RPTR BRYANT

EDTR ROSEN

AMERICANS AT RISK: MANIPULATION

AND DECEPTION IN THE DIGITAL AGE

WEDNESDAY, JANUARY 8, 2020

House of Representatives,

Subcommittee on Consumer Protection and Commerce,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:32 a.m., in Room 2123, Rayburn House Office Building, Hon. Jan Schakowsky [chairwoman of the subcommittee] presiding.

Present: Representatives Schakowsky, Castor, Veasey, Kelly, O'Halleran, Lujan, Cardenas, Blunt Rochester, Soto, Matsui, McNerney, Dingell, Pallone (ex officio), Rodgers, Burgess, Latta, Guthrie, Bucshon, Hudson, Carter, and Walden (ex officio).

Staff Present: Jeff Carroll, Staff Director; Evan Gilbert, Deputy Press Secretary; Lisa Goldman, Senior Counsel; Waverly Gordon, Deputy Chief Counsel; Tiffany Guarascio,

Deputy Staff Director; Alex Hoehn-Saric, Chief Counsel, Communications and Consumer Protection; Zach Kahan, Outreach and Member Service Coordinator; Joe Orlando, Staff Assistant; Alivia Roberts, Press Assistant; Chloe Rodriguez, Policy Analyst; Sydney Terry, Policy Coordinator; Anna Yu Professional Staff Member; Mike Bloomquist, Minority Staff Director; S.K. Bowen, Minority Press Assistant; William Clutterbuck, Minority Staff Assistant; Jordan Davis, Minority Senior Advisor; Tyler Greenberg, Minority Staff Assistant; Peter Kielty, Minority General Counsel; Ryan Long, Minority Deputy Staff Director; Mary Martin, Minority Chief Counsel, Energy & Environment & Climate Change; Brandon Mooney, Minority Deputy Chief Counsel, Energy; Brannon Rains, Minority Legislative Clerk; Zack Roday, Minority Communications Director; and Peter Spencer, Minority Senior Professional Staff Member, Environment & Climate Change.

Ms. Schakowsky. Good morning, everyone. The Subcommittee on Consumer Protection and Commerce will now come to order. We will begin with member statements, and I will begin by recognizing myself for 5 minutes.

Good morning, and thank you for joining us here today. Given what is going on in the world, it is really impressive to see the turnout that is here today, and I welcome everyone.

In the two-plus decades since the creation of the internet, we have seen life for Americans and their families transformed in many positive ways. The internet provides new opportunities for commerce, education, information and connecting people.

However, along with these many new opportunities, we have seen new challenges as well. Bad actors are stocking the online marketplace, using deceptive techniques to influence consumers, deceptive designs to fool them into giving away personal information, stealing their money, and engineering in other unfair practices.

The Federal Trade Commission works to protect Americans from many unfair and deceptive practices, but a lack of resources, authority, and even a lack of will has left many American consumers feeling helpless in this digital world. Adding to that feeling of helplessness, new technologies are increasing the scope and scale of the problem. Deepfakes, manipulation of video, dark patterns, bots and other technological technologies are hurting us in direct and indirect ways.

Congress has, unfortunately, taken a laissez faire approach to regulation of unfair and deceptive practices online over the past decade, and platforms have let them flourish. The result is big tech failed to respond to the grave threats posed by deepfakes, as evidenced by Facebook, scrambling to announce a new policy that strikes me as wholly inadequate -- we will talk about that later -- since it would have done

nothing to prevent the video of Speaker Pelosi that amassed millions of views, and prompted no action by the online platform. Hopefully, our discussion today can change my mind about that.

Underlying all of this is section 230 of the Communications Decency Act, which provides online platform links like Facebook, a legal liability shield for third-party content. Many have argued that this liability shield results in online platforms not adequately policing their platforms, including online piracy and extremist content.

Thus, here we are, with big tech wholly unprepared to tackle the challenges we face today. A top-line concern for this subcommittee must be to protect consumers, regardless of whether they are online or not. For too long, big tech has argued that e-commerce and digital platforms deserve special treatment, and a light regulatory touch.

We are finding out that consumers can be harmed as easily online as in the physical world, and, in some cases, that online dangers are greater. It is incumbent on us in this subcommittee, in this subcommittee, to make clear that the protections that apply to in-person commerce also apply to virtual space.

I thank the witnesses for their testimony today, and I recognize Ranking Member Rodgers for 5 minutes.

Mrs. Rodgers. Thank you. Thank you, Chair Schakowsky. Happy new year, everyone. Welcome to our witnesses. I appreciate the chair leading this effort today to highlight online deception.

I do want to note that last Congress, Chairman Walden also held several hearings on platform responsibility. Disinformation is not a new problem. It was also an issue 130 years ago when Joseph Pulitzer and the New York World and William Randolph Hearst and The New York Journal led the age of, quote, "yellow journalism." Just like clickbait on online platforms today, fake and sensational headlines sold newspapers and

boosted advertising revenue. With far more limited sources of information available in the 1890s, the American people lost trust in the media. To rebuild trust, newspapers had to clean up their act. Now the Pulitzer is associated with something very different.

I believe we are at a similar inflection point today. We are losing faith in sources we can trust online. To rebuild it, this subcommittee, our witness panel and members of the media are putting the spotlight on abuses and deception.

Our committee's past leadership and constructive debates have already led to efforts by platforms to take action. Just this week, Facebook announced a new policy to combat deepfakes, in part, by utilizing artificial intelligence. I appreciate Ms. Bickert for being here to discuss this in greater detail. Deepfakes and disinformation can be handled with innovation and empowering people with more information.

On the platforms they choose and trust, it makes far more productive outcomes when people can make the best decisions for themselves, rather than relying on the government to make decisions for them. That is why we should be focusing on innovation for major breakthroughs, not more regulations or government mandates.

As we discuss ways to combat manipulation online, we must ensure that America will remain the global leader in AI development. There is no better place in the world to raise people's standard of living and make sure that this technology is used responsibly.

Software is already available to face swap, lip sync, and create facial reenactment to fabricate content. As frightening as it is, we can also be using AI to go after the bad actors and fight fire with fire. We cannot afford to shy away from it, because who would you rather lead the world in machine learning technology, America or China? China is sharing its AI surveillance technology with other authoritarian governments, like Venezuela. It is also using its technology to control and suppress ethnic minorities, including the Uyghurs in Chinese concentration camps.

The New York Times has reported just last month that China is collecting DNA samples and could be using this data to create images of faces. Could China be building a tool to further track and crack down on minorities and political dissidents? Imagine the propaganda and lies it could develop with this technology behind the great Chinese firewall, where there is no free speech or an independent press to hold the Communist Party accountable.

That is why America must lead the world in AI development. By upholding our American values, we can use this as a force for good and save people's lives. For example, AI technology and deep learning algorithms can help us detect cancers earlier and more quickly. Clinical trials are already underway and making major breakthroughs to diagnose cancers.

The continued leadership of our innovators is crucial to make sure that we have the tools to combat online deception. To win the future in a global economy, America should be writing the rules for this technology so that real people, not an authoritarian state like China, are empowered.

I am also glad that we are putting a spotlight on dark patterns. Deceptive laws, fake reviews, and bots are the latest version of robocall scams. I am pleased that the FTC has used its section 5 authority to target this fraud and protect people. We should get their input as to how we discuss how to handle dark patterns.

We also must be careful where we legislate so that we don't harm the practices that people enjoy. A heavy-handed regulation will make it impossible for online retailers to provide discounts. This would especially hurt lower and middle income families. In a digital marketplace, services people enjoy should not get swallowed up by strict definition of a dark pattern. How we make these distinctions is important, so I look forward to today's discussion.

I want to thank the panel, and I yield back.

Ms. Schakowsky. The gentlelady yields back.

And the chair now recognizes Mr. Pallone, chair of the full committee, for 5 minutes for his opening statement.

The Chairman. Thank you, Madam Chair.

Americans increasingly rely on the internet for fundamental aspects of their daily lives. Consumers shop online for products ranging from groceries to refrigerators. They use the internet to telecommute or to check the weather and traffic before leaving for the office, and they use social media networks to connect with family and friends, and as a major source of news and information.

When consumers go online, they understandably assume that the reviews of the products that they buy are real, that the people on the social networks are human, and that the news and information they are reading is accurate. But, unfortunately, that is not always the case. Online actors, including nation-states, companies, and individual fraudsters, are using online tools to manipulate and deceive Americans. While some methods of deception are well-known, many are new and sophisticated, fooling even the most savvy consumers.

Today, technology has made it difficult, if not impossible, for typical consumers to recognize what is real from what is fake. And why exactly are people putting so much effort into the development and misuse of technology? Because they know that trust is the key to influencing and taking advantage of people, whether for social, monetary, or political gain. If bad actors can make people believe a lie, then they can manipulate us into taking actions we wouldn't otherwise take.

In some instances, we can no longer even trust our eyes. Videos can be slowed to make someone appear intoxicated. Faces can be photoshopped onto someone else's

body. Audio can be edited in a way that a person's words are basically taken out of context. And the extent of such manipulation has become extreme. Machine learning algorithms can now create completely fake videos, known as deepfakes, that look real. Deepfakes can show real people saying or doing things that they never said or did.

For example, face-swapping technology has been used to place actor Nicolas Cage into movies where he never was. Actor/director Jordan Peele created a deepfake supposedly showing President Obama insulting President Trump.

The most common use of deepfakes is nonconsensual pornography, which has been used to make it appear as if celebrities have been videotaped in compromising positions. And deepfake technology was also used to humiliate a journalist from India who was reporting on an 8-year-old rape victim.

Advances in algorithms are also behind the glut of social media bots, automated systems that interact on social media as if they were real people. These bots are used by companies and other entities to build popularity of brands and respond to consumer service requests. Even more alarming is the use of these bots by both state and non-state actors to spread disinformation, which can influence the very fabric of our society and our politics.

And manipulation can be very subtle. Deceptive designs, sometimes called dark patterns, capitalize on knowledge of our senses, operate to trick us into making choices that benefit the business. Have you ever tried to unsubscribe from a mailing list and there is a button to stay subscribed that is bigger and more colorful than the unsubscribe button? And that is deceptive design. Banner ads have been designed with black spots that look like dirt or hair on the screen to trick you into tapping the "add" on your smartphone. And there are so many other examples.

And since these techniques are designed to go unnoticed, most consumers have

no idea they are happening. In fact, they are almost impossible for experts in types of techniques to detect. And while computer scientists are working on technology that can help detect each of these deceptive techniques, we are in a technological arms race. As detection technology improves, so does the deceptive technology. Regulators and platforms trying to combat deception are left playing a whack-a-mole.

Unrelenting advances in these technologies and their abuse raise significant questions for all of us. What is the prevalence of these deceptive techniques? How are these techniques actually affecting our actions and decisions? What steps are companies and regulators taking to mitigate consumer fraud and misinformation?

So I look forward to beginning to answer these questions with our expert witness panel today so we can start to provide more transparency and tools for consumers to fight misinformation and deceptive practices.

