115th CONGRESS
2nd Session

Printed for the use of the
Commission on Security and Cooperation in Europe

Lies, Bots, and Social Media: What is Computational Propaganda and How Do We Defeat It?

NOVEMBER 29, 2018

Briefing of the
Commission on Security and Cooperation in Europe

Washington: 2019

Commission on Security and Cooperation in Europe
234 Ford House Office Building
Washington, DC 20515
202–225–1901
csce@mail.house.gov
http://www.csce.gov
@HelsinkiComm

Legislative Branch Commissioners

HOUSE
CHRISTOPHER H. SMITH, NEW JERSEY
Co-Chairman
ALCEE L. HASTINGS, FLORIDA
ROBERT B. ADERHOLT, ALABAMA
MICHAEL C. BURGESS, TEXAS
STEVE COHEN, TENNESSEE
RICHARD HUDSON, NORTH CAROLINA
RANDY HULTGREN, ILLINOIS
SHEILA JACKSON LEE, TEXAS
GWEN MOORE, WISCONSIN

SENATE
ROGER WICKER, MISSISSIPPI,
Chairman
BENJAMIN L. CARDIN. MARYLAND
JOHN BOOZMAN, ARKANSAS
CORY GARDNER, COLORADO
MARCO RUBIO, FLORIDA
JEANNE SHAHEEN, NEW HAMPSHIRE
THOM TILLIS, NORTH CAROLINA
TOM UDALL, NEW MEXICO
SHELDON WHITEHOUSE, RHODE ISLAND

Executive Branch Commissioners

DEPARTMENT OF STATE
DEPARTMENT OF DEFENSE
DEPARTMENT OF COMMERCE

ABOUT THE ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

The Helsinki process, formally titled the Conference on Security and Cooperation in Europe, traces its origin to the signing of the Helsinki Final Act in Finland on August 1, 1975, by the leaders of 33 European countries, the United States and Canada. As of January 1, 1995, the Helsinki process was renamed the Organization for Security and Cooperation in Europe (OSCE). The membership of the OSCE has expanded to 56 participating States, reflecting the breakup of the Soviet Union, Czechoslovakia, and Yugoslavia.

The OSCE Secretariat is in Vienna, Austria, where weekly meetings of the participating States' permanent representatives are held. In addition, specialized seminars and meetings are convened in various locations. Periodic consultations are held among Senior Officials, Ministers and Heads of State or Government.

Although the OSCE continues to engage in standard setting in the fields of military security, economic and environmental cooperation, and human rights and humanitarian concerns, the Organization is primarily focused on initiatives designed to prevent, manage and resolve conflict within and among the participating States. The Organization deploys numerous missions and field activities located in Southeastern and Eastern Europe, the Caucasus, and Central Asia. The website of the OSCE is: <www.osce.org>.

ABOUT THE COMMISSION ON SECURITY AND COOPERATION IN EUROPE

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is a U.S. Government agency created in 1976 to monitor and encourage compliance by the participating States with their OSCE commitments, with a particular emphasis on human rights.

The Commission consists of nine members from the United States Senate, nine members from the House of Representatives, and one member each from the Departments of State, Defense and Commerce. The positions of Chair and Co-Chair rotate between the Senate and House every two years, when a new Congress convenes. A professional staff assists the Commissioners in their work.

In fulfilling its mandate, the Commission gathers and disseminates relevant information to the U.S. Congress and the public by convening hearings, issuing reports that reflect the views of Members of the Commission and/or its staff, and providing details about the activities of the Helsinki process and developments in OSCE participating States.

The Commission also contributes to the formulation and execution of U.S. policy regarding the OSCE, including through Member and staff participation on U.S. Delegations to OSCE meetings. Members of the Commission have regular contact with parliamentarians, government officials, representatives of non-governmental organizations, and private individuals from participating States. The website of the Commission is: <www.csce.gov>.

Lies, Bots, and Social Media: What is Computational Propaganda and How Do We Defeat It?

NOVEMBER 29, 2018

Page

PARTICIPANTS

Lies, Bots, and Social Media: What is Computational Propaganda and How Do We Defeat It?

November 29, 2018

Commission on Security and Cooperation in Europe
Washington, DC

The briefing was held at 10:33 a.m. in Room 562, Dirksen Senate Office Building, Washington, DC, Mark Toner, State Department Senior Advisor, Commission on Security and Cooperation in Europe, presiding.

Panelists present: Mark Toner, State Department Senior Advisor, Commission on Security and Cooperation in Europe; Paul Massaro, Policy Advisor, Commission on Security and Cooperation in Europe; Matt Chessen, Acting Deputy Science and Technology Advisor to the Secretary of State, U.S. Department of State; Ambassador Karen Kornbluh, Senior Fellow and Director, Technology Policy Program, The German Marshall Fund of the United States; and Nina Jankowicz, Global Fellow at the Woodrow Wilson International Center for Scholars' Kennan Institute.

Mr. TONER. Good morning, and thanks to all of you for joining us for what I hope is just the start of an ongoing discussion on a topic that is increasingly relevant to all of us in the digital age, and that is computational propaganda and, more broadly, disinformation spread via digital platforms. My name is Mark Toner and I'm joined today by my colleague Paul Massaro.

On behalf of the Commission on Security and Cooperation in Europe, a.k.a. the Helsinki Commission, and the commission's chairman, Senator Roger Wicker, I wanted to thank our three panelists today, each of whom are experts on the issue of computational propaganda and, more broadly, online disinformation—what it is, where it originates, how it works, and what we can do to stop it or at least better manage it, all, of course, while preserving our bedrock freedom of expression.

It's been said we live in a post-truth world. Indeed, information technology has moved at such a pace that many of us have lost our ability to delineate between fact and fiction, a vulnerability that adversaries, either individuals or political groups or corporations or even, God forbid, foreign governments have sought to exploit. It's my hope that our discussion today will unpack not only why this is happening but also how we can best try to fix it.

It's a conversation, of course, that has to include all the different players—that's industry, civil society, and government, of course—and employ technology and policy in new and creative ways. And while there's certainly plenty of blame to go around in our slow response to this threat, there are, I hope, real solutions that we can pursue that can return the internet to the promise of its early days.

Our first speaker, Matt Chessen, is a career U.S. diplomat, technologist, and author who is currently serving as the acting deputy advisor in the Office of Science and Technology to the secretary of state. It's his job to connect State Department foreign policy priorities to research, development, and discoveries emerging from the high tech and private sectors. Matt also manages the development of policy portfolios for artificial intelligence and computational propaganda, and Matt's written and spoken extensively on the problem of computational propaganda and how to address it through AI [artificial intelligence] and other technology.

Our second panelist is Karen Kornbluh, who is currently the senior fellow and director for the technology policy program at the German Marshall Fund of the United States. Karen was previously with the Council on Foreign Relations, where she was the senior fellow for digital policy. She also served as U.S. Ambassador to the OECD [Organisation for Economic Cooperation and Development] from 2009 to 2012, where she spearheaded the development of the first internet policymaking principle.

And our third panelist today is Nina Jankowicz, a global fellow at the Woodrow Wilson Center's Kennan Institute, who is currently working on a book about the evolution of modern Russian influence campaigns in Eastern Europe. She's also advised the Ukrainian Government on strategic communications, and her op-eds have been published in The New York Times and Washington Post, among others. She's also a frequent commentator on disinformation in Russian and Eastern European affairs.

Each of our panelists will give brief remarks before we open it up to questions. They'll talk about different aspects of computational propaganda. Matt will give us a bit of history about why this is such a threat to our core democratic values, provide an overview of computational propaganda, bots, and AI, and then talk a bit about left-brain right-brain solutions to the problem.

Karen will give us more historical context—recent historical context on how we've gotten to this point, from the internet's early promise to today's algorithm-driven platforms. And Nina will talk about some of the platforms—what some of the platforms have done to address the problem, why it's not enough, and also offer some possible solutions. And then, of course, we'll have a discussion. We'll open it up to your questions.

So, Matt, do you want to start us off?

Mr. CHESSEN. Sure. Thank you, Mark, for the excellent overview and introduction.

As Mark said, I'm going to start off by talking about the civilizational context for these issues. So we really need to ask ourselves, why do we care about computational propaganda, weaponized narratives. Why do we care about the possibility of a post-truth world? And I really like the answer that's provided by Arizona State University and it's also mentioned actually by General Michael Hayden quite a bit, and then it's these—the possibility of a post-truth world actually directly undermines the enlightenment ideals of the search for truth through reason.

And so if you go back to the founding of our country, the Founding Fathers were Enlightenment Era thinkers. The Constitution is probably the most important Enlighten-

ment Era document. And so the ideas in the Constitution set the foundation for modern democracy. These democracies are based on rule of law systems where the empirical thinking is really core to their functioning. And so facts and evidence are really critical for everything from administrative due process to judicial processes and evidence.

