song Ye, who reports to ByteDance cofounder and CEO Rubo Liang.

The team primarily conducts investigations into potential misconduct by current and former ByteDance employees. But in at least two cases, the Internal Audit team also planned to collect TikTok data about the location of a U.S. citizen who had never had an employment relationship with the company, the materials show. It is unclear from the materials whether data about these Americans was actually collected; however, the plan was for a Beijing-based ByteDance team to obtain location data from U.S. users' devices.

TikTok spokesperson Maureen Shanahan said that

on users' IP addresses to "among other things, help show relevant content and ads to users, comply with applicable laws, and detect and prevent fraud and inauthentic behavior."

But the material reviewed by *Forbes* indicates that ByteDance's Internal Audit team was planning to use this location information to surveil individual American citizens, not to target ads or any of these other purposes. *Forbes* is not disclosing the nature and purpose of the planned surveillance referenced in the materials in order to protect sources. TikTok and ByteDance did not answer questions about whether Internal Audit has specifically

targeted any members of the U.S. government, activists, public figures or journalists.

TikTok is reportedly close to signing a contract with the Treasury Department's Committee on Foreign Investment in the United States (CFIUS), which evaluates the national security risks posed by companies of foreign ownership, and has been investigating whether the company's Chinese ownership could enable the Chinese government to access personal information about U.S. TikTok users. *(Disclosure: In a past life, I held policy positions at Facebook and Spotify.)*

In September, President Biden signed an executive order enumerating specific risks that CFIUS should consider when assessing companies of foreign ownership. The order, which states that it intends to "emphasize . . . the risks presented by foreign adversaries' access to data of United States persons," focuses specifically on foreign companies' potential use of data "for the surveillance, tracing, tracking, and targeting of individuals or groups of individuals, with potential adverse impacts on national security."

The Treasury Department did not respond to a request for comment.

The Internal Audit and Risk Control team runs regular audits and investigations of TikTok and ByteDance employees, for infractions like conflicts of interest and misuse of company resources, and also for leaks of confidential information. Internal materials reviewed by *Forbes* show that senior executives, including TikTok CEO Shou Zi Chew, have ordered the team to investigate

individual employees, and that it has investigated employees even after they left the company.

The internal audit team uses a data request system known to employees as the “green channel,” according to documents and records from Lark, ByteDance’s internal office management software. These documents and records show that “green channel” requests for information about U.S. employees have pulled that data from mainland China.

TikTok and ByteDance did not answer questions about whether Internal Audit has specifically targeted any members of the U.S. government, activists, public figures or journalists.

“Like most companies our size, we have an internal audit function responsible for objectively auditing and evaluating the company and our employees' adherence to our codes of conduct,” said ByteDance spokesperson Jennifer Banks in a statement. “This team provides its recommendations to the leadership team."

ByteDance is not the first tech giant to have considered using an app to monitor specific U.S. users. In 2017, the New York Times reported that Uber had identified various local politicians and regulators and served them a separate, misleading version of the Uber app to avoid regulatory penalties. At the time, Uber acknowledged that it had run the program, called "greyball," but said it was used to deny ride requests to "opponents who collude with officials on secret 'stings' meant to entrap drivers," among other groups.

TikTok did not respond to questions about whether it has ever served different content or experiences to government officials, regulators, activists or journalists than the general public in the TikTok app.

Both Uber and Facebook also reportedly tracked the location of journalists reporting on their apps. A 2015 investigation by the Electronic Privacy Information Center found that Uber had monitored the location of journalists covering the company. Uber did not specifically respond to this claim. The 2021 book *An Ugly Truth* alleges that Facebook did the same thing, in an effort to identify the journalists' sources. Facebook did not respond directly to the assertions in the book, but a spokesperson told the San Jose Mercury News in 2018 that, like other companies, Facebook "routinely use[s] business records in workplace investigations."

"It is impossible to keep data that should not be

stored in CN from being retained in CN-based servers."

But an important factor distinguishes ByteDance's planned collection of private users' information from those cases: TikTok recently told lawmakers that access to certain U.S. user data — likely including location — will be "limited only to authorized personnel, pursuant to protocols being developed with the U.S. Government." TikTok and ByteDance did not answer questions about whether Internal Audit executive Song Ye or other members of the department are "authorized personnel" for the purposes of these protocols.

These promises are part of Project Texas, TikTok's massive effort to rebuild its internal systems so that China-based employees will not be able to access a swath of "protected" identifying user data about U.S. TikTok users, including their phone numbers, birthdays and draft videos. This effort is central to the company's national security negotiations with CFIUS.

At a Senate hearing in September, TikTok Chief Operating Officer Vanessa Pappas said the forthcoming CFIUS contract would "satisfy all national security concerns" about the app. Still, some senators appeared skeptical. In July, the Senate Intelligence Committee began an investigation into whether TikTok misled lawmakers by withholding information about China-based employees' access to U.S. data earlier this year,

following a June report in BuzzFeed News showing that U.S. user data had been repeatedly accessed by ByteDance employees in China.

In a statement about TikTok's data access controls, TikTok spokesperson Shanahan said that the company uses tools like encryption and "security monitoring" to keep data secure, access approval is overseen by U.S personnel, and that employees are granted access to U.S. data "on an as-needed basis."

It is unclear what role ByteDance's Internal Audit team will play in TikTok's efforts to limit China-based employees' access to U.S. user data, especially given the team's plans to monitor some American citizens' locations using the TikTok app. But a fraud risk assessment written by a member of the team in late 2021 highlighted data storage concerns, saying that according to employees responsible for the company's data, "it is impossible to keep data that should not be stored in CN from being retained in CN-based servers, even after ByteDance stands up a primary storage cetner [sic] in Singapore. [Lark data is saved in China.]" (brackets in original).

Moreover, a leaked audio conversation from January 2022 shows that the Beijing-based team was, at that point, gathering additional information on Project Texas. In the call, a member of TikTok's U.S. Trust & Safety team recounted an unusual conversation to his manager: The employee had been asked by Chris Lepitak, TikTok's Chief Internal Auditor, to meet at an LA-area restaurant off hours. Lepitak, who reports to Beijing-based Song Ye,

then asked the employee detailed questions about the location and details of the Oracle server that is central to TikTok's plans to limit foreign access to personal U.S. user data. The employee told his manager that he was "freaked out" by the exchange. TikTok and ByteDance did not respond to questions about this conversation.

Oracle spokesperson Ken Glueck said that while TikTok does currently use Oracle's cloud services, "we have absolutely no insight one way or the other" into who can access TikTok user data. "Today, TikTok is running in the Oracle cloud, but just like Bank of America, General Motors, and a million other customers, they have full control of everything they're doing," he said.

This corroborates a January statement made by TikTok's Head of Data Defense in another leaked audio call. In that call, the executive said to a colleague: "It's almost incorrect to call it Oracle Cloud, because they're just giving us bare metal, and then we're building our VMs [virtual machines] on top of it."

Glueck made clear that this would change if and when TikTok finalizes its contract with the federal government. "But unless and until that's the case," he said, Oracle is not providing anything "other than our own security" for TikTok.

TikTok did not answer questions from *Forbes* about the status of the company's negotiations with CFIUS. But in a statement to Bloomberg published early this morning, TikTok spokesperson Brooke Oberwetter said: "We are confident that we are on a path to fully satisfy all reasonable U.S. national security concerns."

Richard Nieva contributed reporting.

MORE FROM FORBES

MORE FROM FORBES

Students Viewed This Type Of TikTok 412 Billion Times-And It's Not Porn

By **Emma Whitford**

MORE FROM FORBES

Facebook And Instagram Are Full Of Violent Erotica Ads From ByteDance- And Tencent-Backed Apps

By **Emily Baker-White**

MORE FROM FORBES

LinkedIn Profiles Indicate 300 Current TikTok And ByteDance Employees Used To Work For Chinese State Media-And Some Still Do

By **Emily Baker-White**

MORE FROM FORBES

TikTok Moderators Are Being Trained Using Graphic Images Of Child Sexual Abuse

By **Alexandra S. Levine**

Follow me on Twitter. Send me a secure tip.

Emily Baker-White Follow

I'm a technology reporter and senior writer at Forbes based in San Francisco. Have a tip? Email me at ebakerwhite@forbes.com or emilybakerwhite@protonmail.com.

Editorial Standards Reprints & Permissions

INNOVATION EDITORS' PICK

EXCLUSIVE: TikTok Spied On Forbes Journalists

ILLUSTRATION BY PHILIP SMITH FOR FORBES/IMAGE BY DRAFTER123 GETTY IMAGES

Emily Baker-White Forbes Staff

Follow

Dec 22, 2022, 02:53pm EST 6

ByteDance confirmed it used TikTok to monitor journalists' physical location using their IP

addresses, as first reported by *Forbes* in October.

An internal investigation by ByteDance, the parent company of video-sharing platform TikTok, found that employees tracked multiple journalists covering the company, improperly gaining access to their IP addresses and user data in an attempt to identify whether they had been in the same locales as ByteDance employees.

According to materials reviewed by *Forbes*, ByteDance tracked multiple *Forbes* journalists as part of this covert surveillance campaign, which was designed to unearth the source of leaks inside the company following a drumbeat of stories exposing the company's ongoing links to China. As a result of the investigation into the surveillance tactics, ByteDance fired Chris Lepitak, its chief internal auditor who led the team responsible for them. The China-based executive Song Ye, who Lepitak reported to and who reports directly to ByteDance CEO Rubo Liang, resigned.

"I was deeply disappointed when I was notified of the situation... and I'm sure you feel the same," Liang wrote in an internal email shared with *Forbes*. "The public trust that we have spent huge efforts building is going to be significantly undermined by the misconduct of a few individuals. ... I believe this situation will serve as a lesson to us all."