And, Madam Chair, I just want to say, I think this is a very important hearing. I was just telling my colleague, Kathy Castor, this morning about a discussion that we had at our chairs meeting this morning, where the topic was brought up. And I said, Oh, you know, we are having a hearing on this today. So this is something a lot of members and, obviously, the public care about. So thank you for having the hearing today.

I yield back.

Ms. Schakowsky. The gentleman yields back.

And now the chair recognizes Mr. Walden, the ranking member of the full committee, for 5 minutes for his opening statement.

Mr. Walden. Good morning, Madam Chair. Thanks for having this hearing and welcome everyone in. I guess this is the second hearing of the new year. There is one that started earlier upstairs, but we welcome you all to hear this important topic and glad to hear from our witnesses today, even those who I am told have health issues this

morning, but thanks for being here.

As with anything, the internet presents bad actors with those seeking to harm others some ample opportunities to manipulate the users and take advantage of consumers, which often tend to be some of the most vulnerable in the population. Arguably, the digital ecosystem is such that harmful acts are easily exacerbated, and as we all know, false information or fake videos spread at breakneck speeds.

That is why when I was chairman of this committee, we tried to tackle this whole issue with platform responsibility head on, and we appreciate the input we got from many. Last Congress, we, as you heard, held hearings and legislated on online platforms not fulfilling their Good Samaritan obligations, especially when it comes to online human trafficking.

Companies' use of algorithms and the impact such algorithms have on influencing consumer behavior, we took a look at that. Improving/expanding the reach of broadband services so rural and urban consumers of all ages can benefit in a connected world from the positive aspects of the internet. Explaining the online advertising ecosystem, preservation and promotion across border data flows, a topic we need to continue to work on. Other related issues we face in the connected world, such as cybersecurity, Internet of Things, artificial intelligence, to name just a few.

We also invited the heads of the tech industry to come and explain their practices right in this hearing room. Two of the committee's highest profile hearings in recent memory focused squarely on platform responsibility. The CEO of Facebook, Mark Zuckerberg, came and spent about 5-1/2 hours right at that table to answer some pretty tough questions on the Cambridge Analytica debacle, as well as provide the committee with more insight into how Facebook collects consumer information and what Facebook does with that information.

We also welcomed the CEO of Twitter, Jack Dorsey, to provide the committee with more insight into how Twitter operates, decisions Twitter makes on its platform and how such decisions impact consumers specifically, so voices don't feel silenced.

I am pleased that Chairman Pallone brought in the CEO of Reddit last year, and hope the trend will continue as we understand this ever-evolving and critically important ecosystem system those that sit on the top of it.

This hearing today helps with that, as this group of experts shine a light on questionable practices I hope can yield further fruitful results. Such efforts often lead to swifter actions than any government action can get done.

Following our series of hearings, there is proof that some companies are cleaning up their platforms, and we appreciate the work you are doing. For example, following our hearing on Cambridge Analytica, Facebook made significant changes to its privacy policies and Facebook reformatted its privacy settings, to make more accessible and user-friendly, ease the ability for its users to delete and control their information, took down malicious entities on its platform, and invested in programs to preserve and promote legitimate local news operations.

And during that hearing, Representative McKinley actually pushed Mr. Zuckerberg pretty hard on some specific ads he had seen illegally selling opioids without prescriptions on Facebook, and as a result, Facebook removed those ads. In fact, we got a call, I think as Mr. Zuckerberg was headed to the airport that afternoon, that those had already been taken down.

Also notable, through the Global Internet Forum to Counter Terrorism, platforms such as Facebook, Twitter, and YouTube have been working together to tackle terrorist content and, importantly, disrupt violent extremists' ability to promote themselves, share propaganda, and exploit digital platforms. And we thank you for that work.

Now, this is not to suggest the online ecosystem is perfect. It is far from it. Can these companies be doing more to clean up their platforms? Of course, and I expect them to, and I think you are all working on that.

So let me be very clear. This hearing should serve as an important reminder to all online platforms that we are watching them closely. We want to ensure we do not harm innovation, but, as we have demonstrated in a bipartisan fashion in the past, when we see issues or identify clear harms to consumers, we do not see online entities taking appropriate action, we are prepared to act.

So, Madam Chair, thanks for having this hearing. This is tough stuff. I have a degree in journalism. I am a big advocate of the First Amendment. And it can be messy business to, on the one hand, call on them to take down things we don't like and still stay on the right side of the First Amendment, because vigorous speech, even when it is inaccurate, is still protected under the First Amendment. And if you go too far, then we yell at you for taking things down that we liked. And if you don't take down things we don't like, then we yell at you for that. So you are kind of in a bit of a box, and yet, we know 230 is an issue we need to revise and take a look at as well.

And then speaking of revise, I had to chuckle that we all get the opportunity to revise and extend our remarks throughout this process and clean up our bad grammar. So maybe some of what we have is kind of fake reporting, but anyway, we will leave that for another discussion on another day.

And, with that, I yield back, Madam Chair.

Ms. Schakowsky. The gentleman yields back.

And the chair would like to remind members that pursuant to committee rules, all members' opening statements shall be made part of the record.

I would now like to introduce our witnesses for today's hearing. Ms. Monika

Bickert, vice president of Global Policy Management at Facebook. I want to acknowledge and thank you, Ms. Bickert. I know that you are not feeling well today and may want to abbreviate some of your testimony, but we thank you very much for coming anyway.

I want to introduce Dr. Joan Donovan, research director of the Technology and Social Change Project at the Shorenstein Center on Media, Politics and Public Policy at Harvard Kennedy School.

Mr. Justin Hurwitz, assistant professor of law and director of NU Governance and Technology Center at the University of Nebraska College of Law, and director of Law and Economics Programs at the International Center for Law and Economics.

And finally, Dr. Tristan Harris, who is executive director for the Center for Humane Technology.

We want to thank our witnesses for joining us today. We look forward to your testimony.

At this time, the chair will recognize each witness for 5 minutes to provide their opening statement. Before we begin, I would just like to explain the lighting system for those who may not know it. In front of you are a series of lights. The lights will initially be green at the start of your opening statement. The light will turn to yellow when you have 1 minute remaining, and if you could please begin to wrap up your testimony at that point; and then the light will turn red when your time has expired.

So, Ms. Bickert, you are recognized for 5 minutes.

STATEMENTS OF MONIKA BICKERT VICE PRESIDENT OF GLOBAL POLICY MANAGEMENT, FACEBOOK; JOAN DONOVAN, PH.D., RESEARCH DIRECTOR OF THE TECHNOLOGY AND SOCIAL CHANGE PROJECT, SHORENSTEIN CENTER ON MEDIA, POLITICS, AND PUBLIC

POLICY, HARVARD KENNEDY SCHOOL; TRISTAN HARRIS, EXECUTIVE DIRECTOR, CENTER FOR HUMANE TECHNOLOGY; AND JUSTIN (GUS) HURWITZ, ASSOCIATE PROFESSOR OF LAW, DIRECTOR OF THE NU GOVERNANCE AND TECHNOLOGY CENTER, UNIVERSITY OF NEBRASKA COLLEGE OF LAW, DIRECTOR OF LAW & ECONOMICS PROGRAMS, INTERNATIONAL CENTER FOR LAW & ECONOMICS

STATEMENT OF MONIKA BICKERT

Ms. Bickert. Thank you, Chairwoman Schakowsky, Ranking Member McMorris Rodgers, and other distinguished members of the subcommittee. Thank you for the opportunity to appear before you today.

My name is Monika Bickert. I am the vice president for Global Policy Management at Facebook, and I am responsible for our content policies. As the chairwoman pointed out, I am a little under the weather today so, with apologies, I am going to keep my remarks short, but will rely on the written testimony I have submitted.

We know that we have an important role to play at Facebook in addressing manipulation and deception on our platform. And we have many aspects to our approach, including our community standards, which specify what we will remove from the site, and our relationship with third-party fact-checkers, through which fact-checking organizations can rate content as false. We put a label over that content saying that this is false information, and we reduce its distribution.

Under the community standards, there are some types of misinformation that we remove, such as attempts to suppress the vote or to interfere with the Census. And we announced yesterday a new prong in our policy where we will also remove videos that are edited or synthesized, using artificial intelligence, or deep learning techniques, in

ways that are not apparent to the average person that would mislead the average person to believe that the subject of the video said something that he or she did not, in fact, say.

To be clear, manipulated media that doesn't fall under this new policy definition is still subject to our other policies and our third-party fact-checking. That means that deepfakes are still an emerging technology. One area where internet experts have seen them is in nudity and pornography. All of that violates our policies against nudity and pornography, and we would remove it. Manipulated videos are also eligible to be fact-checked by these third-party fact-checking organizations that we work with to label and reduce the distribution of misinformation.

We are always improving our policies and our enforcement, and we will continue to do the engagement we have done outside the company with academics and experts to understand the new ways that these technologies are emerging and affecting our community. We would also welcome the opportunity to collaborate with other industry partners and interested stakeholders, including academics, civil society, and lawmakers, to help develop a consistent industry approach to these issues. Our hope is that by working together with all of these stakeholders, we can make faster progress in ways that benefit all of society.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Bickert follows:]

******** INSERT 1-1 ********

Ms. Schakowsky. Thank you.

And now, Dr. Donovan, you are recognized for 5 minutes.

STATEMENT OF JOAN DONOVAN, PH.D.

Dr. Donovan. Thank you, Chairwoman Schakowsky, Ranking Member McMorris Rodgers, Chairman Pallone, and Ranking Member Walden, for having me today. It is truly an honor to be invited.

I lead a team at Harvard Kennedy's Shorenstein Center that researches online manipulation and deception, and I have been a researcher of the internet for the last decade. So I know quite a bit about changes in policies as well as the development of platforms themselves and what they were intended to do.

One of the things that I want to discuss today is online fraud, which is a great deal more widespread than many understand. Beyond malware, spam, and phishing attacks, beyond credit card scams and product knock-offs, there is a growing threat from new forms of identity fraud enabled by technological design. Platform companies are unable to manage this alone, and Americans need governance. Deception is now a multi-million-dollar industry.

My research team tracks dangerous individuals and groups who use social media to pose as political campaigns, social movements, news organizations, charities, brands and even average people. This emerging economy of misinformation is a threat to national security. Silicon Valley corporations are largely profiting from it, while key political and social institutions are struggling to win back the public's trust.

Platforms have done more than just given users a voice online. They have

effectively given them the equivalent of their own broadcast station, emboldening the most malicious among us. To wreak havoc with a media manipulation campaign, all one bad actor needs is motivation. Money also helps. But that is enough to create chaos and divert significant resources from civil society, politicians, newsrooms, healthcare providers, and even law enforcement, who are tasked with repairing the damage. We currently do not know the true cost of misinformation.