So if we actually start getting into this post-truth world where a fact is just whatever you can convince people of, then facts don't matter and this is a direct threat to the evidence-based rule of law system that modern democracy is based upon. So I always tell people it's very important that we push back on this idea that we're in a post-truth world. There is an objective reality. Facts do matter. Expertise matters and evidence matters. If we do concede that we're in a post-truth world, then countries, organizations, or even people with very strong information operation capabilities and a casual relationship with the truth can hold inordinate amounts of power.

So if you take the principle that democracy is the superior system and, based on evidence, people would come to that conclusion but you're in a post-truth world, then countries like Russia and China can convince their own populations and the populations of other countries that democracy is inferior to authoritarian rule.

Some people speculate that the challenges we're facing with weaponized narrative and computational propaganda and disinformation spell the end of the enlightenment and I actually want to push back on that idea. We can go into this in more detail in the Q&A if everybody is interested but, really, the enlightenment was about the elites using truth and reason to push back on the established institutions of the time.

What you're seeing now is really hyper-empowered individuals using technology to push back on the elites and push back on the institutions that they've been running for a long period of time. And so we've hyper empowered these individuals with really powerful informational tools but we don't yet have the systems and frameworks to ensure accountability and responsibility. We really don't have a lot of trust in the system.

And so we've had over 200 years to create these checks and balances in everything from the government use of power to peer-reviewed research. But we've only had a few decades to create structures for the internet and social media. And so to illustrate how this works, I'd like to talk about what some people call the collective intelligence system.

The collective intelligence system is the way that a society determines truth from fiction. In the mid–20th century, our collective intelligence system consisted of several major national newspapers, a rich local media ecosystem, a few national TV channels, government, academia, and the church, and that's how people basically filtered what's true from what's not true.

But as the information channels have sort of exploded, confidence in these institutions have gone down and some of this is natural evolution just from the diversity of information outlets and some of it is actually manufactured outrage by some of the malicious actors out there. But the net result is that our collective intelligence system of how our society determines truth from fiction really is broken right now.

Into that gap, malicious actors have stepped in and are using new technologies to create their own collective intelligence system. They're creating malicious collective intelligence systems, and what they do is they attract people into these systems with emotionally pleasing disinformation and then they keep them on an emotional hook and never let them go. And so this is what leads us to this idea of computational propaganda.

So let's talk a little bit about what computational propaganda is and give sort of an overview of some of the techniques. The technical term for this is really online information operations. This comes from sort of a military term. But I like computational propaganda because it's good shorthand. Basically, what it refers to is the use of information and communication technologies to manipulate people's perceptions and influence their behavior.

And so computational propaganda uses a variety of different technologies including big data. You have social media, you have autonomous agents like bots and, increasingly, you're starting to see artificial intelligence applications used. People like to focus on the bots but we really need to keep in mind that there's human beings behind all of this and there's human beings being affected by all of this, right.

So the humans create the content. They circulate the content. They're driving the information campaigns, and that's what's really at the core in computational propaganda. It's this coordinated manipulative activity. And so bots are one tool but it's not the only tool that's used. But since it is something that people talk about a lot we'll talk about the bots.

So bots have some advantages over humans that are based both in the technology and based in human psychology. Most of the bots that are out there are what I call dumb bots in that they are not artificial intelligence and, basically, what they do is they post content either on a schedule or in response to some sort of trigger, and this could be a news key word or it could be some sort of prominent person tweeting and then the bots will go and immediately retweet back.

Generally, there's three different types of bots out there. So there's propaganda bots, and these are just trying to push content out in high volume. You've got follower bots, and the follower bots are trying to do astroturfing, and this is what's basically faking grassroots support. They are liking people or content or following people or content to try and push them up and game the algorithms that are determining trending topics, trending people, trending content.

Then you have roadblock bots, which are really trying to undermine free speech, undermine free expression. A lot of this really started out with spamming hashtags where, you know, a group is trying to organize using a hashtag. Some other group will come in and basically just spam that hashtag with garbage so that they can't actually find the content they're interested in. But it also is used for mass intimidation, typically in combination with doxxing—releasing personal information—and then sort of targeted harassment. This happens a lot in authoritarian countries where an independent journalist will be reporting on something and then they'll get threats from it looks like tens of thousands of people who are saying, We know where your kids go to school, we know where you live, we're going to come kill them or kidnap them, and it basically pressures them into self-censoring their speech.

So why do bots work? This is all rooted in human psychology, right? Bots are actually sitting behind social media accounts that typically look like the target audience they are trying to influence, and just from human psychology, people tend to believe people who look like them, act like them, or are sort of the same as them. And so if they see a bunch of bots that look like actual people, like people in their community, they tend to believe them more.

People are also proven to believe ideas if they're endorsed in volume, right? So that's why astroturfing and gaming these algorithms is persuasive. People like and believe what they think other people like and believe. Bots can also undermine expertise. There are some studies that show that in information-rich environments ideals that are endorsed en masse by a group are more persuasive than ideas that are pushed out by experts.

So there's lots of other techniques that computational propaganda plays off of, and I talk about this because we can't just talk about the technology. We actually have to talk about the science behind these things as well.

So what's coming up next? We really need to think about what's coming up with artificial intelligence because there's a number of emerging technologies that are really going to significantly impact the information space.

And I want to preface this with a statement that there's nothing inherently wrong about these technologies. There's nothing inherently bad about them. Technologies are neutral. It's really the malicious actors, the malicious intent, and the malicious effects that we need to focus on. So let's go through some of these technologies.

So, AI chat bots—if you've never used a chat bot I'd encourage you to try one out. There' s a great one that's put out by Microsoft called Zo. There's been one that's been out in Mandarin for a year. It's called Xiaoice. Chat bots are basically bots that are able to have very human-like conversations and a lot of research shows that people develop very close emotional attachments to some of these chat bots. With Xiaoice, people used to proclaim love for Xiaoice. They'd say, Xiaoice, I wish you were a woman who—or a real girl who I could actually marry. They'd say, Xiaoice, you're my only friend who's available all the time, and people tend to have very high levels of engagement with these chat bots.

There is also the emergence of these affective computing systems. And so these are systems that both can portray human emotions very accurately in either sort of avatars or just through text. But they can also detect human emotions. And so if one of these AI systems is interacting with you online, they can detect your emotional state and then target content based on that particular emotional state.

Psychometric profiling is something that a lot of people know about now because of the Cambridge Analytica scandals. So this is the idea that with, really, relatively few pieces of data you can develop very sort of solid profiles of people and determine their political preferences, determine their personality, their sexuality. You can determine skin color from data. And so every American has somewhere between 2[,000] and 5,000 pieces of data that's just for sale through data brokers, and then we give the data away all the time on social media. And these can be used to, basically, build profiles that then can be used for very personalized manipulative content.

Dynamic content creation systems are also an emerging phenomenon. AI systems are already being used to write news articles. If you've ever read a Minor League Baseball article it was probably generated by an AI from a box score from the game. There's also AI systems that are basically generating articles on company financial reports just from the SEC filings. You have AIs that are writing books and screenplays, which are not very good yet. [Laughter.] But they are actually producing some really good visual art that's starting to win contests and also some classical music and electronic music that's actually pretty good. You can hear that on SoundCloud if you want to.

In combination with this sort of dynamic content generation is probably the phenomenon that I'm most concerned about, which is the audio and video manipulation tools,

right. So right now, you can actually clone someone's voice and you can actually take existing video and make subtle manipulations to it that look very realistic and, you know, it's very easy to see how you could take an existing video that's out there on YouTube of a president or some foreign leader, subtly change the video, subtly change the wording in there, and completely change the meaning and cause some sort of crisis.

A lot of people are familiar with sort of the deep fakes phenomenon. This was something where people basically created programs for mapping actresses' faces to pornographic actresses and then, as a lot of things do on the internet, it started out in pornography and then was being used in sort of other entertainment applications.

People were using it to map Nicholas Cage's face to a bunch of different movies that he was never in. I think someone actually put Harrison Ford's face into the "Solo" movie, which was kind of an interesting one that I just saw, and then there's videos of actually—that are dynamically generated where they've taken a bunch of photos of President Obama and an audio track of one of his speeches and then they can dynamically generate as many different versions of that speech with different vocal intonations, different backgrounds behind it.

And so the ability to actually create this sort of pliable and artificial reality is really becoming sort of profound. I like to tell people, you know, that the machines are coming and they want to have a word with us, and we're entering into this era where a lot of the content and a lot of the speech online could be machines talking to people but also machines talking to machines, because those machines are going to be trying to influence people.

But they're not going to be able to tell which accounts have machines behind them, and so you're going to have machines talking to, persuading, arguing with machines, and we could see the social spaces on the internet really sort of overwhelmed with this machine-driven speech and communication. So that could have profound impacts on sort of the democratic spaces for speech and conversation online.

I do also want to just give an overview of how I like to think about some of the solutions to these types of problems. There's a lot of discussion out there about sort of the left—what I call the left brain, or the rational, solutions. And so these are things like media literacy training, teaching critical thinking, fact-checking tools, all these technology tools that are really around, really giving you more information about your information, right.