"It is standard practice for companies to have an internal audit group authorized to investigate code of conduct violations," TikTok General Counsel Erich Andersen wrote in a second internal email shared with *Forbes*. "However, in this case individuals misused their authority to obtain access to TikTok user data."

Forbes first reported the surveillance tactics, which were overseen by a China-based team at ByteDance, in October. Asked for comment on that story, ByteDance and TikTok did not deny the surveillance, but took to Twitter after the story was published to say that "TikTok has never been used to 'target' any members of the U.S. government, activists, public figures or journalists," and that "TikTok could not monitor U.S. users in the way the article suggested." In the internal email, Liang acknowledged that TikTok had been used in *exactly* this way, as *Forbes* had reported.

"This is a direct assault on the idea of a free press and its critical role in a functioning democracy."

The investigation, internally known as Project Raven, began this summer after *BuzzFeed News* published a story revealing that China-based ByteDance employees had repeatedly accessed U.S. user data, based on more than 80 hours of audio recordings of internal TikTok meetings. According to internal ByteDance documents reviewed by *Forbes*, Project Raven involved the company's Chief Security and Privacy Office, was known to TikTok's Head of Global Legal Compliance, and was approved by ByteDance employees in China. It tracked Emily Baker-White, Katharine Schwab and Richard Nieva, three *Forbes* journalists that formerly worked at BuzzFeed News. (*Disclosure: In a previous life, I held policy positions at Facebook and Spotify*.)

"This is a direct assault on the idea of a free press and its critical role in a functioning democracy," says Randall Lane, the chief content officer of *Forbes*. "We await a direct response from ByteDance, as this raises fundamental questions about what they are doing with the information they compile from TikTok users."

After this story was published, TikTok spokesperson Hilary McQuaide said, "The misconduct of certain individuals, who are no longer employed at ByteDance, was an egregious misuse of their authority to obtain access to user data. This misbehavior is unacceptable, and not in line with our efforts across TikTok to earn the trust of our users."

ByteDance spokesperson Jennifer Banks added, "ByteDance condemns this misguided plan that violated the company's Code of Conduct." She said that

ByteDance has not found evidence that the company surveilled *Forbes* journalists beyond Baker-White, but that the investigation is ongoing. Internal company materials reviewed by *Forbes* indicate surveillance of Schwab and Nieva as well.

Banks also noted that its head of Global Legal Compliance, Catherine Razzano, did not know about the surveillance of journalists until late October, although materials reviewed by *Forbes* show that she was aware of the Project Raven leak investigation before that time.

"This new development reinforces serious concerns that the social media platform has permitted TikTok engineers and executives in the People's Republic of China to repeatedly access private data of U.S. users despite repeated claims to lawmakers and users that this data was protected," Senator Mark Warner told *Forbes*. "The DoJ has also been promising for over a year that they are looking into ways to protect U.S. user data from Bytedance and the CCP — it's time to come forward with that solution or Congress could soon be forced to step in."

According to an internal email sent Thursday by Andersen, ByteDance found that several of its employees obtained the data of "a former BuzzFeed reporter and a Financial Times reporter," as well as a "small number of

people connected to the reporters" through their TikTok accounts. The audit was conducted by the law firm Covington & Burling, which has represented TikTok in litigation against the U.S. government. Covington did not respond to a comment request.

In addition to the firing of TikTok's Chief Internal Auditor, Chris Lepitak, who was suspended after *Forbes*' initial report about the surveillance scheme in October, ByteDance fired two additional TikTok employees in the United States and China as a result of the findings. Lepitak did not immediately respond to a request for comment. "None of the individuals found to have directly participated in or overseen the misguided plan remain employed at ByteDance," Andersen wrote in the internal email.

"This new development reinforces serious concerns that the social media platform has permitted TikTok engineers and executives in the People's Republic of China to repeatedly access private data of U.S. users despite repeated claims to lawmakers and users that this data was protected."

The team that oversaw the surveillance campaign was ByteDance's Internal Audit and Risk Control department, a Beijing-based unit primarily responsible for conducting

investigations into potential misconduct by current and former ByteDance employees.

TikTok chief executive Shou Zi Chew wrote in his own email to employees, "We take data security incredibly seriously," adding that the company's Project Texas, which would limit China-based access to U.S. user data (and which was first reported by Baker-White at BuzzFeed News) was a "testament to that commitment."

In 2021, TikTok became the most visited website in the world, but the app's ownership by Chinese tech giant ByteDance has raised serious concerns about the company's access to the personal information of millions of U.S. citizens, as well as its capacity to manipulate and influence user content. The company is currently negotiating a national security contract with the Treasury Department's Committee on Foreign Investment in the U.S. (CFIUS), which will govern the way the Chinese-owned social media app handles Americans' personal user data. The company has also sought to assuage concerns about ties to China by working to move some U.S. user information stateside to be stored at a data center managed by Oracle as part of Project Texas.

"In this case individuals misused their authority to obtain access to TikTok user data."

Forbes reported in October that the same China-based ByteDance internal audit and investigations team that oversaw the surveillance campaign against journalists

also investigated TikTok global security chief Roland Cloutier, a U.S. Air Force veteran, who was tasked with overseeing efforts to limit Chinese employees' access to American user data. Cloutier stepped down in July 2022. At least five senior employees who led departments at TikTok recently left the company over revelations that they could not meaningfully influence decision-making, *Forbes* also found.

TikTok and ByteDance declined to comment on specific employee investigations or on the departures.

In August, *Forbes* additionally found LinkedIn profiles for three hundred ByteDance employees that showed they previously worked for Chinese state media publications. Twenty-three of the profiles appeared to have been created by ByteDance directors. At the time, ByteDance spokesperson Jennifer Banks said the company makes "hiring decisions based purely on an individual's professional capability to do the job. For our China-market businesses, that includes people who have previously worked in government or state media positions in China. Outside of China, employees also bring experience in government, public policy, and media organizations from dozens of markets."

ByteDance is not the first tech giant to use an app to monitor specific users. In 2017, the New York Times reported that Uber had identified various local politicians and regulators and served them a separate, misleading version of the Uber app to avoid regulatory penalties. At the time, Uber acknowledged that it had run the program, called "greyball," but said it was used to deny

ride requests to "opponents who collude with officials on secret 'stings' meant to entrap drivers," among other groups.

Both Uber and Facebook also reportedly tracked the location of journalists reporting on their apps. A 2015 investigation by the Electronic Privacy Information Center found that Uber had monitored the location of journalists covering the company. Uber did not specifically respond to this claim. The 2021 book *An Ugly Truth* alleges that Facebook did the same thing, in an effort to identify the journalists' sources. Facebook did not respond directly to the assertions in the book, but a spokesperson told the *San Jose Mercury News* in 2018 that, like other companies, Facebook "routinely use[s] business records in workplace investigations."

But an important factor distinguishes ByteDance's collection of private users' information from those cases: TikTok told lawmakers in June that access to certain U.S. user data — likely including location — will be "limited only to authorized personnel, pursuant to protocols being developed with the U.S. Government."

Brendan Carr, an FCC commissioner who called on Apple and Google to ban TikTok following the June BuzzFeed News report, said: "At the precise moment when TikTok is trying to convince U.S. officials that it can be trusted—when it has every incentive to ensure the security of user data—its Beijing-based parent company abused its systems to obtain data on reporters that are covering TikTok? This should be the final nail in the coffin for the idea that U.S. officials can trust TikTok."

This story has been updated to incorporate additional information from TikTok and ByteDance.

MORE FROM FORBES

MORE FROM FORBES

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

By **Emily Baker-White**

MORE FROM FORBES

A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns

By **Emily Baker-White**

MORE FROM FORBES

TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say

By **Emily Baker-White**

MORE FROM FORBES

LinkedIn Profiles Indicate 300 Current TikTok And ByteDance Employees Used To Work For Chinese State Media-And Some Still Do

By **Emily Baker-White**

*Follow me on **Twitter**. Send me a secure **tip**.*

Emily Baker-White Follow

I'm a technology reporter and senior writer at Forbes based in San Francisco. Have a tip? Email me at ebakerwhite@forbes.com or emilybakerwhite@protonmail.com.

Editorial Standards Reprints & Permissions

India Banned TikTok In 2020. TikTok Still Has Access To Years Of Indians' Data.

forbes.com/sites/alexandralevine/2023/03/21/tiktok-india-ban-bytedance-data-access

March 21, 2023

In 2020, Indians burned posters with the TikTok logo in support of their government for banning the Chinese-owned app.
NOAH SEELAM/AFP/GETTY IMAGES

India's 150 million users were forced to stop using the Chinese-owned app in 2020. But an internal tool reviewed by *Forbes* showed that ByteDance and TikTok employees can still mine some of their most sensitive data. One employee called it "NSA-To-Go."

By Alexandra S. Levine, Forbes Staff

Almost three years after TikTok's largest market, India, banned the Chinese-owned social media app over geopolitical tensions, troves of personal data of Indian citizens who once used TikTok remain widely accessible to employees at the company and its Beijing-based parent, ByteDance, *Forbes* has learned.

The revelation comes as President Joe Biden's administration threatens to ban the platform used by more than 100 million Americans if TikTok's Chinese owner does not sell its stake. Officials in the highest levels of the U.S. government see a blanket TikTok ban as a possible solution to the country's national security concerns about the potential for China to surveil or manipulate Americans. Some have called India a "guide star," urging the U.S. to follow its lead.

"I don't think [Indians are] aware of how much of their data is exposed to China right now, even with the ban in place," a current TikTok employee told *Forbes*.