Individuals and groups can quickly weaponize social media, causing others financial and physical injury. For example, fraudsters using President Trump's image, name, logo and voice have siphoned millions from his supporters by claiming to be part of his reelection coalition. In an election year, disinformation and donation scams should be of concern to everyone. Along with my coresearchers Brian Friedberg and Brandi Collins-Dexter, I have studied malicious groups, particularly white supremacists and foreign actors, who have used social media to inflame racial divisions. Even as these imposters are quickly identified by the communities they target, it takes time for platforms to remove inciting content. A single manipulation campaign can create an incredible strain on breaking news cycles, effectively turning many journalists into unpaid content moderators and drawing law enforcement towards false leads.

Today, I argue that online communication technologies need regulatory guardrails to prevent them from being used for manipulative purposes. And in my written testimony, I have provided a longer list of ways that you could think about technology differently.

But right now, I would like to call attention to deceptively edited audio and video to drive clicks, likes, and shares. This is the AI technology commonly referred to as deepfakes. And what I would also like to point out, with my coresearcher Britt Paris, that we have argued that cheapfakes are a wider threat. Like the doctored video of

Speaker Pelosi, last week's decontextualized video of Joe Biden seemingly endorsing a white supremacist talking point poses another substantial challenge. Because the Biden video was clipped from nonaugmented footage, platforms refused to take down this cheapfake. Millions have now seen it.

Platforms, like radio towers, provide amplification power and, as such, they have a public interest obligation. And I point out here that platforms are highly centralized mechanisms of distribution while the internet is not. So I am not trying to conflate platforms with the internet, but this is why we place the burden of moderation on platforms and not with ISPs.

The world online is the real world, and this crisis of counterfeits threatens to disrupt the way Americans live our lives. Right now, malicious actors jeopardize how we make informed decisions about who to vote for and what causes we support, while platform companies have designed systems that facilitate this manipulation.

We must expand the public understanding of technology by guarding consumer rights against technological abuse, including a cross-sector effort to curb the distribution of harmful and malicious content. As Danah Boyd and I have written, platform companies must address the power of amplification and distribution separately from content, so that media distribution is transparent and accountable. I urge Congress to do the same. Platforms and politics and regulation and technology must work in tandem or else the future is forgery. Thank you.

[The prepared statement of Dr. Donovan follows:]

******** INSERT 1-2 ********

Ms. Schakowsky. Thank you.

And now, Mr. Hurwitz, you are recognized for 5 minutes.

STATEMENT OF JUSTIN (GUS) HURWITZ

Mr. Hurwitz. Thank you, Ms. Chairwoman, along with members of the committee, for the opportunity to speak to you today. I would also be remiss if I did not thank my colleague Kristian Stout and research assistant, Justin McCully, for help in drafting my written testimony.

I am a law professor, so I apologize. I have written a short law review article for my written testimony, which I have assigned to you to read. I will turn to discussing that --

Ms. Schakowsky. Make sure your mic -- is your mic on? Pull it up. There you go. Okay.

Mr. Hurwitz. I will turn to discussing the short law review article I have written for you as my testimony and assigned to you to read in a moment. Before I turn to that, I want to make a couple of book recommendations. If you really want to understand what is at stake with dark patterns, you should start by reading Brett Frischmann and Evan Selinger's recent book, Re-Engineering Humanity. In my spare time, I am a door-to-door book salesman. I have a copy here. Their book discusses how modern technology, data analytics, combined with highly programmable environments, are creating a world in which people are, to use their term, programmable. This book will scare you.

After you read that book, you should then read Cliff Kuang and Robert Fabricant's

recent book, User Friendly. This was just published in November. It discusses the importance and difficulty of designing technologies that seamlessly operate in line with user expectations as user-friendly technologies. This book will help you understand the incredible power of user-friendly design and fill you with hope for what design makes possible, along with appreciation for how difficult it is to do design well. Together, these books will show you both sides of the coin.

Dark patterns are something that this committee absolutely should be concerned about, but this committee should also approach the topic with great caution. Design is powerful, but it is incredibly difficult to do well. Efforts to regulate bad uses of design could easily harm efforts to do and use design for good.

How is that for having a professor testify? I have already assigned two books and a law review article of my own for you to read. I will do what I can to summarize some of the key ideas from that article in the next 3 minutes or so.

Dark pattern is an ominous term. It is itself a dark pattern. It is a term for a simple concept. People behave in predictable ways. These behavioral patterns can be used to program us in certain ways, and the concern is that sometimes we can be programmed to act against our own self-interest.

So I have some examples. If we can look at the first example, this is something from the internet. You look at this for a moment. Who here feels manipulated by this image? It is okay to say yes. I do. The designer of this image is using his knowledge of how people read text in an image to make it feel like the image is controlling us, making us control how our eyes are following it and predicting where we are going to go next. Weird stuff.

Let's look at another example. Again, you can definitely tell from the internet. Again, who feels like this image is manipulative? The previous image was harmless, but

this one hints at the darker power of dark patterns. Most of you probably missed the typos in the first line and then the second line until the text points them out to you. What if this had been a contract and this trick was used to insert a material term or distract you from a material term in the contract that you were agreeing to? This has now gone from weird stuff to scary stuff.

On the other hand, these same tricks can be used for good. In this same example, what if this trick were used to highlight an easily missed but important concern for consumers to pay attention to? This could be beneficial to consumers.

Design is not mere aesthetics. All design influences how designs are made. It is not possible to regulate bad design without also affecting good design.

So how much of a problem are dark patterns? Recent research shows that websites absolutely are using them, sometimes subtly, sometimes overtly, to influence users. And other research shows us that these tactics can be effective, leading consumers to do things that they otherwise wouldn't do. We have already heard some examples of these, so I won't repeat what has already been discussed. Rather, I would like to leave you with a few ideas about what, if anything, we should do about them.

First, dark patterns are used both online and offline. Stores use their floor plans to influence what people buy. Advertisers make consumers feel a sense of need and urgency for products. Try canceling a subscription service or returning a product. You will likely be routed through a maddening maze of consumer service representatives. If these patterns are a problem online, they are a problem offline, too. We shouldn't focus on one to the exclusion of the other.

Second, while these tricks are annoying, it is unclear how much they actually harm consumers or how much benefit they may confer. Studies of mandatory disclosure laws, for instance, find that they have limited effectiveness. On the other hand, these

tricks can also be used to benefit consumers. We should be cautious with regulations that may fail to stop bad conduct while reducing the benefits of good conduct.

Third, most of the worst examples of dark patterns very likely fall within the FTC's authority to regulate deceptive acts or practices. Before the legislature takes any action to address these concerns, the FTC should attempt to use its existing authority to address them. It is already having hearings on these issues. If this proves ineffective, the FTC should report to you, to Congress, on these practices.

Fourth, industry has been responsive to these issues and, to some extent, has been self-regulating. Web browsers and operating systems have made many bad design practices harder to use. Design professionals scorn dark patterns practices. Industry standardization and best practices and self-regulations should be encouraged.

Fifth, regulators should --

Ms. Schakowsky. Wrap it up.

Mr. Hurwitz. Yes. Last and building on all of the above, this is an area well-suited to cooperation between industry and regulators. Efforts at self-regulation should be encouraged and rewarded. Perhaps even more important, given the complexity of these systems, industry should be at the front line of combating them. Industry has greater design expertise and ability to experiment than regulators, but there is an important role for regulation to step in where industry fails to police itself.

In a true professor -- thank you. I look forward to discussion.

[The statement of Mr. Hurwitz follows:]

******** INSERT 1-3 ********

Ms. Schakowsky. So, Mr. Harris, you are recognized now for 5 minutes.

STATEMENT OF TRISTAN HARRIS

Mr. Harris. Thank you, Chairwoman Schakowsky and members. I really appreciate you inviting me here.

I am going to go off script. I come here because I am incredibly concerned. I actually have a lifelong experience with deception and how technology influences people's minds. I was a magician as a kid, so I have started off by seeing the world this way. And then I studied at a lab called the Stanford Persuasive Technology Lab, actually with the founders of Instagram. And so I know the culture of the people who build these products and the way that it is designed intentionally for mass deception.

I think there is -- the thing I most want to respond to here is we often frame these issues as we have got a few bad apples. We have got these bad deepfakes, we have got to get them off the platform. We have got this bad content. We have got these bad bots. What I want to argue is this is actually -- and we have got these dark patterns.

What I want to argue is we have dark infrastructure. This is now the infrastructure by which 2.7 billion people, bigger than the size of Christianity, make sense of the world. It is the information environment. And if someone went along, private companies, and built nuclear power plants all across the United States, and they started melting down and they said, Well, it is your responsibility to have HazMat suits and, you know, have a radiation kit, that is essentially what we are experiencing now. The responsibility is being put on consumers when, in fact, if it is the infrastructure, it should be put on the people building that infrastructure.

There are specifically two areas of harm I want to focus on, even though when this becomes the infrastructure it controls all of our lives. So we wake up with these devices. We check our phones 150 times a day. It is the infrastructure for going to bed. Children spend as much time on these devices as they do at the hours at school. So no matter what you are putting in people's brains, kids' brains at school, you have got all the hours they spend, you know, on their phones.

And let's take the kids' issue. So as infrastructure, the business model of this infrastructure is not aligned with the fabric of society. How much have you paid for your Facebook account recently, or your YouTube account? Zero. How are they worth more than a trillion dollars in market value? They monetize our attention. The way they get that attention is by influencing you and using the dark patterns or tricks to do it.

So the way they do it with children is they say, how many likes or followers do you have? So they basically get children addicted to getting attention from other people. They use filters, likes, et cetera, beautification filters that enhance your self-image. And after two decades in decline, the mental health of teen girls, high depressive symptoms -- there is an image here that they will be able to show -- went up 170 percent after the year 2010, with the rise of Instagram, et cetera. Okay. These are your children. These are your constituents. This is a real issue. It is because we are hacking the self-image of children.

On the information ecology front, the business model, think of it like we are drinking from the Flint water supply of information. The business model is polarization, because the whole point is I have to figure out and calculate whatever keeps your attention, which means affirmation, not information, by default. It polarizes us by default.

There is a recent upturn study that it actually costs more money to advertise

across the aisle than it does to advertise to people with your own same beliefs. In other words, polarization has a home field advantage in terms of the business model. The natural function of these platforms is to reward conspiracy theories, outrage, what we call the race to the bottom of the brainstem. It is the reason why all of you at home have crazier and crazier constituents who believe crazier and crazier things, and you have to respond to them. I know you don't like that.

Russia is manipulating our veterans by -- we have totally open borders. While we have been protecting our physical borders, we left the digital border wide open. Imagine a nuclear plant and you said, we are not going to actually protect the nuclear plants from Russian cyber attacks. Well, this is sort of like Facebook building the information infrastructure and not protecting it from any bad actors until that pressure is there.

And this is leading to a kind of information trust meltdown, because no one even has to use deepfakes for essentially people to say, well, that must be a faked video, right? So we are actually at the last turning point, kind of an event horizon, where we either protect the foundations of our information and trust environment or we let it go away.

And, you know, we say we care about kids' education, but we allow, you know, technology companies to basically tell them that the world revolves around likes, clicks, and shares. We say we want to, you know, come together, but we allow technology to profit by dividing us into echo chambers. We say America should lead on the global stage against China with its strong economy, but we allow technology companies to degrade our productivity and mental health, while jeopardizing the development of our future workforce, which is our children.