And so I think these are all incredibly valuable and they're incredibly necessary, but we can't neglect the human element and the emotional element, and the reason that a lot of people consume disinformation is because it resonates with their identity. It's emotionally pleasing to them. And the example I like to use is this idea of what's going on with obesity.

So we have an obesity epidemic in this country. Everybody knows how to lose weight, right, so you eat better and you exercise more, and we give people a huge amount of data and information about their food. If you go into a supermarket and look at any sort of package of food, there's a lot of data and information there. But it doesn't help the problem, right? It's not an informational problem. It has more to do with people's cognition, their psychology, and their emotion.

So I think that's something that's really neglected in this space is really thinking about that. A lot of people just think, Oh, we'll just give people more information about

their information and then they'll make the right decisions. A lot of this is tied into people's identity and a lot of it—I think some of the solutions to this of getting people to believe the truth is actually trying to communicate the truth to them in a way that doesn't throw up their identity-based or their value-based defenses.

We need to combine these left-brain and right-brain solutions together and I think we need to build new institutions of democracy for the 21st century. So unlike these malicious collective intelligence systems, these would be positive democratic collective intelligence systems. These would be open, transparent. They'd include accountability. They'd be based on logic and reason. They'd be bottom-up so they'd be democratically generated. But they also take into account the diversity of values, identities, and beliefs.

I also want to remind people that this is actually critically important. You've got countries like China that are building social credit systems. They're integrating this into their computational propaganda systems. They're integrating this into their surveillance systems, which are increasingly being enabled by AI, and these systems are very effective at exercising top-down control over people.

If they start exporting these systems around the world, you may get sort of serious competition that's highly enabled by technology that really enables this top-down authoritarian social control. And so we don't want that to become the de facto standard for the world. We need to think about what is the democratic alternative of that.

So whether you call it weaponized narratives, computational propaganda, information operations, or simply disinformation, I would say that we are facing a serious challenge to democratic civilization. Now, I'm optimistic because I've been working on this for several years now and in the last couple years I've seen a state change in the amount of awareness, energy, and resources focused on these issues.

But I am concerned and the problem is very serious. We don't want to underestimate the task at hand. We are engaged in a struggle for truth and reason that leads back to the very founding of our country and the creation of modern democracy.

Thank you.

Mr. TONER. That's quite an ending but——

Amb. KORNBLUH. That was great. That was great. Thank you.

Mr. TONER. Over to you, Karen.

Amb. KORNBLUH. Thanks for having me.

Mr. TONER. Sure.

Amb. KORNBLUH. This is really a great conversation. So I'm going to talk to you a little bit about some things that I wrote in an article for *Foreign Affairs*. And the reason I wrote the article is because I was being asked as somebody's who's been around the table for decades as internet policy was being made and was a big booster—and still am a booster of the internet—how could I be saying that we needed to have more regulations—how could I be critical? And I wanted to go back and look at what had been our beliefs at the beginning. What did we do to set up the policy framework of the original internet? And why are we in a different place now?

So I'm going to start by just telling you a little story. So there's this University of Wisconsin researcher and she—Young Mie Kim—and she collected ads in the 2016 election. She had people tape what they were seeing—they were being micro targeted—and send it in to her, and she was combing through it after the election and she just found these horrific, horrific ads. And she would try to trace them back and figure out who had

sponsored them, had they reported to the FEC, did they have a website, had they filed with the IRS, and a bunch of them had just disappeared.

She found one set. They pretended to be travel spots and they would show you—I wish I had a clip of it—they would show you Paris and purport that Paris was now under Sharia law, and they showed the Mona Lisa covered up and, you know, the Eiffel Tower with a big sign in Arabic on it. And it looked like a travel ad and it just had a little clip that it was sponsored and she found out that it was sponsored by a group called Secure America Now, and that was a dead end. And it was only because another group, a watchdog group, Open [Secrets]—opensecrets.org contacted the accountant for the group who mistakenly—he didn't have to do this—sent the IRS filing unredacted that they found out that this was funded by the Mercers.

So I just want to tell you this story to say that there's something wrong in this environment that is supposed to bring more transparency and democracy to all of us when you can have that kind of deception and lack of transparency.

So how did we get here? So a lot of people think that the internet was immaculately conceived in garages and dorm rooms with no policy whatsoever. But, in fact, regulation was there from the beginning to allow it to—allow these entrepreneurs, allow these brilliant engineers to do what they did. In the Clinton administration they called a lot of the steps to create the early framework deregulatory, but actually it was pro-competition, pro-openness.

So what do I mean? In the Communications Act of 1996, they made sure that the underlying telecommunications network would allow the connection of competitive networks. There were spectrum auctions that were contained in the Budget Reconciliation Act of 1993. AOL was allowed to connect to the underlying network without paying the prices that the long distance carriers had to pay. Otherwise, you would have had to pay a permanent charge for sending an email.

There was a limited liability system that was set up for internet platforms. It's referred to as Section 230 of the Communications Decency Act. What it said was we want these platforms to take down incendiary stuff, stuff that's bad for kids, stuff that violates laws, but if you do that, platforms, you won't be considered a publisher so go ahead and do it. And what that's meant over time is that they can't be sued. They're not liable for the information that's on there, and the idea of that was we want this to be a neutral platform. We don't want a lot of friction in the system. We want everybody to be able to speak, and that was the original intention.

On privacy, we have these global principles that came out of the U.S. and were adopted in Canada and then the OECD socialized them—the fair information policy practices that, again, are very based on notice and opt in—and then we had this whole multi stakeholder system where we said instead of having government figure out the ongoing rules we're going to have this very dynamic system where civil society and engineers and so on set the rules for the internet.

So that was the original idea is that we're going to have this—the internet is going to be this competition of the underlying technology space. It's going to be open. Everybody can be a speaker. And at the beginning, it was incredibly exciting and it still is. I mean, people were putting up blogs. Dissidents were able to speak. It was really giving voice to the voiceless and power to the powerless and that was very, very exciting.

But as time went on, as these technologies do, it became much more centralized. So if you look at the social media networks that dominate the internet now, there very much is an intermediary, right. There is a[n] algorithm that mediates which of your friends' postings you see, which of the people that you follow on Twitter you see. This algorithm is determined in order to keep you engaged so that you're online longer, so that more ads can be served to you. So this ad revenue-driven system, this algorithm, really mediates your experience. It's much less that I communicate to anybody I want and they communicate back.

That story about Secure America Now tells you there's a lack of transparency. You didn't know until recently, often, whether something was an ad. Now you know it's an ad but you don't know necessarily who it's coming from. You don't know what kind of data is being collected from you. You don't know who's—whether you're being micro targeted. You often don't know if you're talking to a bot or a human. There are fake accounts or these closed groups. So there's a real lack of transparency in this system whose primary value is, really, transparency.

So there were efforts along the way to update a bunch of policies but they faced obstacles. So the Federal Trade Commission wanted to get rulemaking authority. But it was taken out of a bill. The Obama administration proposed a Consumer Privacy Bill of Rights that didn't get adopted. The FTC, as we all know now, negotiated consent decrees. The one with Facebook really anticipated a lot of the problems that we saw with Cambridge Analytica. But the FTC doesn't have the resources, the manpower, the ability to pay people so that you get sophisticated computer scientists to really follow up on that. The FTC doesn't have subpoena power.

On the campaign spending side, where you could have caught a lot of this stuff if you'd had some of the same kinds of rules as you do on broadcasting but they'd been updated, the FEC—the Federal Election Commission—completely deadlocked. The IRS—I don't know if you all remember this pseudo-scandal under Obama of the IRS was supposedly being biased in looking at charities and whether they were involved in politics.

What that was really about was after Citizens United corporations were allowed to play in politics, and through a series of IRS and FEC decisions, charities, which don't have to disclose their donors, got more and more and more involved in politics. The IRS was really trying to check that. That failed, and so that's a dark money loophole as well for advertising online and various activities online.

And then in the competition space, we have this focus on consumer prices in the antitrust space, and so that doesn't really do much for you when you're in an environment where things are free. So the FTC approved Facebook acquisitions of WhatsApp and Instagram. There's no portability interoperability like there is with telecom.

When I was at the OECD, we negotiated these internet policymaking principles. And the idea was, just as you were saying at the end, we want to have free flow of information. We want to have human rights principles, free expression. Let's not constrain that. But, certainly, governments—individual national governments can set up policy frameworks. But, unfortunately that wasn't followed up on very much.

And then we haven't had the kind of, just stepping back, the big picture conversation that we had when broadcast came into being, even about newspapers at the turn of the century. What is the purpose of this new media and how is it going to further democracy as opposed to undermining democracy?

So when it came to broadcast television we said, well, we're going to have a different First Amendment approach to it because they're using the public airwaves, and so we're going to have a public interest requirement for broadcasters and we don't want them to step all over local news so they're going to have to air local news. They're not going to do certain things in the family hour. They're going to cover both sides. They're going to have to say when it's an ad. They're going to have to provide information to political opponents so they can get the same price for ads.