According to the employee and a review of internal TikTok and ByteDance programs by *Forbes*, almost anyone at the companies with basic access to their tools can retrieve and analyze granular data about past TikTok users in India. (ByteDance has more than 110,000 employees around the world, including in China and Russia, but reportedly fired its entire India staff last month.) Another source also independently confirmed that Indians' data has been accessible since the country banned the app.

> "I don't think [Indians are] aware of how much of their data is exposed to China right now, even with the ban in place."

One social mapping tool—which the TikTok employee jokingly called "NSA-To-Go"—can spit out a list of any public or private user's closest connections on TikTok and personally identifiable information about them, and it still pulls up the TikTok profiles of people in India, according to a review by *Forbes*. Staff can plug in a TikToker's unique identifier or UID, a string of numbers tied to more detailed data about the person, to retrieve the TikTok usernames (often, first and last name) of hundreds of friends and acquaintances; the region where they live; and how they share TikTok content with phone contacts and users across other social platforms. The same UID can be used across TikTok and ByteDance's other internal tools to find even more information about the person—including their search behavior. The TikTok employee described it as a key to building a "digital dossier" on any user, including those with private accounts.

"We have steadfastly complied, and continue to remain in full compliance, with the Government of India order since it was implemented," TikTok spokesperson Jason Grosse said in an email. "All user data is subject to our robust internal policy controls surrounding access, retention, and deletion." ByteDance did not respond to a request for comment.

The purpose of India's 2020 ban appears to have focused on preventing public access to TikTok in the country going forward, given concerns about the app potentially sending data it had collected on Indian users back to China. (Nikhil Gandhi, who was then head of TikTok in India, said at the time that TikTok had "not shared any information of our users in India with any foreign government, including the Chinese government.") The ban did not seem to call for deletion of app data that had already been captured and stored.

As a result, the profiles of Indian users who once used TikTok can still be found online, though their owners haven't been able to post since the 2020 ban. The company would not say how many Indian accounts can be viewed in the internal tool, but TikTok had roughly 150 million monthly active users there at the time it was shut down, according to data analytics firm Sensor Tower. The data in this particular tool appears to be frozen in time for the India users; for other countries like the U.S., where TikTok is widely used today, it updates in real-time.

The current TikTok employee told *Forbes* that nearly anyone with basic access to company tools—including employees in China—can easily look up the closest contacts and other sensitive information about any user. That includes everyone from prominent public figures to the average person, according to the employee and a *Forbes* review of the tool. In the wrong hands, the employee noted, that information could be dangerous.

"From [their social graphs], if you want to start a movement, if you want to divide people, if you want to do any kind of operation to influence the public on the app, you can just use that information to target those groups," they said. This powerful demographic data, especially on TikTok's unmatched Gen Z userbase, could also be highly valuable for commercial purposes, the employee added.

> "We can't ban them from the data they already have."

Beyond the India case, company-wide access to a tool like this could be highly problematic in the context of geopolitical conflict. Data on users from Ukraine and Russia, including details about who they communicate with on the app, has been available in the tool, according to the TikTok employee and internal materials obtained by *Forbes*. Though there is no known instance of this tool or others at TikTok being used against foreign adversaries, such information could jeopardize the safety of soldiers and citizens alike.

"When an authoritarian country like China is able to amass a lot of information about citizens in another country, that's going to raise all sorts of red flags," former National Security Agency general counsel Glenn Gerstell told *Forbes*. He said that while he thought it might be hard for China to actually weaponize that information in practice, it "absolutely raises concerns, heightens tensions [and] puts them in a position potentially to do mischief with the data. And that's obviously a threat."

TikTok has already used its arsenal of tools to target individuals and their networks. A December *Forbes* investigation revealed that ByteDance had tracked multiple journalists who cover the company, gaining access to their IP addresses and other data to try to uncover which ByteDance employees may have been in proximity to them and potentially leaking information. The company vehemently denied that report until its own internal investigation proved it to be accurate, heightening fears across the U.S. government that such surveillance could be conducted on Americans more broadly. The FBI and Justice Department are now investigating ByteDance's use of TikTok to spy on journalists, as *Forbes* first reported. The White House has also ordered federal agencies to wipe TikTok from government employees' devices by the end of this month.

Got a tip about TikTok or ByteDance? Reach out securely to the author, Alexandra S. Levine, on Signal/WhatsApp at (310) 526-1242, or email her at alevine@forbes.com.

TikTok's retention of Indians' data shows why, stateside, a consensual agreement between TikTok and the Committee on Foreign Investment in the U.S. might be far more effective than a ban, Gerstell said. (CFIUS and TikTok have been in talks since 2019 on a deal to address national security concerns about the app.) He said a CFIUS deal could lock down historical data, which the India ban apparently failed to do, and that it would give the U.S. government the ability to set the terms around what happens to Americans' data from past and present. Though a consensual deal wouldn't guarantee that China won't find a way to access that old data, it could afford other protections, he explained.

"If it's a ban—which is the same thing in India—we can't ban them from the data they already have," Gertstell said. "Whatever the data is up to that moment of the ban is TikTok's, is ByteDance's...and we have no legal basis, if all we're doing is banning the thing, to tell them what to do with [it]." It gets even more complicated if the data is already stored outside U.S. jurisdiction, he added.

"The politicians, and the people pounding the table when they talk about bans, in their mind think they're solving a problem," he told *Forbes*, "and they absolutely aren't."

Emily Baker-White contributed reporting.

MORE FROM FORBES

MORE FROM FORBESTikTok's China ProblemBy Emily Baker-WhiteMORE FROM FORBESThe FBI And DOJ Are Investigating ByteDance's Use Of TikTok To Spy On JournalistsBy Emily Baker-WhiteMORE FROM FORBESTikTok CEO Is Quietly Meeting With Lawmakers Ahead Of First-Ever TestimonyBy Alexandra S. LevineMORE FROM FORBESIn The Face Of Attacks, TikTok Tries To Charm Its Critics With TransparencyBy Alexandra S. LevineMORE FROM FORBESHow A TikTok Ban Would Work - And How TikTok Could Fight BackBy Emily Baker-

WhiteMORE FROM FORBESEXCLUSIVE: TikTok Spied On Forbes JournalistsBy Emily Baker-White

Follow me on Twitter. Check out my website. Send me a secure tip.

Alexandra S. Levine

I'm an investigative features writer at Forbes covering technology and society. I previously spent three years covering tech for Politico and three years as a staff columnist at The New York Times.

Phoebe Liu

Forbes Staff

Mar 21, 2023,12:00am EDT

Cornell Brooks Public Policy
Tech Policy Institute

Banning TikTok: What's At Stake and Would a Ban Address the National Security Risk?

Sarah Kreps
Director, Tech Policy Institute
Cornell University

Joshua Clark
Cybersecurity Fellow, Tech Policy Institute
Cornell University

Introduction

In the last several years, the bilateral relationship between the United States and China has become increasingly fraught. Although the growing tensions manifest across all issues, nowhere are they more clearly manifested than in the technology space. Consequently, the United States Government has taken a series of precautionary measures aiming to slow China's tech advancement, specifically in the area of artificial intelligence, semiconductor chips, and 5G technologies. Alongside these measures, the United States has taken notice of the potential for China to misuse data of American citizens. In 2016, a Chinese company bought a gay dating app, Grindr, and the Committee on Foreign Investment in the United States (CFIUS) concluded that Chinese ownership was a national security risk and required that China sell the app, which took place in 2020. In the meantime, TikTok has become a popular social media platform, with 150 million Americans on the platform. Congress has proposed a ban on TikTok, the White House has said it welcomes a bill that would allow it to ban the app, and the TikTok CEO is testifying on Capitol Hill on March 23, 2023.

This policy brief seeks to answer the key questions at stake with a possible TikTok ban. It considers the national security questions motivating debates about the ban, whether a ban would address these risks, whether proposed alternatives–a sale of TikTok or an initiative that would move the data to Texas–would mitigate these risks, the legal grounds for a ban, and how, technically, a ban might work.

What national security concerns does TikTok represent?

TikTok reports over 150 million American users and is owned by the Chinese company ByteDance. A 2017 Chinese National Intelligence Law requires that Chinese entities "support, assist and co-operate" with Chinese intelligence efforts, which has been interpreted to suggest that Chinese-owned companies might be required to share user data with the government. Chinese government access to user data presents two major categories of concern:

Privacy and user data protection

- TikTok collects vast amounts of user data, including location, device information, and user interactions, which could be exploited to build detailed profiles on individuals or to track user activities and preferences.

- TikTok's ownership by ByteDance, a Chinese company, raises concerns about the potential for the Chinese government to access or misuse users' data for espionage or surveillance purposes. Although TikTok says that "since beginning transparency reporting in 2019, we have received zero data requests from the Chinese government," interpretations of the national intelligence law suggest that the company would indeed have to turn over data if asked in the future.
- Certain American individuals hold high intelligence value based on their occupation, location, and interests. While government employees and service members are prohibited from using TikTok on their devices, industry leaders, journalists, researchers in strategic industries, or relatives of government employees are still at risk of foreign intelligence leveraging their personal data.

TikTok as a vector for information warfare

- TikTok has a powerful aggregate user data model that reflects the general preferences and psychology of 150 million American users. By understanding the average mindset of, for example, a 22-year-old American college student, foreign actors are better positioned to manipulate that person psychologically through targeted messaging and curated content.
- TikTok's algorithmic content distribution, young audience, and inherent access to user data and psychological profiles make it a powerful platform for targeted misinformation and propaganda campaigns.
- Foreign actors have proven capable of leveraging social media to attempt to influence elections or exacerbate social division. Inside access to the TikTok algorithm or specific user data would be a powerful tool to achieve these ends, though no evidence of influence operations occurring through TikTok exists.