And so while I am finishing up here, I just want to say that instead of trying to design some new Federal agency, some master agency, when technology has basically

taken all the laws of the physical world -- taken all the infrastructure of the physical world and virtualized it into a virtual world with no laws -- what happens when you have no laws for an entire virtualized infrastructure? You can't just bring some new agency around and regulate all of the virtual world.

Why don't we take the existing infrastructure, existing agencies who already have purview, Department of Education, Health and Human Services, Natural Institutes of Health, and have a digital update that expands their jurisdiction to just ask, Well, how do we protect the tech platforms in the same areas of jurisdiction?

I know I am out of time, so thank you very much.

[The statement of Mr. Harris follows:]

******** INSERT 1-4 ********

Ms. Schakowsky. Thank you.

So now we have concluded our witnesses' opening statements. At this time, we will move to member questions. Each member will have 5 minutes to ask a question of our witnesses. I will begin by recognizing myself for 5 minutes.

So, as chair of the subcommittee, over and over again, I am confronted with new evidence that big tech has failed in regulating itself. When we had Mark Zuckerberg here, I kind of did a review of all the apologies that we have had from him over the years, and I am concerned that Facebook's latest effort to address misinformation on the platforms leaves a lot out.

I want to begin with some questions of you, Ms. Bickert. So, the deepfakes policy only covers video, as I understand it, that have been manipulated using artificial intelligence, or deep learning. Is that correct?

Ms. Bickert. Thank you, Chairwoman Schakowsky. The policy that we announced yesterday is confined to the definition that we set forth about artificial intelligence being used in a video to make it appear that somebody is saying something --

Ms. Schakowsky. I only have 5 minutes. So the video, for example, of Speaker Pelosi was edited to make her look like she was drunk wouldn't have been taken down under the new policy. Is that right, yes or no?

Ms. Bickert. It would not fall under that policy, but it would still be subject to our other policies that address misinformation.

Ms. Schakowsky. And as I read the deepfakes policy, it only covers video where a person is made to appear like they said words that they didn't actually say, but it doesn't cover videos where just the image is altered. Is that true?

Ms. Bickert. Chairwoman Schakowsky, that is correct about that policy. We do

have a broader approach to misinformation that would put a label -- we would actually obscure the image and put a screen over it that says "false information," and directs people to information from fact-checkers.

Ms. Schakowsky. So, Ms. Bickert, I really don't understand why Facebook should treat fake audio differently from fake images. Both can be highly misleading and result in significant harm to individuals and undermine democratic institutions.

Dr. Donovan, in your testimony, you noted that, quote, "cheapfakes," unquote, are more prevalent than deepfakes. Do you see any reason to treat deepfakes and cheapfakes differently?

Dr. Donovan. One of the things --

Ms. Schakowsky. Microphone.

Dr. Donovan. Of course, as if I am not loud enough.

One of the things that cheapfakes leverage is what is sort of great about social media is that it makes things clippier, or smaller. And so, I understand the need for separate policies, but also the cheapfakes issue has not been enforced. Speaking more broadly about social media platforms in general, there is completely uneven enforcement.

So you can still find that piece of misinformation within the wrong context in multiple places. And so, the policy on deepfakes is both narrow, and I understand why. But also, one thing that we should understand is presently, there is no consistent detection mechanism for even finding deepfakes at this point. And, so, I would be interested to know more about how they are going to seek out, either on upload, not just Facebook --

Ms. Schakowsky. I am going to have to cut you off at this point, because I do want to ask Mr. Harris.

Given the prevalence of deceptive content online, are platforms doing enough to stop the dissemination of misinformation, and what can government do to prevent such manipulation of consumers? Should government be seeking to clarify the principle that if it is illegal offline then it is illegal online?

Mr. Harris. Yes. A good example of that -- so first is no, the platforms are not doing enough, and it is because their entire business model is misaligned with solving the problem. And I don't vilify the people because of that. It is just their business model is against the issue.

We used to have Saturday morning cartoons. We protected children from certain kinds of advertising, time, place, manner restrictions. When YouTube gobbles up that part of the attention economy, we lose all those protections. So why not bring back the protections of Saturday morning? We used to have fair price, equal price election ads on TV, the same price for each politician to reach someone. When Facebook gobbles up election advertising, we just removed all of those same protections.

So we are basically moving from a lawful society to an unlawful virtual internet society, and that is what we have to change.

Ms. Schakowsky. Thank you. I yield back.

And now the chair recognizes Mrs. Rodgers, our subcommittee ranking member, for 5 minutes.

Mrs. Rodgers. Thank you, Madam Chair.

I referenced how misinformation is not a new problem, but certainly with the speed of information, how it can travel in the online world, its harm is increasing. That said, I have long believed that the way to address information is more transparency, more sources, more speech, not less. This is important, not just in an election cycle, but also in discussions around public health issues, natural disasters, or any number of significant

events. I am worried about this renewed trend, where some want the government to set the parameters and potentially limit speech and expression.

Ms. Bickert, how does free speech and expression factor into Facebook's content decisions, and can you please explain your use of third-party fact-checkers?

Ms. Bickert. Thank you. We are very much a platform for free expression. It is one of the reasons that we work with third-party fact-checking organizations, because what we do if they have ranked something false is, we share more information on the service. So we put a label over it, this is false information, but then we show people here is what fact-checkers are saying about this story.

We work with more than 50 organizations worldwide, and those organizations are chosen after meeting high standards for fact-checking.

Mrs. Rodgers. Thank you. As a follow-up, with the total volume of traffic you have, clearly human eyes alone can't keep up. So artificial intelligence and machine learning have a significant role to identify not only deepfakes, but also other content that violates your terms of service. Would you just explain a little bit more to us how you use AI and the potential to use AI to fight fire with fire?

Ms. Bickert. Absolutely. We do use a combination of technology and people to identify potential information to send to fact-checkers. We also use people and technology to try to assess whether or not something has been manipulated, media. That would be covered by the policy we released yesterday.

So, with the fact-checking program, we use technology to look for things like -- let's say somebody has shared an image or a news story and people are -- friends are commenting on that, saying, Don't you know this is a hoax, or this isn't true. That is the sort of thing our technology can spot and send that content over to fact-checkers.

But it is not just technology. We also have ways for people to flag if they are

seeing something that they believe to be false. That can send content over to fact-checkers. And then the fact-checkers can also proactively choose to rate something that they are seeing on Facebook.

Mrs. Rodgers. Thank you.

Professor Hurwitz, can you briefly describe how user interfaces can be designed to shape consumer choice and how such designs may benefit or harm consumers?

Mr. Hurwitz. They can be used -- they can be modified, created, structured in any number of ways. We have heard examples, font size, text placement, the course of interaction with a website, or even just a phone menu system. These can be used to guide users into making uninformed decisions, or to highlight information that users should be paying attention to. This broadly falls into the category of nudges and behavioral psychology. That is an intensely researched area. It can be used in many ways.

Mrs. Rodgers. You highlighted some of that in your testimony. Would you explain how the FTC can use its existing section 5 authority to address most of the concerns raised by dark pattern practices?

Mr. Hurwitz. Yes, very briefly. I could lecture for a semester on this, not to say that I have.

The FTC has a broad history, long history of regulating unfair and deceptive practices and advertising practices. Its deception authority, false statements, statements that are material to a consumer, making a decision that is harmful to the consumer. They can use adjudication. They can enact rules in order to take action against platforms or any entity, online or offline, that deceives consumers.

Mrs. Rodgers. Do you think that they are doing enough?

Mr. Hurwitz. I would love to see the FTC do more in this area, especially when it

comes to rule-making and in-court enforcement actions, because the boundaries of their authority are unknown, uncertain, untested. This is an area where bringing suits, bringing litigation, that tells us what the agency is capable of, which this body needs to know before it tries to craft more legislation or give more authority to an entity. If we already have an agency that has power, let's see what it is capable of.

Mrs. Rodgers. Right. Okay. Thank you, everyone. I appreciate you all being here. Very important subject, and I appreciate the chair for hosting, or having this hearing today.

Ms. Schakowsky. I thank the ranking member, who yields back. And now I recognize the chair of the full committee, Mr. Pallone, for 5 minutes.

The Chairman. Thank you, Madam Chair.

I have got a lot to ask here, so I am going to ask you for your responses to be brief, if possible. But in your various testimonies, you all talked about a variety of technologies and techniques that are being used to deceive and manipulate consumers.

We have heard about user interfaces designed to persuade, and sometimes trick people, into making certain choices, deepfakes and cheapfakes, that show fictional scenarios that look real, and algorithms designed to keep people's eyes locked on their screens. And we know these things are happening. But what is less clear is how and the extent to which these techniques are being used commercially and on commercial platforms.

So first let me ask Dr. Donovan: As a researcher who focuses on the use of these techniques, do you have sufficient access to commercial platform data to have a comprehensive understanding of how disinformation and fraud is conducted and by whom?

Dr. Donovan. The short brief answer, no.

The Chairman. Your mic.

Dr. Donovan. The brief answer is no, and that is because we don't have access to the data as it is. There are all these limits on the ways in which you can acquire data through the interface.

And then the other problem is that there was a very good-faith effort between Facebook and scholars to try to get a bunch of data related to the 2016 election. That fell apart, but a lot of people put an incredible amount of time, money, and energy into that effort, and it failed around the issues related to privacy and differential privacy.

What I would love to see also happen is Twitter has started to give data related to deletions and account takedowns. We need a record of that so that when we do audit these platforms for either financial or social harms that the deletions are also included and marked. Because even if you can act like a data scavenger and go back and get data, when things are deleted, sometimes they are just gone for good, and those pieces of information are often the most crucial.

The Chairman. Thank you.

Mr. Harris, should the government be collecting more information about such practices in order to determine how best to protect Americans?

Mr. Harris. Yes. Here is an example: So unlike other addictive industries, for example -- addiction is part of the deception that is going on here -- the tobacco industry doesn't know which users are addicted to smoking. The alcohol industry doesn't know exactly who is addicted to alcohol. But unlike that, each tech company does know exactly how many people are checking more than, you know, 100 times a day between certain ages. They know who is using it late at night.

And you can imagine using existing agencies, say Department of Health and Human Services, to be able to audit Facebook on a quarterly basis and say, Hey, tell us

how many users are addicted between these ages, and then what are you doing next quarter to make adjustments to reduce that number? And every day they are the ones issuing the questions, and the responsibility and the resources have to be deployed by the actor that has the most of them, which, in this case, would be Facebook. And there is a quarterly loop between each agency asking questions like that, forcing accountability with the companies for the areas of their existing jurisdiction.

So I am just trying to figure out is that a way that we can scale this to meet the scope of the problem. You realize this is happening to 2.7 billion people.

The Chairman. Thank you. This week, Facebook released a new policy on how it will handle deepfakes. So, Ms. Bickert, under your policy, deepfakes are -- and I am paraphrasing -- videos manipulated through artificial intelligence that are intended to mislead and are not parody or satire. Did I get that right?