We had a whole conversation about it, and then we constructed public television to get at some of what you were talking about—what's the positive that we want—and they funded public broadcast stations and CPB did the content. In the case of cable, we got C-SPAN. So we've had these kinds of big societal debates about what's the purpose of a new media in a democracy and we haven't had that conversation.

So the problem is that we're left with the situation that Matt was describing and I just want to highlight two things—two misconceptions that people have about what goes on online. I think they think that the internet reveals politics as they are. So you'll hear people say that how are we to know that when we connected people there would be bad people and our politics is broken. We just really have to fix our politics.

But the internet really changes politics and I think it's really important to pay attention to that. So how does that work? Well, it influences smaller numbers of—it augments and makes seem louder and bigger smaller numbers of voters in smaller states. There are very few media sites—supposed news media sites that are responsible for much of the fake news—that we see all over the internet.

So the Knight Foundation found that just 10 sites were responsible for 65 percent of the fake news and conspiracy site links that appeared on Twitter during the 2016 election. So the long tail is amplified. You get a sense of fake consensus. You join a group—a fake group. Let's say it's Blacktivist, which was a Russian group, or the Tennessee GOP had a fake site that was run by the Russians. You joined the group.

It sounds like you. It's posting things that feel familiar, and then gradually it radicalizes you—and this happens with the YouTube recommendation algorithm as well. They call this affinity fraud. You feel like you're in a group but you're not really in a group. So it creates this fake consensus and, as I said, it changes politics. We have this idea of astroturf in politics—you know, something that pretends to be grassroots but it's really astroturf. This is astroturf on steroids.

So there are a bunch of solutions. What I'd like to see [are] solutions that really focus on transparency. The initial value of the internet was really openness and transparency, and I hate to see discussions where it's presumed that the only solutions have to do with the government coming in and deciding what's true and what's not and who can speak and who can't, or Facebook or Google deciding who can speak and what's not. I think a lot more transparency. I think we're not aware of how much centralization and lack of transparency there is.

So I'll give you a couple of examples. The Honest Ads Act was introduced by Warner and Klobuchar and McCain. It has not passed into law. The platforms have said that they've built these ad transparency data bases. Jonathan Albright has just recently published showing all kinds of problems with even what's contained in the data bases.

But I'd like to see them go even further and have almost a "know your customer" kind of procedure, so that if you're Secure America Now it's not just the front group that's

listed in the ad transparency, but they have to find out who's funding Secure America Now. If you want to advertise online, we need to know who's funding you and that's—if you look at the law, McCain-Feingold, that was a provision that's in there that hasn't actually been validated by the Supreme Court. The Supreme Court has usually found transparency to be of value in political speech.

Another example I just want to throw out there on the news media piece—when you pick up The New York Times, there's all kinds of metadata, if you will, that you don't think about. They've separated out what they claim to be news and what they claim to be opinion, and there's a legal basis for that. You can sue them if something that they claim is news is defamatory. That's less likely on the opinion. So you know that you can trust what's in the front of the paper more than the back because of this legal scheme. They have a masthead that says who their publisher is, who their editors are. There's a byline on the article. You know what their sourcing scheme is because there's generally accepted practices.

When you see an article online, all of that metadata is stripped out. You just see an article—it's from The New York Times. It's from Breitbart. It has the same font. You don't know if they're claiming—often a Breitbart article will sound like news but it's actually—they've put in a couple of woulds and coulds so that if you ever tried to sue them they would say, Oh, no, no, no, it's opinion, or it's satire. You don't know often who's written it. You don't know what the sourcing scheme is, who's paying for it, who's editing it, and what procedures they're using.

So, again, in a mode of transparency, what if the platforms whitelisted outlets that actually followed a certain procedure—commonly accepted journalistic procedure about transparency so you could know that these outlets actually follow the systems and you could find that information. That would do—I think that's sort of in between your two ideas of emotional and informational is let's give a user interface that really helps people understand, gives watchdogs information so they can present a narrative about what's going on.

So those are the kinds of things. I have a bunch of other ideas on that score. But I think we just really have to move away from this idea that the only way to fix the problem is by going right to content. There's a lot we can do in terms of transparency and empowering users.

Mr. TONER. Nina.

Ms. JANKOWICZ. Thanks for having me. It's really an honor to be here with such a distinguished panel, and that was a great segue, Karen. So thank you for that.

So from calling the influence of malign foreign actors on our electoral discourse and processes a "pretty crazy idea"—that's a quote from Mark Zuckerberg in 2016—to inviting regulation, however begrudgingly, the social media platforms have come a long way since 2016. Facebook, Twitter, and Google have made political advertising more transparent, creating searchable data bases of political ads, and have tightened restrictions on who can purchase them.

In order to reduce the amount of fake news being spread by ads, Facebook has updated its policies to block ads from pages that repeatedly share stories marked as false by third-party fact-checking organizations and Twitter's policies no longer allow the distribution of hacked materials. Facebook has attempted to increase authenticity and trans-

parency around the governance of pages as an influence vector—which were an influence vector of Russia's internet Research Agency in 2016.

It claims that administrators of pages with large audiences undergo extra verification in order to weed out fake accounts, and Facebook has also made other adjustments to arm users with information about the pages that they follow. All of the platforms have made adjustments to their algorithms in order to attempt to combat the problem of disinformation. Facebook did this by focusing on content from, quote, "friends and family" while Google's Project Owl changed the search engine's algorithm to surface more, quote, "authoritative content."

And Twitter has reverted its newsfeed to a more chronological timeline with less algorithmic intervention. Facebook and Twitter have also invested more in content moderation to identify and remove content that violates platforms' policies, including those related to false information, fake accounts, and hate speech. This is not an exhaustive list of the changes that they have made in the past 2 years but, rather, an overview of the more well-known and purportedly messianic features meant to deliver us from all means of internet evil.

But I'm here to tell you that they are not enough. Among the features that I've just described, loopholes have been exploited, missteps unforeseen, and pernicious disinformation allowed to flourish to a point where there's no question in my mind that social media self-regulation has been a failure. Just a day before the midterm election, over a hundred Facebook and Instagram accounts likely controlled by the IRA [Internet Research Agency] were still active and Facebook only removed them after a tip from the FBI.

This is a more complicated problem, as my panelists—co-panelists have alluded to, than just playing whack-a-troll or removing fake accounts and increasing transparency on political ad buys. These measures are, of course, first steps toward ensuring authentic healthy online discourse. But even a cursory look through the performance metrics of the ads released by the House Democrats after 2016 reveals that plenty of the 2016 IRA disinformation performed very well organically. Because the IRA had, over time, built trust and community with their audience of sometimes hundreds of thousands of users per page, many people saw and engaged with that content without the purchase of a single ad.

Today, a lot of this type of content is spreading through Facebook's groups, which the platform's algorithms prefers based on the misguided understanding that they promote content between friends and family, and these are not subject to the same level of content moderation that public content is.

Yes, of course, groups are means of connecting people, but they're also breeding grounds for disinformation due to their privacy settings. Closed and secret groups are not searchable or transparent and the content shared in them is only visible to members so Facebook is less likely to moderate the content within them. What's more, the platform still incentivizes and promotes this group activity.

Groups were a key vector in my investigation for BuzzFeed News into fake profiles supporting an independent candidate for Senate in Massachusetts. A number of fake persona[s] controlled not by lines of code but, as Matt pointed out earlier, by humans and thus able to slip by some of Facebook's detection tools for fake accounts would astroturf groups with posts in favor of their candidate, creating the guise of grassroots support for

the campaign. And Columbia University's Jonathan Albright has also researched how groups support the spread of disinformation on Facebook, and he's noted that banned groups and pages and brands such as Infowars often move their activity to closed groups after their public pages have been banned.

Finally, the spotty and opaque enforcement of platforms' terms of service including with brands like Infowars, which have a record of spreading hate speech and disinformation, undermines the entire discussion of content moderation to begin with. Legitimate voices are often being silenced for small infractions, such as repeated uses of profanity, while groups with more considerable public reach that are violating much more serious clauses of the platforms' terms of service are allowed to continue their diatribes until public outcry becomes too great.

And to that end, transparency around take downs, as Karen mentioned, has been lamentable. While Twitter has released the entire archive of take downs related to state-backed activity on its service—and that's a very good move, in my opinion—Facebook releases this content only selectively. For instance, we don't know how many fake individual profiles they've removed since 2016 related to, for instance, the IRA or Iran. They only talk about pages, which is a problem. And Google really never releases this information and this contributes to the opacity of the problem and both the congressional and public lack of understanding of how best to solve it.

But I do believe that, especially with the new Congress coming in, there's an opportunity to join together in a bipartisan manner and address this issue, and I have a few ideas about where this might start. I agree with Karen that the Honest Ads Act needs to be passed and I think it should be passed before 2020. There's no reason that online political advertising, which, in 2018, saw at least a 200 percent increase in spending compared with the 2014 midterms, should be subject to different rules than TV, radio, and print ads.