Would a TikTok ban significantly reduce these risks?

A ban would not significantly reduce data privacy risks. While it would prevent TikTok from collecting new data on US users, it would not eliminate the data already collected, which is backed up to servers in Singapore and potentially accessible from China. This ban would also not address the broader issue of data privacy risks posed by the lack of US privacy and data security regulation. Leaked user data from American social media apps is readily available online, and brokers sell data obtained from these American apps with no regulatory supervision to buyers that could easily include Chinese intelligence. Foreign actors do not need TikTok's data or continued operation to engage in disinformation or influence campaigns.

A ban on TikTok would significantly reduce the short-term risk of TikTok specifically being used as a vector for information warfare, as removing access would reduce the virality of misinformation or propaganda on the platform. However, given the existing historical aggregate data on American preferences obtained by TikTok since 2018 and the ready availability of data from other social media apps online, the long-term information warfare risks represented by having the models of American citizen's preferences available for purchase will remain with or without TikTok until more comprehensive privacy legislation is enacted, or accountability mechanisms for all tech companies are strengthened.

Does Project Texas significantly reduce these risks?

Project Texas is the proposal by TikTok to mitigate privacy concerns by storing all American user data in a Texas data center operated by US-based Oracle and 3rd party auditors. From a policy standpoint, Project Texas represents the most stringent set of privacy requirements any social media company has ever been required to comply with. These measures would include localizing all US data, careful access control over

data passing in and out of Oracle's cloud, full visibility into the recommendation system, and making Oracle responsible for compiling the app source code and delivering it to app stores. These steps are inarguably all positive.

However, there are some technical concerns about the feasibility of auditing TikTok's codebase, which is reportedly millions of lines. The prevailing understanding within the cybersecurity community is that there are "always backdoors" within a system this large, and that auditing such a codebase could turn into a "cat and mouse game." Additionally, these measures do not mitigate the risks represented by China using TikTok as a vector for propaganda or disinformation, and do not remove what historical data may have been collected. Finally, as the Chinese division of ByteDance has a full copy of the source code that drives TikTok, their current or ex-employees are uniquely positioned to understand and take advantage of any legacy security vulnerabilities, even after the codebase is transitioned over to US control.

Is a TikTok ban legal?
The Trump White House issued an Executive Order on August 6, 2020 that aimed to ban TikTok. The proposed ban met with a series of legal obstacles. One US District judge stated that "the Government's own descriptions of the national security threat posed by the TikTok app are phrased in the hypothetical" and that the president had overstepped his emergency economic powers that the Trump Executive Order had cited. Another District Judge determined that the Administration had not considered alternatives other than a ban on TikTok.

When President Biden took office, he formally rescinded the ban, but the Committee on Foreign Investment in the US (CFIUS) began examining whether a Chinese-owned social media company can adequately safeguard Americans' data. As the process has dragged on, members of Congress and increasingly President Biden have become impatient. In March 2023, a bipartisan group of Senators announced the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act, the type of statutory reform that would pave the way for a legal and therefore more successful ban than was attempted in 2020. The bill, endorsed by the White House, would grant the Commerce Department the power to regulate technology produced by countries "adversarial" to the United States. Importantly, the bill would circumvent the Berman amendments, Cold War-era measures that restricted the president's authority to regulate or ban imports of "informational materials" from adversarial nations, by authorizing the Commerce Secretary to prohibit "transactions." Further, rather than focusing on an individual app, its emphasis on transactions means that hardware, software, quantum computing, synthetic biology, and robotics would all be included, giving it more longevity than an app-specific bill. Constitutional law history generally suggests that the courts give considerable latitude to the executive branch on issues of national security and that the legislative statutory reform would provide a more unassailable path toward a ban compared to when the ban was attempted in 2020.

What are the technical options to enforce a TikTok ban? Is this feasible?
While some tools exist to enact a TikTok ban, motivated users will be able to find ways to continue to use the app. As TikTok relies on network effects and user-generated content, adding friction to the user experience will likely decrease the total user count and reduce the amount of new data collected by ByteDance, However, the US government does not have an existing technical infrastructure to enforce these bans, and would need to lean on partners in the tech industry to implement these changes.

Three major mechanisms for bans are detailed below, along with the feasibility and effectiveness.

Network ban: Direct Internet Service Providers (ISPs) to block traffic to and from TikTok

- ISPs route traffic for mobile devices via cellular and WiFi networks. By denying access to TikTok IP addresses, no content can be sent to or received from existing TikTok apps or via browser. This practically renders the app useless.
- This method can be circumvented using VPNs, or tools that allow users to route their traffic through 3rd party intermediaries hosted outside the US and therefore not required to block TikTok IPs. VPNs are easily downloadable on iOS and Android.

App Store ban: Direct Apple and Google to remove TikTok from app stores

- Apple and Google remove apps that break the law or their terms of service, and have complied with similar orders in India.
- App store bans limit new downloads, and gradually degrade the stability of existing users by blocking application updates.
- This method can be circumvented through sideloading or downloading apps directly from 3rd party stores or websites. Sideloading is currently possible on Android devices and jailbroken iPhones, though recent EU legislation will require sideloading for all EU iPhones with iOS 17.

Financial ban: Direct US companies to suspend business relationships with TikTok

- By suspending these relationships, TikTok would be unable to monetize via advertising, pay creators, or have server or content delivery infrastructure within the US.
- This method can be circumvented by moving server operations to Canada, South America, or Europe. This would result in some degree of latency, but not so much as to be unacceptable to users.
- This method will not necessarily reduce the incentive for influencers to create content, as the majority of content creators monetize through bespoke brand deals and growing their audience on higher-paying social media platforms such as Youtube, not through TikTok's ad program.
- This method was successfully challenged on legal grounds during the Trump administration, though the new RESTRICT legislation may re-enable this approach.

Are there examples of apps or technology being banned? How successful were these efforts?
India implemented network and app store bans for more than 56 Chinese apps, including TikTok, successfully. In the aftermath, local apps replicating the functionality of the banned apps were adopted, and replaced the use of the banned apps, despite the ability for motivated or technical users to circumvent the bans.

China blocks practically all American owned social media apps through their national firewall. They also act as vendors for internet censorship technology to other countries interested in limiting assembly online. Nearly all social media is centralized to large players, such as WeChat, and are required to provide backdoor access to Chinese intelligence. Individuals can still access sites through VPNs but there is no doubt that the firewall complicates access, which achieves the intended goal.

The US has issued a ban on PokerStars/internet poker, which led to a massive user drop, though a smaller community remains in states where it remains legal. For almost a century the United States has restricted the

export of data encryption technology as it would a bomb or missile, although encryption software is nearly ubiquitous. The US has instituted export controls on artificial intelligence to China to slow the military and economic advancement of the country. Export controls, or in this case bans, are not intended to prevent the use but slow the spread or make it more inconvenient to the point that users choose alternatives.

***Should* the US impose a TikTok ban?**

American citizens seem to have decided that they value user experience and personalized content more than their privacy, which is resulting in a growing national security concern. To address this issue, steps need to be taken across the social media landscape to better protect private user data and incentivize tech companies to take on that responsibility. Motivated users would likely continue to find ways to use the app after a ban, but as with other social media platforms, TikTok is characterized by strong network effects. If major influencers find it inconvenient or less financially attractive, they may migrate elsewhere and draw their followers with them, denting the potential national security value of user data.

A TikTok ban will not fully address the underlying national security concerns around user data and privacy, however. Moreover, the United States, as a democracy, will be taking steps that impede the ability of the TikTok constituency (young Americans), to express themselves and earn a livelihood. Given the potentially limited benefits and costs of a TikTok ban, legislators should consider establishing more comprehensive data privacy protections, and push for mitigation strategies such as Project Texas, before resorting to a ban.

https://www.wsj.com/articles/tiktok-algorithm-sex-drugs-minors-11631052944

BUSINESS

How TikTok Serves Up Sex and Drug Videos to Minors

The popular app can quickly drive young users into endless spools of adult content, including videos touting drug use and promoting pornography sites

By Rob Barry Follow *, Georgia Wells* Follow *, John West* Follow *, Joanna Stern* Follow *and Jason French*

Sept. 8, 2021 7:59 am ET

The account was one of dozens of automated accounts, or bots, created by The Wall Street Journal to understand what TikTok shows young users. These bots, registered as users aged 13 to 15, were turned loose to browse TikTok's For You feed, the highly personalized, never-ending feed curated by the algorithm.

An analysis of the videos served to these accounts found that through its powerful algorithms, TikTok can quickly drive minors—among the biggest users of the app—into endless spools of content about sex and drugs.

TikTok served one account registered as a 13-year-old at least 569 videos about drug use, references to cocaine and meth addiction, and promotional videos for online sales of drug products and paraphernalia. Hundreds of similar videos appeared in the feeds of the Journal's other minor accounts.

TikTok also showed the Journal's teenage users more than 100 videos from accounts recommending paid pornography sites and sex shops. Thousands of others were from creators who labeled their content as for adults only.

Still others encouraged eating disorders and glorified alcohol, including depictions of drinking and driving and of drinking games.

The Journal shared with TikTok a sample of 974 videos about drugs, pornography and other adult content that were served to the minor accounts—including hundreds shown to single accounts in quick succession.

Of those, 169 were removed from the platform before the Journal shared them—whether by their creators or TikTok couldn't be determined. Another 255 were removed after being shared with the company, among them more than a dozen portraying adults as "caregivers" entering relationships with people pretending to be children, called "littles."