Ms. Bickert. Yes, that is right.

The Chairman. Okay. Now, I understand that Twitter and YouTube either do not have or use the same definition for deepfakes, and that is indicative of a lack of consistent treatment of problematic content across the major platforms. Banned hate speech or abusive behavior on one site is permitted on another. There seems to be very little consistency across the marketplace, which leaves consumers at a loss.

So let me go to Dr. Donovan again. Is there a way to develop a common set of standards for these problematic practices so that consumers are not facing different policies on different websites? Your mic, again.

Dr. Donovan. I got it.

I think it is possible to create a set of policies, but you have to look at the features that are consistent across these platforms. If they do, for instance, use attention to a specific post in their algorithms to boost popularity, then we need a regulation around that, especially because bots or unmanned accounts, for lack of a better term, are often used to accelerate content and to move content across platforms.

These are things that are usually purchased off platform, and they are considered a dark market product, but you can purchase attention to an issue. And so as a result, there has to be something more broad that goes across platforms, but also looks at the features and then also tries to regulate some of these markets that are not built into the platform themselves.

The Chairman. All right. Thank you.

Thank you, Madam Chair.

Ms. Schakowsky. Thank you.

Mr. Bucshon, you are recognized for 5 minutes.

Mr. Bucshon. Thank you, Madam Chairwoman. I am sorry, I have two of these

hearings going on at the same time, so I am back and forth.

I appreciate the hearing and the opportunity to discuss the spread of misinformation on the internet, but I want to stress that I am concerned over the efforts to make tech companies the adjudicators of "truth" in quotation marks.

In a country founded on free speech, we should not be allowing private corporations, in my view, or, for that matter, the government, to determine what qualifies as, again in quotation marks, the "truth," potentially censoring a voice because that voice disagrees with a mainstream opinion. That said, I totally understand the difficulty and the challenges that we all face together concerning this issue, and how we are, together, trying to work to address it.

Ms. Bickert, can you provide some more information on how Facebook might or will determine if a video misleads? What factors might you consider?

Ms. Bickert. Thank you. Just to be clear, there are two ways that we might be looking at that issue. One is with regard to the deepfakes policy that we released yesterday. And we will be looking to see, specifically, were we seeing artificial intelligence and deep learning? Was that part of the technology that led to change or fabricate a video in a way that really wouldn't be evident to the average person. And that will be a fundamental part of determining whether there is misleading.

Separately --

Mr. Bucshon. Can I ask a question? Who is the average -- sorry, I will wait until you quit coughing so you can hear me.

Ms. Bickert. I am sorry.

Mr. Bucshon. The question then -- I mean, I am playing devil's advocate here -- who is the average person?

Ms. Bickert. Congressman, these are exactly the questions that we have been

discussing with more than 50 experts, as we have tried to write this policy and get it in the right place.

Mr. Bucshon. And I appreciate what you are doing. I am not trying to be difficult here.

Ms. Bickert. No, these are real challenging issues. It is one of the reasons that we think generally, the approach to misinformation of getting more information out there from accurate sources is effective.

Mr. Bucshon. And you stated in your testimony that once a fact-checker rates a photo or video as false, or partly false, Facebook reduces the distribution. Is there a way for an individual who may have posted these things to protest the decision?

Ms. Bickert. Yes, Congressman. They can go directly to the fact-checker. We make sure there is a mechanism for that. And they can do that either if they dispute it, or if they have amended whatever it was in their article that was the problem.

Mr. Bucshon. Right. Because I would say -- I mean, people with good lawyers can dispute a lot of things, but the average citizen in southwest Indiana who posts something online, there needs to be, in my view, a fairly straightforward process that the average person, whoever that might be, can understand to protest or dispute the fact that their distribution has been reduced. Thank you.

Mr. Hurwitz, you have discussed that the FTC has current authority to address dark pattern. However, I would be interested to know your thoughts on how consumers can protect themselves from these patterns and advertisements. Is the only solution through government action, or can consumer education help highlight these advertisement practices?

Mr. Hurwitz. The most important thing for any company, especially in the online context, is trust, the trust of the consumers. Consumer education, user education is

important, but I think that it is fair to say, with condolences perhaps to Ms. Bickert, Facebook has a trust problem. If consumers -- if users stop trusting these platforms, if hearings such as this shine a light on bad practices, then they are going to have a hard time retaining users and consumers. That puts a great deal of pressure.

In addition, stability of practices. One dark pattern is to constantly change the user interface, so users don't know how it operates. If we have stability, if we have platforms that operate in consistent, predictable ways, that helps users become educated, helps users understand what the practices are, and learn how to operate in this new environment. Trust on the internet is different. We are still learning what it means.

Mr. Bucshon. And I know you went over this, but can you talk again about how these dark pattern practices took place before the internet, and are currently happening in brick-and-mortar stores and other areas, mail pieces that politicians send out.

I mean, I just want to reiterate again, this is a broader problem than just the internet, this is something that has been around for a while.

Mr. Hurwitz. Yes. Dark patterns, these practices, they go back to the beginning of time. Fundamentally, they are persuasion. If I want to convince you of my world view, if I want to convince you to be my customer, if I want to convince you to be my friend, I am going to do things that influence you. I am going to present myself to you in ways that are going to try and get you to like me or my product.

If you come into my store and ask for a recommendation, what size tire do I need for my car? My sales representative is going to give you information. The store is going to be structured -- these have been used consistently throughout --

Mr. Bucshon. My time is expired. My point was is that when we look at this problem, we need to, in my view, take a holistic approach about what has happened in

the past and, with emerging technology, how we address that consistently and not just target specific industries.

Thank you. I yield back.

Ms. Schakowsky. The gentleman yields back.

I now recognize Congresswoman Castor for 5 minutes.

Ms. Castor. Well, thank you, Chairwoman Schakowsky, for calling this hearing.

You know, the internet and online platforms have developed over time without a lot of safeguards for the public. And government here, we exercise our responsibility to keep the public safe, whether it is the cars we drive, or the water we drink, airplanes, drugs that are for sale. And really, the same should apply to the internet and online platforms.

You know, there is a lot of illegal activity being promoted online, where the First Amendment just does not come into play. And I hope we don't go down that rabbit hole, because we are talking about human trafficking, terrorist plots, illicit sales of firearms, child exploitation.

And now, what we have swamping these online platforms that control the algorithms that manipulate the public are the deepfakes, these dark patterns, artificial intelligence, identity theft. But these online platforms, remember, they control these algorithms that steer children and adults, everyone in certain directions, and we have got to get a handle on that.

For example, Mr. Harris, one manipulative design technique is the auto-play feature. It is now ubiquitous across video streaming platforms, particularly billions of people that go onto YouTube or Facebook. This feature automatically begins playing a new video after the current video ends. The next video is determined using an algorithm. It is designed to keep the viewer's attention.

This platform-driven algorithm often drives the proliferation of illegal activities and dangerous ideologies and conspiracy theories. It makes it much more difficult for the average person to try to get truth-based content.

I am particularly concerned about the impact on kids, and you have raised that and I appreciate that. You discuss how the mental health of kids today really is at risk. Can you talk more about the context in which children may be particularly harmed by these addiction-maximizing algorithms and what parents can do to protect kids from becoming trapped in a YouTube vortex, and what you believe our responsibility is as policymakers?

Mr. Harris. Thank you so much for your question. Yeah, this is very deeply concerning to me.

So laying it out, with more than 2 billion users, think of these on YouTube as 2 billion Truman shows. Each of you get a channel, and a super computer is just trying to calculate the perfect thing to confirm your view of reality. This, by definition, fractures reality into 2 billion different polarizing channels, each of which is tuned to bring you to a more extreme view.

The quick example is imagine a spectrum of all the videos on YouTube laid out in one line, and on my left side over here, you have the calm Walter Cronkite rational science side of YouTube, and the other side you have crazy town. You have UFOs, conspiracy theories, Alex Jones, crazy stuff.

No matter where you start on YouTube, you could start in the calm section or you could start in crazy, if I want you to watch more, am I going to steer you that way or that way? I am always going to steer you towards crazy town. So imagine taking the ant colony of 2.1 billion humans and then just tilting it like that.

Three examples of that per your kids example: 2 years ago on YouTube, if a teen

girl watched a dieting video, it would auto-play anorexia videos, because those were more extreme. If you watched a 9/11 news video, it would recommend 9/11 conspiracy theories. If you watched videos about the moon landing, it would recommend flat earth conspiracy theories.

Flat earth conspiracy theories were recommended hundreds of millions of times. This might sound just funny and, oh, look at those people, but, actually, this is very serious. I have a researcher friend who studied this. If the flat earth theory is true, it means not just that all of government is lying to you, but all of science is lying to you. So think about that for a second. That is like a meltdown of all of our rational epistemic understanding of the world.

And, as you said, these things are auto-playing. So auto-play is just like -- it hacks your brain's stopping cue. So, as a magician, how do I know if I want you to stop? I put a stopping cue and your mind wakes up. It is like a right angle in a choice. If I stop drinking, if the water hits the bottom of the glass, I have to make a conscious choice, do I want more? But we can design it so the bowl never stops. We can just keep refilling the water, and you never stop. And that is how we basically have kept millions of kids addicted. In places like the Philippines, people watch YouTube for 10 hours a day, 10 hours a day.

Ms. Castor. This has significant cost to the public, and that is one of the points I hope people will understand. As Dr. Donovan says, there is economy of misinformation now. These online platforms now are passing along -- they are monetizing, making billions of dollars. Meanwhile, public health costs, law enforcement costs are adding up to the public, and we have a real responsibility to tackle this and level the playing field.

Mr. Harris. And by not acting, we are subsidizing our societal self-destruction. I mean, we are subsidizing that right now. So yeah, absolutely. Thank you so much.

Ms. Schakowsky. I recognize Representative Burgess for 5 minutes.

Mr. Burgess. Thank you. Thanks for holding this hearing. I apologize. We have another health hearing going on upstairs, so it is one of those days you got to toggle between important issues.

Mr. Hurwitz, let me start by asking you -- and this is a little bit off topic, but it is important. In 2018, United States District Court for Western Pennsylvania indicted seven Russians for conducting a physical cyber hacking operation in 2016 against Western targets, including the United States Anti-Doping Agency, in response to the revelation of Russia's state-sponsored doping campaign. These hackers were representatives of the Russian military, the GRU. According to the indictment, the stolen information was publicized by the GRU as part of a related influence and disinformation campaign designed to undermine the legitimate interests of the victims. This information included personal medical information about United States athletes.

So these GRU hackers used fictitious identities and fake social media accounts to research and probe victims and their computer networks. While the methods we are talking about today are largely in the context of perhaps deceiving voters or consumers, the harmful potential effects is actually quite large.

So, in your testimony, you defined the dark pattern as the practice of using design to prop desired, if not necessarily desirable behavior. Can these dark patterns be used to surveil people and find ways to hack them in the service of broader state-sponsored operations?