The sooner these rules are harmonized across platforms, including smaller online advertisers—right now, the legislation focuses on kind of the big kahunas and I think we need to talk about the smaller ones as well—and integrated with existing FCC and FEC regulations, the safer and more equitable our electoral processes will be. But as I noted earlier, regulating advertising only covers a fraction of the malicious information shared on social media. So I believe that Congress should really push for more transparency surrounding groups, pages, and some of the fronting organizations that purchase ads, as was mentioned before.

And, further, I think Congress should explore the establishment of a specialized independent regulatory or oversight mechanism that could harmonize definitions of concepts like hate speech, abuse, and disinformation across the internet because right now all of the terms of service define these concepts differently and that makes it extremely hard to implement an overarching solution related to them.

They ought to define and require that platforms obtain informed and meaningful consent to terms of service, serving as an awareness-building mechanism about data privacy issues and the limits of speech on the platforms, because they are not free speech zones. They are private platforms. They could also serve as a neutral appellate body for users who feel their content has been unjustly removed, which right now there is a really limited appeals process, as well as conduct public audits of algorithms, account take downs, and data stewardship.

And then, finally, Congress also should consider the role of education, in particular, media and digital literacy, critical thinking skills and civics, and I totally agree with Matt's point that this needs to be considered from an emotional point of view as well in protecting online discourse and empowering citizens. Congress could consider earmarks for grants for educational initiatives in this area. I detailed a lot of this in testimony before the Senate Judiciary Committee earlier this year, so you can look that up if you're interested. [1]

But I'd also be interested in exploring the use of taxes or fines paid by social media companies to fund such initiatives. The U.K. is looking into this right now. Ultimately, these are generational investments and ones that Congress needs to begin now because no regulatory or oversight solution can be complete without an informed and discerning electorate, in my opinion.

Finally, I think it's just important to note the critical awareness building and oversight role that Congress can play even without the passage of new legislation. It was pressure from investigative journalists and Congress that led the social media platforms to begin to reform over the past couple of years and that should continue in the new Congress.

Thank you very much.

Mr. TONER. Thanks very much. Those were three very good and very comprehensive presentations. I don't know if I should run from the room screaming with some of the—you certainly broadened my awareness and I've covered or looked at this issue for many years. But the extent of the sea change, however you want to frame it—seismic change—in the way we communicate is sometimes overwhelming.

I'll start with a question. Someone said—you've addressed it, Nina, and then others as well—but to what extent is this a question of a lack of competition in the industry and, really, a lack—because of that lack of motivation on some of these companies to make the kind of changes such as greater transparency, such as sourcing political ads in a way that show where they come from and what—and kind of buyer beware, readers can see where they come from—to what extent is the problem that, that you've got a few companies who dominate the space as opposed to the internet of the 1990s where it was just big open space that everyone thought would bring greater freedom of expression and what not?

And my second question is maybe best to you, Matt, but others can chime in, is how close are we with AI to having the tools to look at content and trace it back to where it's coming from and provide that transparency to users?

Mr. CHESSEN. Okay. So I'll talk about the second one first. So on AI there [are] various aspects to this. When you're talking about the automated detection of malicious behavior, this is something where there is a lot of advances in this area. There's a lot of companies out there now that are—their business model is basically around helping companies and organizations identify this coordinated manipulative behavior and they're using AI and machine learning techniques to do a lot of this.

I heard a statistic from Twitter that just a couple years ago they were only filtering about 20 percent of the accounts that were suspended using automated tools. The rest were, basically, filtered and reviewed by people. Now it's about 95 percent, and of that 95 percent, 75 percent of those accounts are actually suspended before they even push out

[1] https://www.c-span.org/video/?c4735072/nina-jankowicz-testimony-senate-judiciary-committee; https://www.judiciary.senate.gov/imo/media/doc/06-12-18%20Jankowicz%20Testimony.pdf

one tweet. So they're actually able to identify patterns of behavior that are highly correlated with this malicious behavior before people are even pushing out content. So there's a lot more use of these types of tools.

Now, the problem is that when you're actually going and looking at the content—so a lot of the success in this area is in a very content-neutral type of way. They're using these tools to really identify these patterns in behavior where different accounts that may not seemingly be connected to each other are in fact engaging in coordinated manipulative activity and some of these platforms are actually changing their terms of service to specifically ban that type of activity.

They're not necessarily looking at content in the first instance. There's a lot of challenges with that because AI systems just aren't that good at extracting meaning yet from the content. And so this is going to develop over time. The problem we have, really, right now is either over fit issues or under fit issues, right.

So you're either basically suspending accounts for journalists who are talking about ISIS as well as the actual people that are promoting the ISIS ideology, or you have an under fit issue where you're not getting enough of the extremist content that's out there, right, or enough of the disinformation that's out there.

So this is when we start filtering based on content that's sort of fraught with problems, right. What we don't want to do in this case is do anything that censors legitimate speech, and we don't want to undermine free expression online. But anytime you're starting to make decisions about this content is good, this content is bad—Karen, you mentioned sort of this whitelisting, blacklisting—I think if you do that off of objective criteria that's one thing. If you start going into what the content is and making content decisions, that becomes a lot more problematic, and right now AIs are just not good at figuring out what the meaning is in content well enough to have sort of these automated filtering tools that are just going to basically—that's not going to solve the problem for us.

Amb. KORNBLUH. Just a minor addition to that. I think that's why it's useful, what I was trying to say, is to focus on the outlet rather than the content and the practices of the outlet, and even better, transparency as a key practice of the outlet so that you're not doing that. I think the problem with what they're doing is it doesn't get at some of these issues where the First Amendment talks about the press and I think online we treat the press as just another speaker, and I think having a legitimate press as part of our information integrity is incredibly important.

And if you have an outlet like the Daily Caller, the Koch Brothers, apparently, fund—this just came out over the weekend—close to 100 percent of the Daily Caller Foundation, which supplies the content for what's, in large part—not completely, not every piece of content on there is false—but a lot of conspiracy theories. The birther stuff came out there, the caravan stuff. We don't want to be looking at the content and saying, this is false—this is true.

But you step back and that outlet functions in a very different way from what we consider traditional press and we have to have some objective fashion to get these—these platforms should welcome some objective fashion of getting them out of the business of deciding whether or not an outlet like that is going to be treated exactly the same as the Washington Post or The New York Times. But they haven't welcomed that and so now they're up in front of the Judiciary Committee again, being accused of censoring.

Ms. JANKOWICZ. One quick update. On my way here, I saw that Facebook has now updated its ad policies related to publishers, so news organizations that are buying ads to promote content related to political or issue organizations. So they're no longer going to be subject to the same disclosures, which is a good development. It should have been that way to begin with and I'm glad that they've heard the outcry.

On the AI point that Matt was talking about, there are a couple of examples of AI false positives related to the ad transparency that I have seen. There was a researcher who is at the University of Pittsburgh, I believe, who has a podcast about Russia and was talking about how Russians view Trump, and he was not allowed to place that ad for his podcast because it had the words Russia and Trump in it, and even when he appealed a number of times to a human being, still, he was not allowed to place that out without becoming a certified political advertiser. So that's one of those wrinkles that the platforms don't seem to be keen to figure out.

And then going back to Mark's initial question about whether these platforms just have too much market share, I certainly think it's a problem. In preparing for this panel, I read a little bit about the jurisprudence related to antitrust law, and Karen touched on it. It seems like new regulations are going to need to be developed if there's any way forward in that regard.

Karen, maybe you want to speak about that a little bit. I don't know. [Laughter.] It's a big thorny issue. It certainly seems to me that Facebook should not have the market share it has not only with its billions of users but with WhatsApp and Instagram under its wings as well. And that's all I'll say about that.

Mr. CHESSEN. I just want to mention that point on lack of competition. I mean, I think I haven't made up my mind on this one. But I would like to point out, you know, who remembers MySpace? Who remembers Friendster, right? So they dominated—I'm surprised. It looks like a younger crowd tonight. [Laughter.]

So, you know, they dominated the social media space and then Facebook came along and out-innovated them. And I don't see necessarily major obstacles to other companies coming in and out-innovating Facebook. I think there are some concerns around sort of things like data portability, right, and the fact that probably one of the most valuable things about Facebook for a lot of people is just the network of contacts that you build and that would be very hard to replicate on any other platform.

So I think there are things that can be done in maybe a regulatory context or, you know, through legislation that could basically improve the opportunities for other companies to basically have the ability to innovate and compete. But I am also not necessarily convinced that Facebook and Google or Twitter or anyone else is not vulnerable to the type of disruption that Friendster and MySpace experienced.

Mr. TONER. Paul.

Mr. MASSARO. All right. Great. Well, thank you all so much. I have two sort of totally unrelated questions, so I'd like to ask the first and then get some answers, if anyone wants to bite, and then I'll ask a second.