The woman in the role-playing video said she wished TikTok did a better job of keeping adult content out of minors' feeds.

"I do have in my bio that is 18+ but I have no real way to police this," she wrote in a message. "I do not agree with TikTok showing my content to someone so young."

A spokeswoman declined to address the content of the individual videos, but said the majority didn't violate guidelines. She said TikTok removed some of the videos after the Journal's accounts viewed them, and restricted the distribution of other videos to stop the app from recommending them to other users, but declined to say how many.

The spokeswoman said the app doesn't differentiate between videos it serves to adults and minors but said that the platform is looking to create a tool that filters content for young users.

TikTok's terms of service say that users must be at least 13 years old, and that users under 18 need consent from their parents.

"Protecting minors is vitally important, and TikTok has taken industry-first steps to promote a safe and age-appropriate experience for teens," the spokeswoman said in a statement. She noted that the app allows parents to manage screen time and privacy settings for their children's accounts.

The addiction machine

An earlier video investigation by the Journal found that TikTok only needs one important piece of information to figure out what a user wants: the amount of time you linger over a piece of content. Every second you hesitate or re-watch, the app tracks you.

Through that one powerful signal, TikTok can learn your most hidden interests and emotions, and drive users of any age deep into rabbit holes of content—in which feeds are heavily dominated by videos about a specific topic or theme. It's an experience that other social-media companies like YouTube have struggled to stop.

"All the problems we have seen on YouTube are due to engagement-based algorithms, and on TikTok it's exactly the same—but it's worse," said Guillaume Chaslot, a former YouTube engineer who worked on that site's algorithm and is now an advocate for transparency in how companies use those tools. "TikTok's algorithm can learn much faster."

The Journal assigned each of its 31 minor accounts a date of birth and an IP address. Most were also programmed with various interests, which were revealed to TikTok only through lingering on videos with related hashtags or images and through scrolling quickly past the others. Most didn't search for content and instead simply watched videos that appeared in their feed.

Here's how that can work:

The creator promoting the 420 friendly website didn't respond to questions about the video being shown to an account registered to a 13-year-old.

About a dozen of the Journal's 31 minor accounts ended up being dominated by a particular theme.

This can be especially problematic for young people, who may lack the capability to stop watching and don't have supportive adults around them, said David Anderson, a clinical psychologist at The Child Mind Institute, a nonprofit mental-health care provider for children.

He said those teens can experience a "perfect storm" in which social media normalizes and influences the way they view drugs or other topics.

Even when the Journal's accounts were programmed to express interest in multiple topics, TikTok sometimes zeroed in on single topics and served them hundreds of videos about one in close succession.

TikTok served one account, which had been programmed with a variety of interests, hundreds of Japanese film and television cartoons. In one streak of 150 videos, all but four featured Japanese animation—many with sexual themes.

The TikTok spokeswoman said the Journal's bots "in no way represents the behavior and viewing experience of a real person," in part because humans have diverse and changing interests. She added that the platform was "reviewing how to help prevent even highly unusual viewing habits from creating negative cycles, particularly for our younger users."

The spokeswoman said that when users encounter something they don't want to see, they can select "not interested" to see less of that content.

Dozens of the videos promoting paid pornography have since been deleted from the app.

In some cases, TikTok creators were clear about not wanting children to see their videos, labeling them (or their accounts) as for adults only. But the app served them anyway.

In one stretch of 200 videos, nearly 40% were labeled as being for adults only.

In all, at least 2,800 such videos were served to the Journal's minor accounts.

The proliferation of sexually charged content has stirred concerns inside TikTok. Videos directing people to OnlyFans were so abundant that in a meeting in the fall of 2020, the company's chief operating officer, Vanessa Pappas, asked employees to explain what the site was, according to a person familiar with the meeting.

After the meeting, TikTok at first decided to ban content directing users to OnlyFans, since employees argued much of the content on the site is pornographic, the person familiar with the decision said. The platform then decided to allow users to link to the site after other

employees pointed out that not everything on OnlyFans is X-rated, and that other social-media platforms allow links to the content.

The TikTok spokeswoman said that it prohibits nudity and sexual solicitation and removes accounts that redirect users to sexual content or services, including on OnlyFans.

A spokeswoman for OnlyFans said the site is strictly for people 18 years and older and declined to comment on TikTok accounts directing people to the site.

Policing

TikTok relies on a combination of algorithms and more than 10,000 people to police its huge and growing volume of content, according to former executives of the company.

The company said in a recent report that it removed 89 million videos in the second half of last year.

But it has been hard to keep up with the app's growth, the former executives said: TikTok now has about 100 million users in the U.S. consuming and producing videos, from about 25 million in 2019.

The company said that users upload tens of thousands of videos every minute.

To keep pace, moderators focus on the most popular content, leaving videos with lower view counts largely unreviewed, the former executives said.

In July, TikTok said that in the U.S. it would begin relying on its algorithms to both identify and remove certain types of videos that violate its rules in an effort to enforce its rules more quickly. Previously, TikTok's algorithms identified rule-breaking videos, but humans reviewed them before removal.

The company made the announcement after the Journal shared hundreds of examples of potentially rule-breaking content that the app had served its bots. TikTok said it has been experimenting with this new system over the past year.

TikTok's spokeswoman said that no algorithm will ever be completely accurate at policing content because of the amount of context that goes into understanding a video, particularly ones about drugs.

TikTok has also struggled to eradicate video posts promoting eating disorders.

Policing content has been complicated by the company's decisions in recent years to loosen some restrictions in the U.S., including around skin exposure and bikinis, according to several former executives and content moderators.

The result has been more sexualized videos on the platform, the people said.

The spokeswoman for TikTok said the company's policies evolve in response to industry norms and changing user behavior. She also said the company expects new and different content as TikTok's audience grows older and more diverse.

And that bot account registered for a teenage user that fell into the world of role-playing and other sexually oriented content?

—Kara Dapena, Joel Eastwood, Dave Cole, Maureen Linke and Siung Tjia contributed to this article.

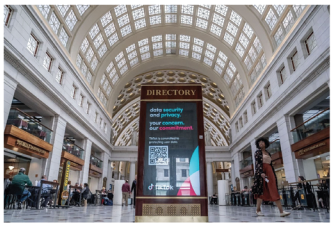
Appeared in the September 9, 2021, print edition as 'TikTok Serves Up Sex and Drug Videos To Young Users'.

https://www.wsj.com/articles/china-says-it-opposes-a-forced-sale-of-tiktok-1a2ffc62

BUSINESS

China Says It Opposes Forced Sale of TikTok

Biden administration demands that video app divest itself from its Chinese parent or face a U.S. ban



A TikTok advertisement at Union Station in Washington, D.C., addresses user security and privacy concerns.
PHOTO: NATHAN HOWARD/BLOOMBERG NEWS

By Raffaele Huang Follow

Updated March 23, 2023 9:09 am ET

SINGAPORE—China said it would strongly oppose any forced sale of TikTok, responding for the first time to a Biden administration demand that the short-video app divest itself from its Beijing-based parent ByteDance Ltd. or face a nationwide ban.

The comments came hours before TikTok Chief Executive Shou Zi Chew testifies Thursday at a congressional hearing over national-security concerns about user data. They put TikTok in the middle of geopolitical tensions between the U.S. and China that have largely centered around technology.

China's Commerce Ministry said Thursday that a sale or divestiture of TikTok would involve exporting technology and had to be approved by the Chinese government.

The reported efforts by the Biden administration would severely undermine global investors' confidence in the U.S., said Shu Jueting, a ministry spokeswoman.

"If the news is true, China will firmly oppose it," she said, referring to the forced sale.

The Biden administration has demanded that TikTok's Chinese owners sell their stakes, citing national-security concerns that Beijing could access U.S. users' data and influence the content that Americans consume.

Mr. Chew will be questioned Thursday over safety and security concerns about the Chinese-controlled platform that is popular in the U.S. He has said divesting the company from its Chinese owners doesn't offer any more protection than a multibillion-dollar plan TikTok has already proposed to ringfence U.S. user data.

ByteDance and TikTok didn't immediately respond to requests for comment after the ministry issued its stance. The companies have said they wouldn't share data with the Chinese government even if requested.

Beijing has increasingly signaled its desire to protect Chinese technology. It recently proposed to amend a

regulation restricting the export of Chinese-created content-recommendation algorithms, a secret sauce of TikTok's global success, which lawyers say is a reminder that Beijing has a hand to play in any deal.

TikTok has more than 150 million users in the U.S., its most lucrative market.

In 2020, when the Trump administration was pushing for a sale of TikTok's U.S. operations, China added algorithms to an export-control list. Any deals that involve transferring such technologies developed in China to a third party outside the country now require government approval.

ByteDance said at the time that it had applied for government approval for the preliminary agreement it reached with Oracle Corp. and Walmart Inc. to set up a new U.S. entity, TikTok Global. The idea eventually fell by the wayside, and China's official records show ByteDance has never received an approval for tech export.

TikTok's recommendation algorithm was initially developed from algorithms and artificial-intelligence models created by its parent, people familiar with the company have said, though the app's systems run on servers in Singapore and the U.S.

TikTok also shares a common algorithm architecture with ByteDance's China-focused video-sharing app Douyin, they said.

In recent exchanges with Beijing officials, ByteDance executives have understood that Beijing is very likely to block a sale or divestiture of TikTok's U.S. operations, even though the officials didn't explicitly say that, people familiar with the matter said Thursday. The authorities have encouraged ByteDance to firmly defend its interests, they said.

—Grace Zhu contributed to this article.