Mr. Hurwitz. Yes, absolutely, they can. And this goes to the broader context in which this discussion is happening. We are not only talking about consumer protection, we are talking about a fundamental architecture. The nature, as I said before, of trust online is different. All of those cues that we rely on for you to know who I am when you

see me sitting here. We have gone through some vetting process to be sitting here. We have identities. We have telltale cues that you can rely on to know who I am and who you are. Those are different online, and we need to think about trust online differently.

One example that I will highlight that goes to an industry-based solution and, more important, the nature of how we need to think about these things differently, in the context of targeted advertising and political advertising in particular, how do we deal with targeted misinformation for political ads?

Well, one approach which Facebook has been experimenting with is, instead of saying you can't speak, you can't advertise, if I target an ad at a group of speakers, Facebook will let someone else target an ad to that same group, or they have been experimenting with this.

It is a different way of thinking about how we deal with establishing trust or responding to untrustworthy information. We need more creative thinking. We need more research about how do we establish trust in the online environment.

Mr. Burgess. Well, thank you, and thank you for those observations.

Ms. Bickert, if I ever doubted the power of Facebook, 3 years ago that doubt was completely eliminated. One of your representatives actually offered to do a Facebook event in the district that I represent in northern Texas. And it was not a political; it was a business-to-business. It is how to facilitate and run your small business more efficiently. And wanted to do a program, and we selected a Tuesday morning. And I asked how big a venue should we get, thinking maybe 20, 30. And I was told 2,000, expect 2,000 people to show up. I am like 2,000 people on a Tuesday morning for a business-to-business Facebook presentation. Are you nuts?

The place was standing room only, and it was the power of Facebook getting the

word out there that this is what we are doing. And it was one of the most well-attended events I have ever been to as an elected representative. So if I had ever doubted the power of Facebook, it was certainly brought home to me just exactly the kind of equity that you are able to wield.

But recognizing that, do you have a sense of the type of information on your platforms that needs to be fact-checked, because you do have such an enormous amount of equity?

Ms. Bickert. Yes, Congressman. And thank you for those words. We are concerned not just with misinformation, that is a concern, and that is why we developed the relationships we have now with more than 50 fact-checking organizations. But we are also concerned with abuse of any type. I am responsible for managing that, so whether it is terror propaganda, hate speech, threats of violence, child exploitation content, content that promotes eating disorders. Any of that violates our policies, and we go after it proactively to try to find it and remove it. That is what my team is.

Mr. Burgess. Do you feel you have been successful?

Ms. Bickert. I think we have had a lot of successes and we are making huge strides. There is always more to do. We have begun publishing reports in the past year and a half or so, every 6 months, where we actually show across different abuse types how prevalent is this on Facebook from doing a sample, how much content did we find this quarter and remove, and how much did we find before anybody reported it to us?

The numbers are trending in a good direction, in terms of how effective our enforcement measures are, and we hope that will continue to improve.

Mr. Burgess. As policymakers, can we access that fund of data to, say, for example, get the number of anti-vaccine issues that have been propagated on your

platform?

Ms. Bickert. Congressman, I can follow up with you on the reports we have and any other information.

Mr. Burgess. Thank you. I will yield back.

Ms. Schakowsky. If I could just clarify that question. Is that information readily available to consumers or no?

Ms. Bickert. Chairwoman, the reports I just mentioned are publicly available and we can follow up with any detailed requests as well.

Ms. Schakowsky. I recognize Mr. Veasey for 5 minutes for questioning.

Mr. Veasey. Thank you, Madam Chair. Outside of self-reporting, what can be done to help educate communities that may be specifically targeted by, you know, all these different platforms?

I was wondering, Mr. Harris, if you could address that specifically, just because I think that a great deal of my constituency, and even on the Republican side, I think, a great deal of their constituencies, are probably being targeted, based on things like race and income, religion, and what have you.

And is there anything outside of self-reporting that can be done to just help educate people more?

Mr. Harris. Yeah, there are so many things here. And, as you mentioned, in the 2016 election Russia targeted African American populations. I think people don't realize -- I think every time a campaign is discovered, how do we back-notify people, all of whom were affected, and say, you were the target of an influence operation.

So right now every single week, we hear reports of Saudi Arabia, Iran, Israel, China, Russia, all doing various different influence operations. Russia was recently going after U.S. veterans. Many veterans would probably say that is a conspiracy theory,

right? But Facebook is the company that knows exactly who was affected, and they could actually back-notify every time there is an influence operation, letting those communities know that this is what happened, and that they were targeted.

We have to move from this is a conspiracy theory to this is real. I have studied cult deprogramming for a while, and how do you wake people up from a cult when they don't know they are in? You have to show them essentially the techniques that were used on them to manipulate them. And every single time these operations happen, I think that has to be made visible to people.

And just like we said, you know, we have laws and protections. We have a Pentagon to protect our physical borders. We don't have a Pentagon to protect our digital borders, and so we depend on however many people Facebook chooses to hire for those teams. One example of this, by the way, is that the city of Los Angeles spends 25 percent of its budget on security. Facebook spends 6 percent of its budget on security, so it is underspending the city of L.A. by about four times.

So, you know, you can just make some benchmarks and say, are they solving the problem? They have got 2.2 billion fake accounts, Facebook has, that they took down, fake accounts. So they have 2.7 billion real accounts and then there was 2.2 billion fake accounts. And, you know, I am sure they got all of them I think would be the line to use here.

Mr. Veasey. Ms. Bickert, you know, given the fact that it does seem like these foreign agents, these foreign actors are targeting people specifically by their race, by their economics, by what region of the country that they live in, is Facebook doing anything to gather information or to look at how specific groups are being targeted?

If African Americans are being targeted for political misinformation; if whites that live in rural America, if they are being targeted for political misinformation; if people

based on their likes -- like, if you could gather information, if these foreign actors could gather information based on people based on things that they like.

So let's say that you were white and you lived in rural America and you liked one American news and you like these other things and you may be more likely to believe in these sorts of conspiracy theories. Are you sure that some of the things that people are sharing on your platform, the likes and dislikes, aren't being used as part of that scheme as well?

Could you answer both of those?

Ms. Bickert. Yes, Congressman. Thank you for the question. There are, broadly speaking two, things that we do. One is trainings and tools to help people, especially those who might be most at risk, recognize ways to keep themselves safe from everything from hacking to scams and other abuse.

Separately, whenever we remove influence operations under our, what we call this coordinated inauthentic behavior -- we have removed more than 50 such networks in the past year -- any time we do that we are very public about it, because we want to expose exactly what we are seeing. And we will even include examples in our post saying, here is a network; it was in this country; it was targeting people in this other country. Here are examples of the types of posts that they were putting in their pages. We think the more we can shine a light on this, the more we will be able to stop it.

Mr. Veasey. Before my time expires, but if people are being scientifically -- if their likes, and Dr. Burgess' district being specifically targeted because of certain television or news programming that they like, if they are African Americans that are being specifically targeted because Russian actors may think that they lean a certain way in politics, don't you think that information ought to be analyzed more closely instead of relying on -- instead of just leaving it up to the user to be able to figure all of this out?

Especially when people work odd hours and may only have time to digest what they immediately read, and they may not have an opportunity to go back and analyze something so deeply as far as what you are saying.

Ms. Bickert. Congressman, I appreciate that. And I will say, attribution is complicated, and understanding the intent behind some of these operations is complicated. We think the best way to do that is to make them public. And we don't just do this ourselves.

We actually work hand in hand with academics and security firms who are studying these types of things, so that they can see. And sometimes we will say as we take down a network, we have done this in collaboration or conversation with, and we will name the group.

So there are groups who can look at this and together hopefully shine light on who the actors are and why they are doing what they are doing.

Mr. Veasey. Thank you. I yield back.

Ms. Schakowsky. I recognize Mr. Latta for 5 minutes.

Mr. Latta. Well, thank you, Madam Chair, and thanks very much for holding this very important hearing today. And thank you to our witnesses for appearing before us. And it is really important for Americans to get this information.

In 2018, the experts out there estimated that criminals were successful in stealing over $37 billion from our older Americans through different scams through the internet, identity theft, friends, family abuse and impostor schemes. And last year in my district, I had the Federal Trade Commission and the IRS out for a senior event, so that the seniors could be educated on the threat of these scams and how to recognize, avoid, ward off and how to recover from them.

Congress recognized that many of these scams were carried out through the use

of manipulative and illegal robocalls. To combat these scams, I introduced the STOP Robocalls Act, which was recently signed into law as part of the tray stack, which I am very glad the President signed over the Christmas holiday.

While I am glad that we were able to get this done, I continue to be concerned with the ability of scammers to evolve and adapt to changes in the law by utilizing new technologies and techniques like deep and cheapfakes.

And, Ms. Bickert, I don't want to pick on you, and I truly appreciate you being here today, especially since you are a little under the weather. And I also appreciated reading your testimony last night. I found it very interesting and enlightening.

I have several questions. As more and more seniors are going online and joining Facebook to keep in contact with their family, friends, and neighbors, in your testimony, you walk us through Facebook's efforts to recognize misinformation and what the company is doing to combat malicious actors using manipulated media. Is Facebook doing anything specifically to help protect seniors from being targeted on the platform or educating them on how to recognize fake accounts or scams?

Ms. Bickert. Thank you for the question. We are, indeed. And that includes both in-person trainings for seniors, which we have done and will continue to do. We also have a guide that can be more broadly distributed that is publicly available that is a guide for seniors on the best ways to keep themselves safe.

But I want to say more broadly, and as somebody who was a Federal criminal prosecutor for 11 years, looking at that sort of behavior, this is something we take seriously across the board. We don't want anybody to be using Facebook to scam somebody else, and we look proactively for that sort of behavior and remove it.

Mr. Latta. Just a quick follow-up. I think it is really important, because, you know, from what we have learned in a lot of times is that seniors don't want to report

things, because they are afraid that, boy, you know, I have been taken. I don't want to tell my relatives, I don't want to tell my friends, because they are afraid of losing some of what they might have, and not just on the money side, but how they can get out there.

And so, I think it is really important that we always think about our seniors and just to follow up, because at the workshop that we had in the District last year, the FTC stated that one of the best ways to combat scams is to educate the individuals on how to recognize the illegal behavior so they can turn that in to educate their friends and neighbors.

In addition to your private sector partnerships, would Facebook be willing to partner with agencies like the FTC to make sure the public is informed about scammers operating on their platform?

Ms. Bickert. Congressman, I am very happy to follow up on that. We think it is important for people to understand the tools that are available to keep themselves safe online.

Mr. Latta. Ms. Donovan.

Dr. Donovan. Yes, one of the things that we should also consider is the way in which people are targeted by age for -- I have looked at reverse mortgage scams, retirement funding scams, fake healthcare supplements. You know, when you do retire, it becomes very confusing. You are looking for information. And if you are looking primarily on Facebook and then posting about it, you might be retargeted by the advertising system itself.

And so, even when you are not information-seeking, Facebook's algorithms and advertising are giving other third parties information, and then serving advertising to seniors. And so it is a persistent problem.