And my first actually deals with an innovation topic, and that's to say: You know, it seems to me like a lot of the issue is how these platforms are monetized and that was through ads, right, essentially through the use of user data in some capacity. As consumers sort of get hip as to what's going on and as platforms come under fire for exploitation, have we seen any trend toward subscription-based models, other forms of alter-

native monetization that would sort of reduce the problem in just kind of like a, just a standard sort of creative destruction kind of pattern? I know WhatsApp at some point had like—you pay a dollar a year. And obviously it's hard to do ads with an end-to-end encrypted service, even if it's owned by Facebook.

Ms. JANKOWICZ. I think I would say we've seen kind of the opposite, at least in Europe, with the GDPR [General Data Protection Regulation] regulations, in which people can opt out of their data being used for advertising and still use the service. In fact, it's a requirement of the legislation that people can opt out and still use the service. It just—how many people do that, because it affects your experience, and how much understanding there is around that I think is a separate question. But no, I'm not sure anyone would pay for social media, the same way that very few people pay for news these days.

Amb. KORNBLUH. I also—a lot of people talk about how the problem is that ad-supported—the ad-revenue-supported model, and I think there's a lot to that. One response that you get is, well, if you want to constrain that in any way, you're going to hurt small businesses, and there's a lot of talk about the commercial implications. And I think one of the reasons—I just want to take a step back for a second. One of the reasons that the Cambridge Analytica scandal I think hit so hard was because it's one thing for these big murky data brokers to have information on my shoe size and my taste in shoes. I might prefer that they advertise better options to me on shoes, instead of the same pair of slippers that I bought 2 years ago that follow me around the internet. But when it comes to my political beliefs and my philosophical beliefs and they're inferring that and using that to micro-target propaganda at me, I think people felt very, very differently. And I think we haven't teased that out enough. And it's driven by the ad system, but there's no reason that the platforms need to treat those two in the same way, the commercial advertising and the political advertising.

And Helen [sic; Elizabeth] Denham, the information commissioner in the U.K., has suggested even a pause in micro-targeting in the political space until we figure this all out. I don't know if that would pass First Amendment scrutiny here, but it's really interesting.

And one of the things—Nina mentioned GDPR. One of the things that European law does is, it treats your political and philosophical views as sensitive information. So, theoretically, they're supposed to come to you and say, an opt-in basis, is it okay if I infer your philosophical views by the magazines that you subscribe to in order to micro-target propaganda to you? I've yet to see that question be asked of anybody, but theoretically——

Ms. JANKOWICZ. It should be asked exactly that way. [Laughter.]

Amb. KORNBLUH. Exactly. Theoretically that should be a brake on some of this.

But I do think it's useful—in the U.S. it's really difficult because we don't—we affirmatively don't want to burden political speech. But there has to be some way we can think about the whole ad-revenue ecosystem in the political sphere, differently from are small businesses going to be able to target their users online?

Mr. CHESSEN. So just a couple points on that, also. I mean, I think money generally is something we really need to take a close look at. You know, part of—there have been studies that showed that basically what drives engagement on some of these platforms is anger, right? And so in a lot of ways, that's what some of these algorithms are actually optimizing for, because it keeps you on the platform longer, then you're looking at more ads. There's also this phenomenon where there's certain actors who are pushing out

disinformation, not because they necessarily care about the content or the substance of the disinformation, but because they're trying to basically earn ad dollars. And they're either trying to get the revenue from the clicks, or they're actually trying to drive you off of the platform to their own site, where they then essentially put adware slash spyware on your computer that then can track your behavior throughout the internet and then they can sell you information. So there's some malicious ad networks that these directly plug in to, and there's some disinformation actors, where there is this nexus—there is—I know one in particular where there's a nexus between the ideology but it's also a for-profit, money-making enterprise. Right? So I think we have to tease that out.

We also have to look at individual choices here, because all of our individual choices are really dragging this system. We've all got addicted to free stuff on the internet. We all have gotten addicted to free news. And so the market and the systems have responded, and so basically when you have clickbait-driven ads and clickbait-driven revenue for news sites, you know, that's sort of eviscerated local media, it's eviscerated a lot of the editorial departments, and it's incentivized this sort of yellow journalism and clickbait-driven news. So we have to think about how we as individuals are actually incentivizing this.

And I think the last thing to think about is, is I'm sort of intrigued by this idea that people are throwing around of the public utility for social, right? So if you think about why some of these public utilities came around for water or electricity, it's because those entities that were providing those services, their interests weren't necessarily directly in line with the users, and there were some negative incentives there. So maybe that's something we need to consider is, do we need some sort of new institution for democracy that basically serves this type of civic function? And it wouldn't necessarily be social media; it could be something that basically serves other functions, like connecting people better to government or enabling, you know, Members of Congress to better connect to their constituents.

Mr. MASSARO. So I thought my second question was not related and then you both brought up the EU, so the second question is: The EU approach—you know, they've taken a very proactive stance on a lot of these issues. What are the sort of positives and pitfalls of what's going on there, in your view?

Ms. JANKOWICZ. Well, I think it's too early to say, really, what GDPR has done for privacy- and disinformation-related issues in the EU. But one thing that I have been looking at and I'm going to mess up the name—I forget exactly what it's called, but the EU in September signed with the social media companies essentially a code of conduct related to disinformation. And actually—was that just yesterday?—two days ago in the U.K. the nine parliamentarians or members of Parliament who convened for the DCMS [Department for Digital, Culture, Media and Sport] select committee also signed a related document. And I think that's something that prior to legislation coming forward should happen here, just setting the rules of the road, defining what we mean by disinformation, by hate speech, by all these things, and kind of identifying a common set of core values going forward that can govern the decisions that the United States makes legislatively. I think that's something to aspire to. We'll see if the social media companies—one of the clauses in this agreement they made with the EU is that they need to report on their activities related to take-downs, so we'll see next September if they actually do that and to what level of transparency they do.

Amb. KORNBLUH. As I'm sure you're aware, California passed its own privacy law that's modeled to some degree on GDPR and now there's talk about a Federal privacy law

in the U.S. And I think there's going to be a lot of conversation then. As Nina said, it's too soon, really, to say about GDPR, in part because the enforcement actions haven't been taken yet, and so there's been a lot of complaints about the way some of the companies have been implementing GDPR, that they appear to give you choice, but the way the user interface is designed, it looks like you don't have a choice and so you click "agree" because you think that's the only way to get the service, when in fact that's not what the law says.

So we'll see how the enforcement goes, and that should become clear so that we'll have some data points into how all of this is working and what makes sense and what doesn't before the Federal law is passed. And I think it will be really interesting to see how that debate goes and what happens between now and then. The California law isn't scheduled to come into effect for some time, so it gives us that window.

Mr. CHESSEN. So I think, generally, looking at the EU approach, I think one of the things that's been really positive is the fact that they have taken a very broad multi-stakeholder, consultative approach toward these issues, so they had a high-level experts group that met for several months that produced a report. The EC then took that and actually put out some policy guidance. One of those pieces of guidance was for this code of practice, which they negotiated with the social media companies. There are some concerns that this could be—lead to regulation or legislation that could de facto regulate U.S. companies, so I think a lot of people are watching to see where this goes.

But I think the lesson from the EU approach that we might take is I think we need to engage in a national conversation about these issues. And so since we're here at Congress, you know, one of the things that I've talked about is maybe Congress needs to convene a commission on data privacy, information security and disinformation, because I think we need to have a national conversation in this country about our data privacy practices. I think we need to have a conversation about a lot of these issues, about whitelisting, blacklisting, content controls, what's acceptable, do we want to change the business models for these companies? Do we need to regulate them to promote more innovation? This is not a conversation we're having in any sort of—you know, with a methodology or any sort of systematic way. And I think it's a conversation we need to have before we sort of rush in and regulate or create policy around this. And that's really what I see missing from the U.S. discussion.

Mr. TONER. Thank you so much. At this point, I think we'd like to open up to any audience questions. So if you've got questions, I know we have a mic available. Did I see a hand come up?

QUESTIONER. Yes. I can try without a mic.

Mr. TONER. You can try without a mic. [Laughs.] I can hear you.

QUESTIONER. Matt, just to your—[inaudible]. To your point about a commission, why haven't we seen tech executives sort of brought up to the Hill the way the cigarette company executives were in 1994 and really account in a much more comprehensive way for their sort of complicity in a lot of this? We've had that, obviously, piecemeal, but I think—I mean, I wonder why. Why has Congress not done that, do you think?

Mr. CHESSEN. Well, I'm not going to speak for Congress. I mean, one thing that I can guess is because I think in the difference with the cigarette case is there was a sort of intentional, perhaps malicious activity involved and some intentional disinformation there. I think what you're seeing with the tech companies—it's not that they're malicious.

I mean, there's a lot of fantastic people working in the tech industry—they're trying to build great products, they're trying to build products people use. There's actually a lot of great people who are very strong proponents of U.S. national security who work for Facebook and other companies. I think it's more that they didn't necessarily see these problems coming, like a lot of us didn't see these problems coming. And so I do think there needs to be a lot more accountability for, hey, now that you know that the problem's there, what are you doing about? Right? But I don't think it rises to the same level of, you know, sort of maliciousness or—it wasn't necessarily as problematic. That's just my personal take; you know, my colleagues probably have opinions as well.