Write to Raffaele Huang at raffaele.huang@wsj.com

Corrections & Amplifications
Shu Jueting is a spokeswoman for China's Commerce Ministry. An earlier version of this article incorrectly spelled her name as Shu Yuting. (Corrected on March 23)

← **Thread**

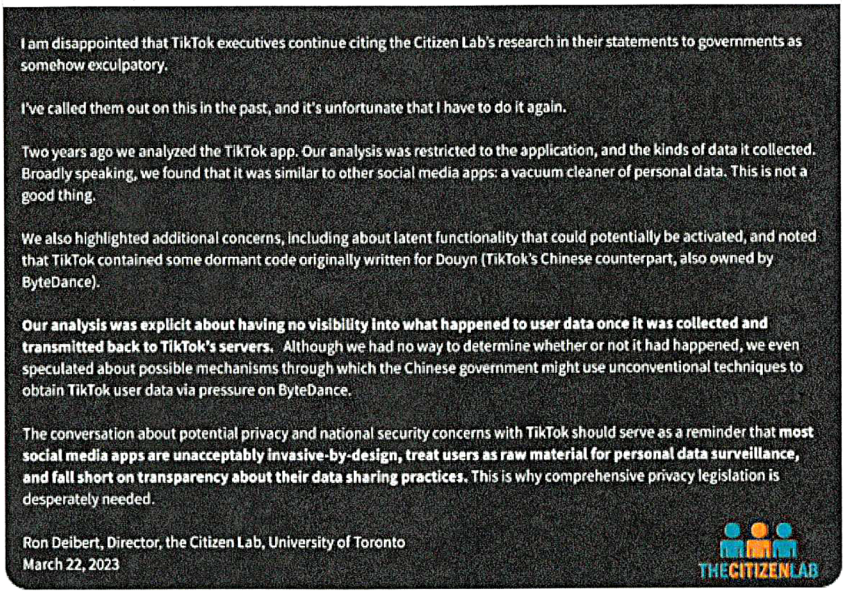
John Scott-Railton
@jsrailton

Citizen Lab doesn't hand out Good Housekeeping seals of approval to apps.

And if we did, #TikTok wouldn't get one.

Their execs need to stop citing our research in their testimony as somehow exculpatory.

> **profdeibert** @RonDeibert · 8h
> My statement about #TikTok's continuing reference to @citizenlab research 👇
> Show this thread



11:10 PM · Mar 22, 2023 · **23.6K** Views

36 Retweets **154** Likes **5** Bookmarks

I am disappointed that TikTok executives continue citing the Citizen Lab's research in their statements to governments as somehow exculpatory.

I've called them out on this in the past, and it's unfortunate that I have to do it again.

Two years ago we analyzed the TikTok app. Our analysis was restricted to the application, and the kinds of data it collected. Broadly speaking, we found that it was similar to other social media apps: a vacuum cleaner of personal data. This is not a good thing.

We also highlighted additional concerns, including about latent functionality that could potentially be activated, and noted that TikTok contained some dormant code originally written for Douyn (TikTok's Chinese counterpart, also owned by ByteDance).

Our analysis was explicit about having no visibility into what happened to user data once it was collected and transmitted back to TikTok's servers. Although we had no way to determine whether or not it had happened, we even speculated about possible mechanisms through which the Chinese government might use unconventional techniques to obtain TikTok user data via pressure on ByteDance.

The conversation about potential privacy and national security concerns with TikTok should serve as a reminder that **most social media apps are unacceptably invasive-by-design, treat users as raw material for personal data surveillance, and fall short on transparency about their data sharing practices.** This is why comprehensive privacy legislation is desperately needed.

Ron Deibert, Director, the Citizen Lab, University of Toronto
March 22, 2023

THECITIZENLAB

Crunch Time for TikTok and Americans' Freedom of Speech

March 22, 2023 / Caitlin Vogus

A nationwide ban on TikTok in the U.S. may violate the First Amendment and won't protect users

TikTok may be operating on borrowed time in the United States, as Congress and the White House increasingly target the social media app. Both the House and Senate have proposed a flurry of bills aimed squarely at TikTok, some of which would ban the app entirely in the U.S. Others would give the President or federal agencies the authority to restrict or ban foreign-owned information technology services like TikTok, or impose transparency requirements on services that store data in China. The White House has demanded that the Chinese company that owns TikTok, ByteDance, sell the app to divest it of Chinese ownership, and has threatened to ban TikTok in the U.S. if it does not. All of this follows laws passed in several states and Congress that prohibit TikTok on government-issued devices.

Lawmakers and the Biden administration say these steps are needed because TikTok may give the Chinese government access to private information about the app's users and allow it to influence TikTok's content moderation. TikTok denies these claims and, in any case, asserts they can be addressed through structural mechanisms of the sort it has proposed to the Committee on Foreign Investment in the United States (CFIUS).

It's true that many social media platforms and other consumer-facing technologies, including TikTok, pose privacy concerns — and that governments, including China, use social media for disinformation campaigns or to otherwise try to influence public opinion. However, a nationwide ban on TikTok is not the answer to these concerns. Banning TikTok would undermine free expression in the United States and abroad, and it would not solve the problems the government believes TikTok creates.

A nationwide ban on TikTok would raise serious First Amendment concerns by directly restricting users' ability to speak and receive information. Americans — especially younger Americans — use TikTok to both spread and find information about many important topics, including police brutality against Black people, LGBTQ rights, labor movements, the experiences and rights of people with disabilities, reproductive health, campus safety, and environmental policy and climate change. Some users participate in our democracy through TikTok, by hosting or viewing voter registration campaigns or subscribing to official accounts of political candidates, elected officials, or government entities.

The Supreme Court has long recognized that the First Amendment protects not only the right to speak, but also the right to receive information – including the right to receive information from abroad. For example, in the 1960s, the Supreme Court struck down a federal law requiring the Postmaster General to detain "communist political propaganda" printed or prepared in a foreign country and mailed to the U.S., notify the addressee, and deliver the mail only upon request. Recognizing the likely deterrent effect of requiring an addressee to affirmatively request delivery of materials the government had labeled as communist propaganda, the Court held that the law violates the First Amendment. It explained that the government cannot "control the flow of ideas to the public," including ideas (even propaganda) from abroad.

The Court has also held that prohibiting too much protected speech can violate the First Amendment, especially if a law forecloses a unique and important means of communication. These First Amendment limits ensure that people can exercise other First Amendment rights of speech, press, and assembly and protect Americans' participation in our democracy. For example, voters who are informed about political candidates and issues are better able to exercise their right to vote.

While other online services may remain available, a TikTok ban would foreclose users from speaking and receiving information through an important and distinct medium of expression. TikTok's users choose to use the app to reach particular audiences, especially young people connecting with other young people, and because of its distinctive capabilities for communication. Just as the Supreme Court has recognized that bans on yard signs, pamphlets, or live entertainment are not permitted under the First Amendment simply because other means of expression remain available, a ban on TikTok suppresses a unique medium of expression and suppresses too much speech.

Banning TikTok in the U.S. would also be what's known as a "prior restraint" on speech, or a limit imposed on speech before it happens. A ban would prevent the millions of Americans who use TikTok from being able to speak through the app in the future and would prohibit new users from downloading the app. This "freeze" on TikTok users' speech would come with a heavy presumption against its constitutional validity. The Supreme Court has long recognized that the chief purpose of the First Amendment is to prohibit prior restraints and that prior restraints can be justified only by the most extraordinary circumstances. In the past, the Court has rejected even justifications based on national security interests, explaining that the First Amendment permits a prior restraint only when the government can demonstrate that "disclosure . . . will surely result in direct, immediate, and irreparable damage to our Nation or its people."

Empowering the government to suppress TikTok nationwide may also mean giving it startling powers to censor, monitor, and screen other online services. While it is not clear how such a ban would be carried out as a technical matter, it could take the form of prohibiting app stores from carrying TikTok, potentially impinging on the First Amendment rights of app stores themselves (to make their own choices about what apps they host in their stores), as well as the rights of individuals to access communications apps. In addition, an app store prohibition may, ironically, create

security risks for American TikTok users by preventing them from downloading updates to the app that fix security vulnerabilities. Alternatively, a ban may require internet service providers (ISPs) to engage in filtering to block the service from American users, furthering concerns about prior restraints and potentially opening the door to other types of censorial filtering at the ISP level.

Not only would a TikTok ban suppress the speech of Americans, but it would also provide other countries with a justification for banning online services that facilitate free expression in their countries. While a ban on an entire online speech service would be novel in the United States, other countries have unfortunately already adopted this approach to silence criticism and dissent. Turkey, for example, has repeatedly blocked social media sites such as YouTube and Twitter, citing national security concerns. Most recently, Turkey sparked outrage after constraining access to Twitter and TikTok following devastating earthquakes in that country and arresting scores of people for "sharing provocative posts." A ban on TikTok in the U.S. would embolden governments worldwide — authoritarian and democratic alike — to impose their own restrictions on social media services in the name of privacy and national security. As a result, billions of people worldwide may lose access to the online services that provide easy to use, freely available outlets for their speech.

In addition to potentially violating the First Amendment and undermining free expression worldwide, a TikTok ban would not necessarily help protect Americans' privacy. Even if banning TikTok would remove the Chinese government's ability to collect data on Americans directly from the app, there are other avenues it could use to obtain this data. Private data brokers routinely sell data to American law enforcement and intelligence agencies and face no legal barrier to selling data from other social media apps to the Chinese government or its proxies – or other foreign governments or potentially hostile actors. If Congress is serious about addressing risks to Americans' privacy, it could accomplish far more by focusing its efforts on passing comprehensive privacy legislation like the American Data Privacy and Protection Act.