Mr. Latta. Thank you. Again, Ms. Bickert, if I can just follow up quickly with my

remaining 30 seconds. Many of the scammers look for ways to get around Facebook's policies, including through the development and refinement of new technologies and techniques.

Is Facebook dedicating the resources and exploring ways to proactively combat scams instead of reacting after the fact?

Ms. Bickert. Yes, Congressman, we are. I have been overseeing content policies at Facebook for about seven years now, and in that time, I would say that we have gone from being primarily reactive in the way that we enforce our policies to now primarily proactive. We are really going after abusive content and trying to find it. We grade ourselves based on how much we are finding before people report it to us, and we are now publishing reports to that effect.

Mr. Latta. Thank you very much.

Madam Chair, my time is expired and I yield back.

Ms. Schakowsky. The gentleman yields back.

And I now recognize Mr. O'Halleran for 5 minutes.

Mr. O'Halleran. I want to thank the chairwoman for holding this important and timely meeting here today, hearing. I echo the concerns of my colleagues. The types of deceptive online practices that have been discussed today are deeply troubling. I have continually stressed that a top priority for Congress should be securing our U.S. elections.

We could see dangerous consequences if the right tools are not in place to prevent the spread of misinformation online. This is a national security concern. As a former law enforcement officer, I understand that laws can be meaningless if they are not enforced. I look forward to hearing more from our witnesses about the FTC's capabilities and resources to combat these deceptive online practices.

Dr. Donovan, in your testimony you say that regulatory guardrails are needed to protect users from being misled online. I share your concerns about deception and manipulation online, including the rise in use of the dark patterns, deepfakes and other kinds of bad practices that can harm consumers.

Can you explain in more detail what sort of regulatory guardrails are necessary to prevent these instances?

Dr. Donovan. I will go into one very briefly. One of the big questions is if I post something online that is not an advertisement, you know, I am just trying to inform my known networks. The problem isn't necessarily always that there is a piece of fake content out there. The real problem is the scale, being able to reach millions.

In 2010, 2011, we lauded that as a virtue of platforms. It really emboldened many of our important social movements and raised some incredibly important issues. But that wasn't false information. It wasn't meant to deceive people. It wasn't meant to siphon money out of other groups. At that time too, you weren't really able to scale donations. It was much harder to create networks of fake accounts and pretend to be an entire constituency.

And so, when I talk about regulatory guardrails, we have to think about distribution differently than we think about the content. And then we can also assuage some of the fears that we have about freedom of expression by looking at what are the mechanisms by which people can break out of their known networks? Is it advertising? Is it the use of fake accounts? How are people going viral? How are posts going viral, information going viral?

The other thing I would like to know from the government perspective is, does the FTC have enough insight into platforms to monitor that, to understand that? And if they don't, if they don't know why and how tens of millions of dollars are being siphoned out

of Trump's campaign, then that is also another problem and we have to think about what does transparency, what does auditing look like in a very meaningful way.

Mr. O'Halleran. Doctor, do you believe then that the FTC has the adequate authority under section 5 of the FTC Act to take action against individuals and companies engaged in deceptive behavior practices online? And I do want to point out a Wall Street Journal report that said of the millions of dollars, 200-and-some million dollars of fines that they have only collected about $7,000 since 2015.

Dr. Donovan. Wow. I think that you do have to look a lot closer at what the FTC has access to and how they can make that information actionable. For example, proving that there is substantial injury, if only one group has access to the known cost or knows the enormity of a scam, then we have to be able to expedite the transfer of data and the investigation in such a way that we are not relying on journalists or researchers or civil society organizations to investigate. I think that the investigatory powers of the FTC have to also include assessing substantial injuries.

Mr. O'Halleran. Thank you, Doctor.

Mr. Harris, do you believe the agency has enough resources to responsibly, swiftly, and appropriately address the issues? And I just want to point out that we flat-line them all the time. And on the other side, industry continues to expand at exponential rates.

Mr. Harris. That is the issue that you are pointing to is that the problem-creating aspects of the technology industry, because they operate at exponential scales, create exponential issues, harms, problems, scams, et cetera. And so how do you, you know, have a small body reach such large capacities? This is why I am thinking about how can we have a digital update for each of our different agencies who already have jurisdiction over, whether it is public health or children or scams or deception, and just have them ask

the questions that then are forced upon the technology companies to use their resources to calculate, report back, set the goals for what they are going to do in the next quarter.

Mr. O'Halleran. Thank you, Mr. Harris.

And I yield.

Ms. Schakowsky. The chair now recognizes Mr. Carter for 5 minutes.

Mr. Carter. Thank you, Madam Chair.

And thank all of you for being here. This is extremely important and extremely important to all of our citizens.

I want to start by saying that, you know, when we talk about deepfake and cheapfake, to me, that is somewhat black and white. I can understand it. But, Mr. Hurwitz, when we talk about dark patterns, I think that is more gray in my mind. And I will just give you an example.

I was a retailer for many years. And I grew up in the South, okay? We had a grocery store chain, some of you may be familiar with it, Piggly Wiggly. Now, I always heard that the way they got their name -- and I tried to fact-check it, but I couldn't find it. But anyway, I always heard the way they got their name is they arranged their stores to when you went in you had to kind of wiggle all the way around before you could get back out so that you would buy more things. It was like a pig wiggling through the farmyard or something. And they came up with Piggly Wiggly. Well, that is marketing.

And, you know, another example is all of us go to the grocery store. When we are at the grocery store and you are in the checkout line, you got all these things up there that they are trying to get you to buy. They are not necessarily -- you could argue that they are impulse items. But then again, you could also make the argument that when you get home you say, geez, I wish I had gotten that at the grocery store. I wish I would have gotten these batteries or Band-Aids or whatever.

How do you differentiate between what is harmful and what is beneficial?

Mr. Hurwitz. A great question, because it is gray. And, as I said previously, dark patterns, the term itself is a dark pattern intended to make us think about this as dark. There are some clear categories, clear lies, clear false statements, where we are talking about classic deception. That is pretty straightforward.

But when we are talking about more behavioral nudges, it becomes much more difficult. Academics have studied nudges for decades at this point, and it is hard to predict when they are going to be effective, when they are not going to be.

In the FTC context, the deception standard has a materiality requirement. So there needs to be some demonstration that a practice is material to the consumer harm, and that is a good sort of framework. If we don't have some sort of demonstrable harm requirement and causal connection there, I am a law professor, causation is a basic element of any legal claim. If you don't have some ability to tie the act to the harm, you are in dark waters for due process.

Mr. Carter. So do you think we should be instructing the FTC to conduct research on this as to what is going on here?

Mr. Hurwitz. I think more information is good information. The FTC is conducting some hearings already. I think greater investigation is very powerful, both so that the FTC understands what they should be doing so they can use this information to establish rules. Where materiality is difficult to establish, the FTC can issue a rule, go through a rule-making process which makes it easier to substantiate an enforcement action subsequently.

And even to respond, in part, to a previous question, to the extent that one of the FTC's core powers, even if it doesn't lack this as an enforcement authority, is to report to this body and say, Look, we are seeing this practice. It is problematic. We don't have

the authority. Can you do something about it? And perhaps this body will act and give it power, perhaps this body will take direct action, or perhaps the platforms and other entities will say, Oh, wow, the jig's up, we should change our practices before Congress does something that could be even more detrimental to us.

Mr. Carter. Right. Mr. Harris, did you have something?

Mr. Harris. Yes. I have studied this topic for also about a decade. So you asked what is different about this? You have got the pig going through the thing. You have got the supermarket aisle. You have got the last minute of sort of last-minute purchase items. There are two distinct things that are different.

The first is that this is infrastructure we live by. When you talk about children waking up in the morning and you have auto-play, that is not like the supermarket where I occasionally go there and I just made some purchases and I am at the very end of it, and that is the one moment, the one little micro-situation of deception or marketing, which is okay.

In this case, we have children who are like spending 10 hours a day. So imagine a supermarket, you are spending 10 hours a day and you wake up in that supermarket. And so that is the degree of intimacy and sort of scope in our lives. That is the first thing.

The second thing is the degree of asymmetry between the persuader and the persuadee. So in this case, you have got someone who knows a little bit more about marketing who is arranging the shelf space so that the things in the top are at eye level versus at bottom level. That is one very small amount of asymmetry.

But in the case of technology, we have a supercomputer pointed at your brain, meaning like the Facebook news feed sitting there, and using the vast resources of 2.7 billion people's behavior to calculate the perfect thing to show you next and to not be

discriminant about whether it is good for you, whether it is true, whether it is trustworthy, whether it is credible. And so, it knows more about your weaknesses than you know about yourself, and the degree of asymmetry is far beyond anything we have experienced.

Mr. Carter. And you want the Federal Government to control that?

Mr. Harris. I think we have to ask questions about when there is that degree of asymmetry, about intimate aspects of your weaknesses, and its business model is to exploit that asymmetry. It is as if a psychotherapist who knows everything about your weaknesses, uses it with a for-profit advertising business model.

Mr. Hurwitz. The challenge is that can also go the other way. It can used to strength.

Mr. Carter. Yes, yes.

Mr. Hurwitz. Mr. Harris used the example earlier of what if auto-play is shifting us towards conspiracy theories. Okay, that is a dark pattern, that is bad. What if, instead, it was using us to shift us the other way, to the light, to greater education. If we say auto-play is bad, then we are taking both of those options off the table.

This can be used for good, and the question that you asked about how do we differentiate between good uses and bad, that is the question.

Mr. Carter. Thank you, Madam Chair. I yield back.

RPTR DEAN

EDTR CRYSTAL

[12:15 p.m.]

Ms. Schakowsky. Mr. Cardenas is recognized for 5 minutes.

Mr. Cardenas. Thank you, Madam Chair, and thank you so much for holding this very important hearing that, unfortunately, I think most Americans don't understand how important this is to every single one of us, especially to our children and future generations.

There is an app, TikTok, question mark. Is it a deepfake maker? Five days ago, TechCrunch reported that ByteDance, the parent company of the popular video-sharing app TikTok, may have secretly built a deepfake maker. Although there is this no indication that TikTok intends to actually introduce this feature, the prospect of deepfake technology being made available on such a massive scale and on a platform that is so popular with kids raises a number of troubling questions.

So my question to you, Mr. Harris, is in your testimony you discuss at length the multitude of ways that children are harmed by new technology. Can you talk about why this news may be concerning?

Mr. Harris. Yes. Thank you for the question.

So deepfakes is a really complex issue. I think if you look at how other governments are responding to this, I don't mean to look at China for legal guidance, but they see this as so threatening to their society, the fabric of truth and trust in their society, that if you post a deepfake without labeling it clearly as a deepfake you can actually go to jail.

So they are not saying if you post a deepfake you go to jail. They are saying if

you post it without labeling it, you go to jail. You can imagine a world where Facebook says, if you post a deepfake without labeling it, we actually maybe suspend your account for 24 hours, so that you sort of feel -- and we label your account to other people who see your account --

Mr. Cardenas. Hold on a second. My colleague on the other side of the aisle just warned, quote, "And you want to have the government control this?" You just gave an example of where private industry could, in fact, create deterrents --

Mr. Harris. That is right.