Amb. KORNBLUH. Yes. I mean, just having been involved since the early regulatory discussions, there is this idea that this technology itself was pro-democratic and that there was no need for regulation because it was going to further the goals of democracy. It was instead of broadcast, which was, you know, concentrated, that it was—you know, everyone was a publisher, everyone was a speaker. It was going to give voice to the voiceless, power to the powerless. And as things have changed, as it's become more centralized, as our lives, our whole lives have moved on to the internet, I think we still have that image of the guy in his garage, and I think maybe we need to mature a little bit more and say, gee, if our campaigns are all taking place online, maybe we have to update our campaign finance laws. And if we're purchasing online, maybe we have to update our consumer protection laws. I think as a society we haven't taken the responsibility seriously enough.

Ms. JANKOWICZ. Just briefly, I'll also add, I agree with everything that's been said and I think one of the reasons that we have been slow to kind of coagulate around this issue is because of how we came to it, through a very political lens, and I think it's really important to take a step back and de-politicize this because it's a question of democratic discourse. It's not partisan.

Mr. TONER. Another—there you go, over there.

QUESTIONER. Is this good? Okay, sorry. [Laughs.] Growing up as a Millennial/Generation Z, however you want to go and classify that, I was able to see firsthand the way that social media is able to impact a generation. And one of the scary things that I have seen is that people are moving away from reading books and reading more legitimate news sources like The Wall Street Journal, so forth, and going more toward free, more interesting content, I guess, on social media. So I want to know—and to me, the way that I see it is almost trading knowledge for information. So I want to know, are the platforms partially themselves responsible for creating this problem by giving us too much information than what we're able to process and creating more extremist content by that?

Mr. TONER. Sorry, could you give us your name and affiliation?

QUESTIONER. Sure.

Mr. TONER. I know this guy over here so I can—[laughter]—I can get it afterward. But——

QUESTIONER. I'm Jake Hannigan, working for Congressman Tom O'Halleran of Arizona's First District.

Amb. KORNBLUH. I mean, there's been a lot of work by folks who are looking at—to applying different sociology, anthropologies, psychology to what's happening on the internet, and the platforms themselves are starting to take this really seriously, so you'll notice that you're now getting reports about how much time you've spent online. You know, that's still a very blunt instrument; it's not telling you what you spent your time

doing. But I think there's starting to be more awareness of this, just how many hours people are spending. What's the impact on kids? You know, what's our impact on delayed gratification if everything's a click?

My kids, I had them watch one of these former Google guys who's done this whole presentation about what notifications does to you and how it trains your brain. And my kids are very loath to take any of my advice but they watched this and they turned off all their notifications. I think there's starting to be an awareness, but not nearly enough. I think it's a really interesting question.

Mr. CHESSEN. I would answer that by just saying yes. I mean, I think that the technology is an enabler of all of us getting information overload and having short attention spans. I mean, if you just look at a news feed, right—so whether you—take your news app. Right? So it used to be that you would read a newspaper and the newspaper had a set amount of content, and when you were done with the newspaper, you put it aside and you were done. News feeds basically are endless, right? You keep reading, you keep reading. So that encourages behavior where you would scroll and scan and have much less detailed, in-depth engagement with things. And that sort of trains us in how we consume things.

I think some other interesting factors are just, you know, the fact that it was explained to me once when someone was talking about why their kids were using Snapchat and just exchanging images with each other. And it was explained to them, well, that's how they're talking; they're actually communicating using that. And so, if you don't understand meme culture and you don't understand how much information can be spread during memes, which is just an image sometimes with text with it, you know, that drove a lot of sort of the expression during the 2016 campaign. You're seeing it drives a lot of expression online. And this is around this idea, you know—you mentioned the images about sharia law in Paris. Right? I think that was less about people actually believing that those things were credible and more about the posture. Right? And so this is what you're seeing a lot more of now, and I think this is driven by technology, is it's not so much the content, the substance; it's actually the posture that that content or that meme or that image pushes out that reinforces someone's belief and identity.

So you're seeing these very profound changes, you know, that are being driven somewhat by technology or enabled by technology. And I don't necessarily think we know exactly where this is going to go. When you start having AI systems producing a lot more content, images, TV shows, things like that, it's going to change this dynamic further. And so yes, pay attention in this space because I think there's going to be a lot of dynamic knowledge generated, but I think it's also something we need to pay attention to vulnerabilities in this space as well.

Amb. KORNBLUH. Can I just add one other thing? Because I don't want us to be all grim. There have been a couple of studies that have actually shown that there's an upside, too, for kids and for teens about social media. Vicky Rideout has done some amazing work, and there was just another study out really recently about how when kids are lonely they can find mental health services online.

So, you know, again, I think sometimes it's not the technology, it's how it's used, how aware we are of how we're being manipulated and so on, and that it can be a really valuable—I know for me, I read the news all the time now, but I'm finding all kinds of specialized sources that I wouldn't have found otherwise. You know, the whole Me Too movement—people have talked about it, but just from a personal point of view, watching young

women speak up has changed my perceptions of things. So I think there's a huge amount of good in this, but I think your generation is going to be so much more aware of its impact and it's going to be able, I hope, to mold it so we get more of the good and less of the bad.

QUESTIONER. Hi. Maria Yates [ph] from the Voice of America Russian Service.

I just wanted to touch on Russian disinformation tactics. Do you see Russia being, indeed, less active because of the public scrutiny? Or do you see them developing new strategies or tactics for disinformation, developing—[inaudible]—in the future?

Thank you.

Ms. JANKOWICZ. As far as I'm concerned, a lot of the Russian disinformation that likely happened during the 2018 midterms has just not been located yet. If you think back to November, December 2016, we didn't know the extent of what was going on then. And I think it's been shown through the criminal complaints and indictments that Mueller's team has released that these efforts are ongoing and that they are—because the rules and regulations on the platforms have changed, Russians and also other malign actors, including Iran and China, have been able to get around those regulations and be a bit more clever about how they are putting out their information operations.

Mr. CHESSEN. I think the only thing I would add to that is, you know, Russia is not giving up the information game. I think they, maybe, are just going to be doing it in a way that is a little bit more savvy and isn't going to—isn't going to generate the obvious public blowback, but they're still committed to information operations. What I think also we need to pay attention to is that there a lot of other actors who have learned from how Russia behaved and a lot of their tactics, and those actors are now adopting those tactics. There's a lot of people who are more worried about domestic actors now pushing out disinformation than they are about some of the international actors. So that's particularly concerning.

Mr. TONER. We do have time for just a couple more questions, if there are out there.

QUESTIONER. Thank you. [Inaudible.]

I had a followup to my—[inaudible]—question. If we think of Facebook as a social network from, like—[inaudible]—and now it is this big company moving to the news gig, do you think maybe Facebook moved too fast or maybe wasn't supposed to go on that market? And what's your stand on other social networks? Should they go to the news gig, too, or no?

Mr. TONER. Sorry, just to clarify, you said the news becoming kind of a media——

QUESTIONER. Yes, I wanted to——

Mr. TONER. ——or like a news outlet?

QUESTIONER. Yes. Yes, do you think that maybe it was really a mistake of Facebook to go that fast to the news market?

Mr. TONER. Market, right.

QUESTIONER. Yes.

Amb. KORNBLUH. I'm troubled by what's happened—[laughs]—to the press online and I'm not sure that—you know, I'm not sure that I would blame Facebook as much as I would blame society for not thinking more about this. But, you know, a lot of these outlets felt the only way they could—they needed to go where the eyeballs were; the eyeballs were online. They started to go online but they lost—as I was saying before, they lost a lot of

the information that lends to their credibility. And so you've had this flattening where—and this due to a lot of causes but where the mainstream news has gotten less credible, and some of these conspiracy sites have gained by looking like normal press outlets. They've gained credibility. And that's just really unfortunate.

And obviously there have been a lot of causes that have been leading to that, but if you think about in the physical world where you had a newsstand and maybe the tabloids were separated, maybe they were in a different place behind the checkout counter or they were in the back of the kiosk, and now it's all muddled together. I mean, you don't even know if it's an opinion piece from The Wall Street Journal or a news piece when you see it online. So all of that, that framework that we had in our brains that allowed us to trust a piece of news, we're now realizing we have less trust, but we also are still—the remaining trust we have we're attaching to these other outlets that are just conspiracy sites, so it's really troubling.

And as Nina laid out, there's this effort to try to dial some of that back by Facebook where they're emphasizing your friends and family in your feed instead of news, but I think we have—we've created quite a mess and it's going to be really hard to get out of it.