Concerns that the Chinese government could put a thumb on TikTok's content moderation decisions to spread disinformation and propaganda are also not appropriately addressed by a ban. Even if the Chinese government — or any foreign country — uses TikTok or other social media in this way, the First Amendment prohibits the government from banning a service because it disagrees with the viewpoints expressed on it. Instead, counterspeech, both in the form of investigations that reveal disinformation campaigns and speech responding to and debunking disinformation, are the better way to respond to this concern while preserving free expression.

It is also important that any action that the government takes against TikTok or any other online service that facilitates speech on the basis of national security be done transparently, with sufficient information made available to the public so Americans can judge for themselves whether the government's action is necessary. Not only should the government be required to give a public explanation of its actions "if practicable" (as one proposed bill states), but there should be a strong presumption that the government

must make the reasons for a ban or other restriction, and evidence supporting those reasons, publicly available. The government should not be able to keep its justification secret on the basis of nebulous or unjustified national security or law enforcement interests. The government's reasons for taking action against a speech intermediary like TikTok would also be at the heart of a court's consideration of a First Amendment challenge to those actions, since courts apply a high level of scrutiny to government restrictions on speech based on content or viewpoint.

In the midst of these debates over legislation to ban TikTok, the company has been negotiating a national security agreement with the Committee on Foreign Investment in the United States (CFIUS). According to reports by those briefed on TikTok's proposal, nicknamed Project Texas, TikTok would create a new subsidiary based entirely in the United States that would control access to U.S. users' data and content moderation decisions. The U.S. entity would be controlled by an independent board of directors selected by TikTok but approved by CFIUS, and the board would also report to CFIUS. Data from U.S. users would be hosted in the United States by Oracle, which would also oversee TikTok's content moderation and recommendation algorithm in the U.S., and report potential risks to the government, "which will then have the authority to inspect the issue in more detail."

Some have criticized Project Texas as not doing enough to protect Americans from Chinese spying and influence, and CFIUS has not, to date, approved the plan. It has negotiated with TikTok since 2019 and can reject the plan and order divestiture. If it becomes the basis for resolution of the concerns that prompted the CFIUS review, Project Texas may raise First Amendment problems of its own, particularly if it empowers the government to oversee and overrule a private online service's editorial decisions about what content to host, bar, recommend, or deprioritize.

However, given the serious negative impacts of an outright ban on freedom of expression and the fact that it will not solve the privacy concerns that Congress claims motivate these bills, the government should consider other paths. If the government does not believe Project Texas sufficiently protects Americans' interests, it should explain the basis for its objections and why no other mitigation measures can adequately address the risk. Suppressing speech should be used only as an absolute last resort, in response to a government interest of the highest importance. The U.S. government should not undermine online free speech with an ill-conceived ban that sets a dangerous precedent for the U.S. and countries around the world.

Dear Member of Congress,

We, the undersigned organizations, write to express our concern about federal legislation and proposals that seek to impose a wholesale ban on TikTok in the United States. If passed by Congress and enacted into law, a nationwide ban on TikTok would have serious ramifications for free expression in the digital sphere, infringing on Americans' First Amendment rights and setting a potent and worrying precedent in a time of increased censorship of internet users around the world. A ban on TikTok by means of executive action would have a similar impact.

We recognize the grave concerns that TikTok and other social media platforms pose for the privacy of individual users. We are also aware and we recognize that U.S. government officials have cited serious concerns with respect to the threat that TikTok may pose to U.S. national security. ByteDance's prevarication in response to repeated queries about its handling of American users' data is unacceptable. But solutions short of a full-scale ban can address these vulnerabilities without resorting to an ill-advised, blanket approach that would impair free speech and set a troubling precedent that could curtail free expression worldwide.

The rise of apps like TikTok poses novel challenges to the digital commons. Nearly 150 million Americans use TikTok[1] to connect, and to create and share content. Whether they use the app to live stream, promote a small business, share their creative work, connect with family, or find information on how to vote, their speech is protected by the First Amendment. The Supreme Court has long recognized that the First Amendment encompasses the right to receive information, irrespective of its source, free from government interference.[2] If the government were to intervene to ban TikTok entirely, it would impair the rights of citizens to communicate in a manner of their choosing, giving rise to significant First Amendment concerns.

The Supreme Court has recognized that the digital realm is currently "one of the most important places to exchange views."[3] People in the U.S. have a constitutional right to speak via the internet, and to do so on the platform of their choosing. For citizens, and particularly the tens of millions of young Americans who use TikTok, to witness a popular social media platform summarily shut down by the government will raise serious questions in the minds of a rising generation about the sanctity of free speech in our system of governance. Moreover, the enforcement of such a ban could force major changes in the operation of the internet in the United States, including potential requirements on service platforms to police and censor the traffic of users, or even a national firewall to prevent users from downloading TikTok from sources across our borders.

---

[1] TikTok [@tiktok], *Our CEO, Shou Chew, shares a special message on behalf of …* [TikTok video], https://www.tiktok.com/@tiktok/video/7212953186724842795, March 21, 2023.

[2] *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas."); *Red Lion Broadcasting Co., Inc v. FCC 395 U.S. 367, 390* (1969) ("It is the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences … ").

[3] *Reno v. ACLU*, 521 U. S. 844, 870 (1997).

In addition to the implications of a ban on domestic free expression, a legislative ban on TikTok in the U.S. would set an alarming global precedent, lending legitimacy to authoritarian regimes in shutting down and excluding services they disfavor. Major American digital platforms have been banned or severely restricted by governments, including the Chinese Communist Party,[4] Pakistan,[5] and Uganda,[6] among others,[7] seeking to silence dissent and opposition and obstruct the open flow of communication and information. When Nigeria banned Twitter for seven months in June 2021, the U.S. condemned the ban, reiterating its support for "the fundamental human right of free expression and access to information as a pillar of democracy in Nigeria." Last year, the U.S. similarly denounced "Russia's shuttering of independent media and technology platforms,"[8] and when mass protests erupted in Iran after the killing of Mahsa Amini, the U.S. government strongly condemned the actions of the Iranian regime and called on the Iranian authorities to refrain from the "blocking or filtering of services."[9] In 2018, the Department of the Treasury's Office of Foreign Assets Control designated individuals responsible for the blocking of social media applications in Iran as "engaging in censorship activities that prohibit, limit, or penalize the exercise of freedom of expression or assembly by citizens of Iran." If the U.S. were to now put its statutory imprimatur on wholesale banning as a means of redressing its security concerns about digital platforms, other governments will follow suit, insisting that their own security concerns are equally pressing. A ban on TikTok would sorely undermine U.S. credibility as a defender of digital freedom, and invite copycat measures that could lead to severe constriction of expression worldwide.

Measures short of an outright ban may address potential security concerns raised in relation to TikTok. A proposal by Senators Blumenthal and Moran to expedite the investigation by the Committee on Foreign Investment in the United States (CFIUS) into TikTok could yield a plan that would mitigate security risks without denying users access to the platform.[10] A comprehensive consumer privacy bill would limit data commodification, thereby dramatically increasing users' security online. A robust privacy bill could address concerns not just at TikTok but across the multiple social media platforms—current and future—that have proven to be

---

[4]Eglė Juodytė, *Which websites and apps are blocked in China?*, https://nordvpn.com/blog/blocked-sites-china/ (noting blocked sites include Western media sources, social media applications, and search engines), January 3, 2023.

[5]Abid Hussain, *Wikipedia ban in Pakistan over alleged blasphemous content lifted*, https://www.aljazeera.com/news/2023/2/7/wikipedia-ban-in-pakistan-over-alleged-blasphemous-content-lifted, February 7, 2023.

[6]Arthur Arnold Wadero, *Facebook to remain shut as govt talks with tech giant stall*, https://www.monitor.co.ug/uganda/news/national/facebook-to-remain-shut-as-govt-talks-with-tech-giant-stall-3912172, August 12, 2022.

[7]Martin Armstrong, *Where Social Media is Suppressed*, https://www.statista.com/chart/23804/countries-blocking-social-media/, January 17, 2022.

[8]*Statement by NSC Spokesperson Emily Horne on Russian Disinformation and Efforts to Undermine Free Press*, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/05/statement-by-nsc-spokesperson-emily-horne-on-russian-disinformation-and-efforts-to-undermine-free-press/, March 5, 2022.

[9]*Joint Statement on Internet Shutdowns in Iran*, https://www.state.gov/joint-statement-on-internet-shutdowns-in-iran/, October 20, 2022.

[10]Letter from Senators Richard Blumenthal and Jerry Moran to Secretary of the Treasury Janet Yellen (February 16, 2023), https://www.blumenthal.senate.gov/imo/media/doc/20230216cfiustiktok.pdf.

vulnerable to intrusion by the CCP and other foreign governments.[11] It could also mitigate concerns not just of foreign data mining but also hacking, ransomware and other security vulnerabilities.

Current legislative and administrative proposals to ban TikTok risk violating First Amendment rights, and setting a dangerous global precedent for the restriction of speech. More effective, rights-respecting solutions are available and provide a viable alternative to meet the serious concerns raised by TikTok.

Sincerely,

PEN America
Access Now
Advocacy For Principled Action In Government
American Civil Liberties Union
Authors Guild
Center for Democracy & Technology
Fight for the Future
Free Press Action
Knight First Amendment Institute at Columbia University
National Coalition Against Censorship
New America's Open Technology Institute
Organization for Identity & Cultural Development
Public Knowledge
Surveillance Technology Oversight Project
Tully Center for Free Speech
Woodhull Freedom Foundation

---

[11] Twitter, *Disclosing state-linked information operations we've removed*, https://blog.twitter.com/en_us/topics/company/2021/disclosing-state-linked-information-operations-we-ve-removed, December 2, 2021; Twitter Safety, *Disclosing networks of state-linked information operations we've removed*, https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020, June 12, 2020; Ben Nimmo and David Agranovich, *Removing Coordinated Inauthentic Behavior From China and Russia*, https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/, September 27, 2022; Taylor Hatmaker, *Former Twitter employee found guilty of spying for Saudi Arabia*, https://techcrunch.com/2022/08/09/twitter-spy-convicted-saudi-arabia/, August 9, 2022.

The Government Hasn't Justified a TikTok Ban

By Adam Schwartz and David Greene
March 16, 2023

Freedom of speech and association include the right to choose one's communication technologies. Politicians shouldn't be able to tell you what to say, where to say it, or who to say it to. So we are troubled by growing demands in the United States for restrictions on TikTok, a technology that many people have chosen to exchange information with others around the world. Before taking such a drastic step, the government must come forward with specific evidence showing, at the very least, a real problem and a narrowly tailored solution. So far, the government hasn't done so.

Nearly all social media platforms and other online businesses collect a lot of personal data from their users. TikTok raises special concerns, given the surveillance and censorship practices of its home country, China. Still, the best solution to these problems is not to single-out one business or country for a ban. Rather, we must enact comprehensive consumer data privacy legislation. By reducing the massive stores of personal data collected by all businesses, TikTok included, we will reduce opportunities for all governments, China included, to buy or steal this data.

Many people choose TikTok

TikTok is a social media platform that hosts short videos. It is owned by ByteDance, a company headquartered in China. It has 100 million monthly users in the United States, and a billion worldwide. According to Pew, 67% of U.S. teenagers use Tiktok, and 10% of U.S. adults regularly get news there. Many users choose TikTok over its competitors because of its unique content recommendation system; to such users, social media platforms are not fungible.

TikTok videos address topics "as diverse as human thought." Political satirists mock politicians. Political candidates connect with voters. Activists promote social justice. Many users create and enjoy entertainment like dance videos.

Problems with TikTok bans

If the government banned TikTok, it would undermine the free speech and association of millions of users. It would also intrude on TikTok's interest in disseminating its users' videos—just as bookstores have a right to sell books written by others, and newspapers have a right to publish someone else's opinion.

In a First Amendment challenge, courts would apply at least "intermediate scrutiny" to a TikTok ban and, depending upon the government's intentions and the ban's language, might apply "strict scrutiny." Either way, the government would have to prove that its ban is "narrowly tailored" to national security or other concerns. At the very least, the government "must demonstrate that the recited harms are real, not merely conjectural." It also must show a "close fit" between the ban and the government's goals, and that it did not "burden substantially more speech than is necessary." So far, the government has not publicly presented any specific information showing it can meet this high bar.

Any TikTok ban must also contend with a federal statute that protects the free flow of information in and out of the United States: the Berman Amendments. In 1977, Congress enacted the International Emergency Economic Powers Act (IEEPA), which limited presidential power to restrict trade with foreign nations. In 1988 and 1994, Congress amended IEEPA to further limit presidential power. Most importantly, the President cannot "regulate

or prohibit, directly or indirectly," either "any...personal communication, which does not involve a transfer of anything of value," or the import or export of "any information or informational materials." Banning TikTok would be an indirect way of prohibiting information from crossing borders. Rep. Berman explained:

> "The fact that we disapprove of the government of a particular country ought not to inhibit our dialog with the people who suffer under those governments...We are strongest and most influential when we embody the freedoms to which others aspire."

A TikTok ban would cause further harms. It would undermine information security if, for example, legacy TikTok users could not receive updates to patch vulnerabilities. A ban would further entrench the social media market share of a small number of massive companies. One of these companies, Meta, paid a consulting firm to orchestrate a nationwide campaign seeking to turn the public against TikTok. After India banned TikTok in 2020, following a border dispute with China, many Indian users shifted to Instagram Reels and YouTube Shorts. Finally, a ban would undermine our moral authority to criticize censorship abroad.

The 2020 TikTok ban

In 2020, former President Trump issued Executive Orders banning TikTok and WeChat, another Chinese-based communications platform. EFF filed two amicus briefs in support of challenges to these bans, and published three blog posts criticizing them.

A federal magistrate judge granted a preliminary injunction against the WeChat ban, based on the plaintiff's likelihood of success on their First Amendment claim. The court reasoned that the government had presented "scant little evidence," and that the ban "burden[ed] substantially more speech than is necessary."

In 2021, President Biden revoked these bans.

The DATA Act

This year, Rep. McCaul (R-TX) filed the federal "DATA Act" (H.R. 1153). A House committee approved it on a party-line vote.

The bill requires executive officials to ban U.S. persons from engaging in "any transaction" with someone who "may transfer" certain personal data to any foreign person that is "subject to the influence of China," or to that nation's jurisdiction, direct or indirect control, or ownership. The bill also requires a ban on property transactions by any foreign person that operates a connected software application that is "subject to the influence of China," and that "may be facilitating or contributing" to China's surveillance or censorship. The President would have to sanction TikTok if it met either criterion.

It is doubtful this ban could survive First Amendment review, as the government has disclosed no specific information that shows narrow tailoring. Moreover, key terms are unconstitutionally vague, as the ACLU explained in its opposition letter.

The bill would weaken the Berman Amendments: that safeguard would no longer apply to the import or export of personal data. But many communication technologies, not just TikTok, move personal data across national borders. And many nations, not just China, threaten user privacy. While the current panic concerns one app based in one country, this weakening of the Berman Amendments will have much broader consequences.

The Restrict Act

Also this year, Sen. Warner (D-VA) and Sen. Thune (R-SD), along with ten other Senators, filed the federal "RESTRICT Act." The White House endorsed it. It would authorize the executive branch to block "transactions" and "holdings" of "foreign adversaries" that involve "information and communication technology" and create "undue or unacceptable risk" to national security and more.

Two differences between the bills bear emphasis. First, while the DATA Act requires executive actions, the RESTRICT Act authorizes them following a review process. Second, while the DATA Act applies only to China, the

RESTRICT Act applies to six "foreign adversaries" (China, Cuba, Iran, North Korea, Russia, and Venezuela), and can be expanded to other countries.

The RESTRICT Act sets the stage for a TikTok ban. But the government has publicly disclosed no specific information that shows narrow tailoring. Worse, three provisions of the bill make such transparency less likely. First, the executive branch need not publicly explain a ban if doing so is not "practicable" and "consistent with ... national security and law enforcement interests." Second, any lawsuit challenging a ban would be constrained in scope and the amount of discovery. Third, while Congress can override the designation or de-designation of a "foreign adversary," it has no other role.

Coercing ByteDance to sell TikTok

The Biden administration has demanded that ByteDance sell TikTok or face a possible U.S. ban, according to the company. But the fundamental question remains: can the government show that banning TikTok is narrowly tailored? If not, the government cannot use the threat of unlawful censorship as the cudgel to coerce a business to sell its property.

The context here is review by the Committee on Foreign Investment in the United States (CFIUS) of ByteDance's ownership of TikTok. The CFIUS is a federal entity that reviews, and in the name of national security can block, certain acquisitions of U.S. businesses by foreign entities. In 2017, ByteDance bought TikTok (then called Musical.ly), and in 2019, CFIUS began investigating the purchase.

In response, TikTok has committed to a plan called "Project Texas." The company would spend $1.5 billion on systems, overseen by CFIUS, to block data flow from TikTok to ByteDance and Chinese officials. Whether a TikTok ban is narrowly tailored would turn, in part, on whether Project Texas could address the government's concerns without the extraordinary step of banning a communications platform.

Excluding TikTok from government-owned Wi-Fi

Some public universities and colleges have excluded TikTok from their Wi-Fi systems.

This is disappointing. Students use TikTok to gather information from, and express themselves to, audiences around the world. Professors use it as a teaching tool, for example, in classes on media and culture. College-based news media write stories about TikTok and use that platform to disseminate their stories. Restrictions on each pose First Amendment problems.

These exclusions will often be ineffective, because TikTok users can switch their devices from Wi-Fi to cellular. This further reduces the ability of a ban to withstand First Amendment scrutiny. Moreover, universities are teaching students the wrong lesson concerning how to make fact-based decisions about how to disseminate knowledge.

Excluding TikTok from government-owned devices

More than half of U.S. states have excluded TikTok from government-owned devices provided to government employees. Some state bills would do the same.

Government officials may be at greater risk of espionage than members of the general public, so there may be heightened concerns about the installation of TikTok on government devices. Also, government has greater prerogatives to manage its own assets and workplaces than those in the private sector. Still, infosec policies targeting just one technology or nation are probably not the best way to protect the government's employees and programs.

The real solution: consumer data privacy legislation

There are legitimate data privacy concerns about all social media platforms, including but not limited TikTok. They all harvest and monetize our personal data and incentivize other online businesses to do the same. The result is that detailed information about us is widely available to purchasers, thieves, and government subpoenas.

That's why EFF supports comprehensive consumer data privacy legislation.

Consider location data brokers, for example. Our phone apps collect detailed records of our physical movements, without our knowledge or genuine consent. The app developers sell it to data brokers, who in turn sell it to anyone who will pay for it. An anti-gay group bought it to identify gay priests. An election denier bought it to try to prove voting fraud. One broker sold data on who had visited reproductive health facilities.

If China wanted to buy this data, it could probably find a way to do so. Banning TikTok from operating here probably would not stop China from acquiring the location data of people here. The better approach is to limit how *all* businesses here collect personal data. This would reduce the supply of data that any adversary might obtain.