Ms. JANKOWICZ. One small anecdote that I'll relay from a recent conversation I was involved in with Facebook and a number of European governments: One of the advisers to a prime minister of an Eastern European government stood up and asked the representative from Facebook what—this is analogous to the news platforms but also, you know, information coming from governments—he said, Since you changed your algorithm, the content that we need to deliver to our constituents is no longer getting the engagement that we would hope that it gets. Are we expected to buy ads to reach our constituents? And the Facebook representative actually suggested that this adviser to a prime minister create a Facebook group in order to reach their constituents, because that was prioritized in the algorithm. And I think it's really crazy that legitimate information from governments, from news sources is being demoted in order to just kind of feed this engagement mechanism on Facebook. And I don't think they've really thought that through, that, you know, people might be fed more and more content from Ariana Grande rather than their elected officials. So it's something I agree with you that they probably moved too fast in that scenario.

Amb. KORNBLUH. But I do like what Matt was saying and I've been thinking about that as well: What's our civic infrastructure? You know, it's one thing for us to complain, it's another thing for us to think about, what do we want to actually see? What are the positive infrastructures that we want to see? And people are just starting to put that together and think about that. And then how do we get that—how do we make sure that that actually gets eyeballs, that's attractive enough for people to actually go on to it—so what's the PBS or the C-SPAN or whatever your analogy is?

Mr. TONER. It's in some ways a problem of curation, which is what you talked about—you know, that you know what you're getting with The New York Times, you know that it's been looked at by an editorial staff and positioned correctly, where the bad stuff has been thrown out and culled. And you don't have that——

Amb. KORNBLUH. It's not so much that you know, gee, I know that editor and I trust him, but you know what their standards and procedures are.

Mr. TONER. Exactly. And their reputation's on the line. Yes.

Amb. KORNBLUH. Right. So, you know, I'm sitting over here looking at Yahoo! News and there's ProPublica. There are a bunch of very credible outlets that have come online since we've been reading all our press online. You don't have to be a physical newspaper, but you need to know what procedures they use.

Mr. TONER. Agreed.

Amb. KORNBLUH. Yes. Yes, yes, yes. So I think that kind of credibility—how do we establish that kind of credibility so that we can have a public discourse online? And that's going to—you know, we have to think about things like—you know, government has thought of itself as a provider of certain facts. You know, in the Constitution you find reference of the census. The government has put out scientific studies and facts. You know, how are we going to help people to find that and to have this fact base I think is a real interesting challenge.

Mr. TONER. Okay. Go ahead, Kyle.

QUESTIONER. Thank you all. I'm Kyle Parker, Helsinki Commission.

On one level, there's an optimism I hear up here. But it's not where I think the optimism should be. I sense and take this view that politicians meddling in political things, don't trust them, don't trust the government, you know, don't trust Facebook either, but probably trust Facebook more than the government, and don't want the government to wreck things.

A lot of these proposals for solutions sound to me like so much manipulation to correct other manipulation. I don't trust it, and I feel like the mess you're talking about has a real bright side and I hope it gets even messier. I wonder if we're not simply reacting to what a democratic or a more democratic free-for-all public square actually looks like. And it's uncomfortable to us, particularly for those of a generation that watched Cronkite at 7 o'clock and got their news delivered that way.

Why are we so naive? Technology is not a good. Why this misplaced faith in linear progress? To me it's about time that the scales fall from our eyes. As that happens, it seems to me the real problem is civic hygiene. Voting is serious business. And I don't trust The New York Times' news or any of them. There's opinion involved in creating the news.

So I'm concerned that these measures that aim to try to steer or control or, as you mentioned, make news appealing. Yet again, more Madison Avenue tactics to package information and get this to the electorate in a way that they'll actually click on it or watch it—is perhaps—creating of more problem, because the internet being what it is—like you say, you ban something, you drive traffic to it, there's mirror sites. You can't get rid of it.

Maybe the best solution is for people to think about civic hygiene, improve critical thinking skills. Don't trust anything you read anywhere. Be skeptical. Get off the internet and stop flattening your civic engagement to this one-dimensional online medium and get out and talk to your friends and neighbors. Be active in your local community —this focus on hacking elections to me is an unhelpful reduction of civic engagement to showing up for, what, a half an hour every few years to vote? You call that civic engagement? There's a lot more to civic engagement. To me our outrage just reeks of establishment fury.

Here we are in Washington, working for politicians. If you're a politician, elections loom large in your mind. Well, they don't loom nearly as large in the minds of the American people. There's a whole lot more to this country and to real civic engagement. Yet I see these bills come across my desk. I saw one last Congress; I think it was a hundred

million dollars to the Department of Homeland Security to educate Americans about consuming news. This is frightening, Orwellian, even. I don't want the government and politicians in this space. I want more of the public square in this place, more of a free-for-all. We're the ones who are ultimately the problem. We're the market for this clickbait and we're the ones who click on it. So what do we expect from Facebook and others? They do exactly what they're designed to do and they do it well.

Amb. KORNBLUH. So the one thing that I'll throw back at you is where I come down again and again and again is the role for government is transparency, that you can't—you can get all the education and literacy that you want, but if you don't know if you're dealing with a bot, if you don't know how many actual people endorsed this and it looks like it's a lot more than it really is, if you think that Blacktivist is an actual, you know, group of likeminded people but it's actually the Russians, if you don't know that this travel ad is being sponsored by somebody who has a conflict of interest, then you can't look out for yourself.

So I don't think of that as a real public square if you don't have the information, if you don't know what's going on. And people—unfortunately, the internet, which we thought of as this great transparent voice of the voiceless, there's far too much opportunity for fraud, really. So I come down on, isn't there a role for the government in transparency? And the Supreme Court, even Scalia, has said that in political speech there's a role for transparency. So I think that's a role for government. The government isn't saying what's true, what's not true, what's good, what's bad, what should be whitelisted or not; you know, they're just saying let's have—let's give you more information about what you're seeing online. I think that can help a lot.

Mr. CHESSEN. So, actually, a lot of what you said resonates with me. I think the way I would conceptualize what you're talking about is—taking it back to the Enlightenment again—is that you've got a lot of institutions that are being run by elites. That's how we've run things for 200 years. And now you have hyper-empowered individuals who are using technology to push out a lot of ideas that are challenging those elites and institutions. I think all of that is very healthy and I think—I am a firm believer in free expression in the marketplace of ideas, and people have a right in this country to put out disinformation, if they want to.

Where I think it goes off the rails, and what we have to worry about, is when it turns into coordinated, manipulative activity using technology. Right? And so I think that's where we start to draw the line. It basically goes to what Karen and Nina have said. You know, it's basically when you have groups of people that are using techniques from human cognition and human psychology and the technology tools and then hacking the features of those technology tools to basically manipulate people without their knowing they're being manipulated, that's where it becomes a problem.

So I—but I totally agree that I think we are really missing out—and Karen talked about this, a lot of the positive aspects of technology and what it's doing for society. I think we can't lose sight of that focus and that vibrancy and the fact that this diversity of ideas is a good thing and we don't need to say that this is the death of the Enlightenment, we need to create Enlightenment 2.0.

I would also caution that I think there's a difference between promoting critical thinking and promoting people having sort of a questioning eye, versus just saying don't believe anything you see. Right? That's actually pushing us into this post-truth world. That's what adversaries like Russia want, right? They want us in this post-truth world,

because in that world a fact is just whatever you can convince people of, and then countries that may not be able to compete with the United States diplomatically, economically, militarily, but can compete on an information basis, they have outsized power. Right?

And so that's the real danger. And like I said, that post-truth world, where you don't believe anything, in that world people tend to retreat into their tribal identities; they tend to retreat into their little window of what they believe about the world and they interpret everything through that because they just don't know what to believe.

This is really fundamentally a trust issue. Right? And this gets back to the transparency. People need to know what they can trust. They need to know where the information's coming from, who's doing it, and they need to be able trust that the information they're getting is being provided to them in a way where they're not manipulated.

QUESTIONER. Just to clarify: The point is not "don't believe anything you see" but it's "don't believe anything you see without constant critical reassessment." So it's not a one-time thing where [you] trusted this paper 20 years but everything that's coming in is vetted through a notion of is—you know, a critical——

Mr. CHESSEN. Keep your brain on.

QUESTIONER. Right. [Laughter.]

Mr. TONER. I think we're going to have to conclude on that very good exchange. But I can't thank our three panelists enough for really a very illuminating discussion. I've learned a lot today. I hope all of you have. I think this is a really useful exchange. And I hope, as I said, it's just the beginning.

But thank you so much for coming today. I appreciate it. Thank you on behalf of the Helsinki Commission. [Applause.]

[Whereupon, at 12:04 p.m., the briefing ended.]

○

This is an official publication of the **Commission on Security and Cooperation in Europe.**

★ ★ ★

This publication is intended to document developments and trends in participating States of the Organization for Security and Cooperation in Europe [OSCE].

★ ★ ★

★ ★ ★

www.csce.gov **@HelsinkiComm**

The Commission's Web site provides access to the latest press releases and reports, as well as hearings and briefings. Using the Commission's electronic subscription service, readers are able to receive press releases, articles, and other materials by topic or countries of particular interest.

Please subscribe today.