Mr. Cardenas. -- to bad behavior, not the government, but actual industry. Okay, go ahead.

Mr. Harris. So that is right. And so they can create -- and that is the point, is instead of using these AI whack-a-mole approaches where the engineers at Facebook -- how many engineers at Facebook speak the 22 languages of India where there was an election last year? They are controlling the information infrastructure not just for this country, but for every country, and they don't speak the languages of the countries that they operate in and they are automating that.

And instead of trying to use AI where they are just missing everything going by -- yes, they have made many investments, we should celebrate that, there are people working very hard, it is much better than it was before -- but they have created a digital Frankenstein where there is far more content, advertising, variations of texts, lies, et cetera, than they have the capacity to deal with.

And so you can't create problems way beyond the scope of your ability to address them. It would be like creating nuclear power plants everywhere with the risk of meltdown, without actually having a plan for security.

Mr. Cardenas. Now, getting back to your example where industry could, in fact,

for example, Facebook could say we are going to suspend your account for 24 hours or something like that, with all due respect, in that example, Facebook might lose a little bit of revenue, as well as the person that they are trying to deter from bad action is likely going to lose revenue as well, correct?

Mr. Harris. That is correct. But maybe that is an acceptable cost, given we are talking about the total meltdown of trust.

Mr. Cardenas. Yes, but maybe it is acceptable when you look at it intellectually and honestly. But when you look at it from whether or not private industry is going to take it upon themselves to actually impact their shareholders' revenue, that is where government has a place and space to get involved and say, proper actions and reactions need to be put in place so that people can understand that you can't and you shouldn't just look at this from a profit center motive.

Mr. Harris. That is right.

Mr. Cardenas. Because in this world sometimes the negative actions are more profitable for somebody out there than positive good actions. And that is one of the things that is unfortunate.

And you talk about languages around the world, but the number one target, in my opinion, for these bad actions for both financial gain and also the tearing down of the fabric of the democracy of the greatest Nation on the planet, the United States, is the United States, we are the biggest target for various reasons.

Two main reasons are because we are supposed to be the shining light on the hill for the rest of the world for what a good democracy should be like. And secondly, we are by far and away the largest economy, the biggest consumer group of folks on the planet.

So, therefore, there is a motive for people to focus on profit and focus on their

negative bad intentions against our interests, the interests of the American people. Is that accurate?

Mr. Harris. That is exactly right. And this is a national security -- I see this as a long-term -- I mean, the polarization dynamics are accelerating towards civil war-level things, #civilwariscoming.

Our colleague Renee DiResta says: If you can make it trend, you can make it true. When you are planting these suggestions and getting people to even think those thoughts because you can manipulate the architecture, we are profiting, as I said, we are subsidizing our own self-destruction if the government doesn't say that these things can't just be profitable.

Mr. Cardenas. Thank you to the witnesses. And thank you, Mr. Harris. I have run out of time. I wish I had more time. Thank you.

Ms. Schakowsky. The gentleman yields back.

And now I recognize Mr. Soto for 5 minutes.

Mr. Soto. Thank you, Madam Chair.

It has been my experience that a lie seems to be able to travel faster on the internet than the speed of light while the truth always goes at such a snail's pace. I suppose that is because of the algorithms we see.

I want to start with deepfakes and cheap fakes. We know through New York Times v. Sullivan that defamation of public figures requires actual malice. And some of these just appear to be malicious on their face.

I appreciate the labeling, Ms. Bickert, that Facebook is doing now. That is something that we actually were pondering in our office as well. But why wouldn't Facebook simply just take down the fake Pelosi video?

Ms. Bickert. Thank you for the question.

Our approach is to give people more information so that if something is going to be in the public discourse, they will know how to assess it, how to contextualize it. That is why we work with the fact-checkers.

I will say that in the past 6 months it is feedback from academics and civil society groups that has led us to come up with stronger warning screens.

Mr. Soto. Would that be labeled under your current policy now as false, that video?

Ms. Bickert. I am sorry, which video?

Mr. Soto. Would the fake Pelosi video be labeled as false under your new policy?

Ms. Bickert. Yes. And it was labeled false. At the time we did -- we think we could have gotten that to fact-checkers faster and we think the label that we put on it could have been more clear. We now have the label for something that has been rated false. You have to click through it so it actually obscures the image. And it says, false information. And it says, this has been rated false by fact-checkers. You have to click through it and you see information from the fact-checking source.

Mr. Soto. Thanks.

In 2016 there was a fake Trump rally put together by Russians in Florida, complete with a Hillary Clinton in a prison and a fake Bill Clinton.

Could a fake rally be created today through Facebook in the United States by the Russians under existing technology?

Ms. Bickert. The network that created that was fake and inauthentic, and we removed it. We were slow to find it.

I think our enforcement has gotten a lot better. And as a data point for that, in 2016 we removed one such network. This past year we removed more than 50 networks. Now, that is a global number all over the world. But these are organizations

that are using networks of accounts -- some fake, some real -- in an attempt to obscure who they are or to push false information.

Mr. Soto. So could it happen again right now?

Ms. Bickert. Our enforcement is not perfect. However, we have made huge strides, and that is shown by the dramatic increase in the number of networks that we have removed.

And I will say that we do it not just by ourselves, but we work with security firms and academics who are studying this to make sure we are staying on top of it.

Mr. Soto. What do you think Facebook's duty is, as well as other social media platforms, to prevent the spread of lies across the internet?

Ms. Bickert. I am sorry. Could you repeat that?

Mr. Soto. What you do think Facebook and other social platforms' duty is to prevent the spread of lies across the internet?

Ms. Bickert. I can speak for Facebook. We think it is important for people to be able to connect safely and with authentic information. And my team is responsible for both.

So there is our approach to misinformation where we try to get people -- label contented as false and get them accurate information. And then there is everything we also do to remove abusive content that violates our standards.

Mr. Soto. Thank you, Ms. Bickert.

Dr. Donovan, I saw you reacting to the fake Trump rally aspect. Could that still happen now under existing safeguards in social media?

Dr. Donovan. Yeah. And the reason why it can still happen is because the platform's openness is now turning into a bit of a vulnerability for the rest of society.

So what is dangerous about events like that is the kind of research we do we are

often trying to understand, well, what is happening online. And what happens when the wires -- the interaction between the wires and the weed? Like when people start to be mobilized, start to show up places, that to us is one order of magnitude much more dangerous.

Mr. Soto. What do you think we should be doing as government to help prevent something like that?

Dr. Donovan. There are ways in which I think when people are using particularly events features, group features, there has to be added transparency about who, what, when, where those events are being organized by.

And there have been instances in Facebook very recently where they have added transparency pages, but it is not always clear to the user who is behind what page and for what reason they are launching a protest.

What is dangerous, though, is that actual constituents show up, real people show up as fodder for this. And so we have to be really careful that they don't stage different parties like they did in Texas across the street from one another at the same time. And so we don't want to have manipulation that creates this serious problem for law enforcement, as well as others in the area.

Mr. Soto. Thanks. My time has expired.

Ms. Schakowsky. I now recognize Congresswoman Matsui for 5 minutes.

Ms. Matsui. Thank you very much, Madam Chair. And I really appreciate the witnesses here today, especially on this really important issue.

I introduced the Blockchain Promotion Act with Congressman Guthrie to direct the Department of Commerce to convene a working group of stakeholders to develop a consensus-based definition of blockchain. Currently there is no common definition, which has hindered its deployment.

Blockchain technology could have interesting applications in the communication space, including new ways of identity verification. This technology is unique in that it can help distinguish between credible and noncredible news sources in a decentralized fashion, rather than relying on one company or organization to serve as a sole gatekeeper.

I have a lot of questions. I would like succinct answers to this.

Ms. Donovan, do you see value in promoting impartial decentralized methods of identity verification as a tool to combat the spread of misinformation?

Dr. Donovan. I think in limited cases yes, especially around purchasing of advertising which is allowing you to break out of your known networks and to reach other people, especially if those advertising features do allow you to target very specific groups.

I am interested in learning more about this consensus on definition because I also think it might help us understand what is a social media company, what are their -- how do we define their broadcast mechanisms, how do we define them related to the media, media company, as well as the other kinds of products that they build. And I think it would also get us a lot further in understanding what it is we say when we say deepfakes or even AI.

Ms. Matsui. Okay. The European Commission has recently announced that it will be supporting research to advance blockchain technology to support a more accurate online news environment.

The entire panel, just a yes or no is sufficient.

Do you believe the U.S. should be keeping pace with Europe in this space? Yes or no?

As far as blockchain, do you think that the European Commission is supporting research to advance blockchain technology to support a more accurate online news

development? Do you believe that the U.S. should be keeping pace with Europe regarding this?

Ms. Bickert. This is not my area.

Ms. Matsui. Okay. Dr. Donovan, I probably would say --

Dr. Donovan. Yeah, more research could help us understand this better.

Ms. Matsui. Mr. Hurwitz, yes or no?

Mr. Hurwitz. Around the world many are outpacing us in blockchain.

Ms. Matsui. Okay.

Mr. Harris?

Mr. Harris. It is not my area, but I know that China is working on a decentralized currency and could basically get all of the countries in which it is indebting them to their infrastructure with these huge Belt and Road plans. If they switch the global currency to their decentralized currency, that is a major national security threat and would change the entire world order. I think much more work has to be done in the U.S. to protect against China gaining currency advantage and changing the world of reserve currency.

Ms. Matsui. Thank you.

It is an undisputed fact, reaffirmed by America's intelligence agencies, that Russia interfered in our 2016 and 2018 elections through targeted and prolonged online campaigns. We know that Russia is ramping up for 2020, and the American voters will once again be exposed to new lies, falsehoods, and misinformation designed to sow division in our democratic process.

While I was glad to see the recent funding bill included $425 million in election security grants, this is only part of a much larger solution. To protect the most fundamental function of our democracy, social media companies need to take clear, forceful action against foreign attempts to interfere with our elections.

Mr. Harris, how have the various election interference strategies evolved from the 2016 and 2018 election cycles?

Mr. Harris. You know, I am actually not an expert on exactly what Russia is doing now. What I will say is I think that we need a mass public awareness campaign to inoculate the public. Think of it as like a cultural vaccine.

And there is actually precedent in the United States for this. So back in the 1940s, we had the Committee for National Morale and the Institute for Propaganda Analysis that actually did a domestic awareness campaign about the threat of fascist propaganda.

You have probably seen the videos from -- they are black and white -- from 1947. It was called, "Don't Be a Sucker." And they had us looking at a guy spouting fascist propaganda, someone starting to nod, and then the guy taps him on the shoulder and says, "Now, son, that is fascist propaganda and here is how to spot it."

We actually saw this as a deep threat, a national security threat to our country. We could have another mass public awareness campaign now and we could have the help of the technology companies to collectively use their distribution to distribute that inoculation campaign so everybody actually knew the threat of the problem.

Ms. Matsui. Does the rest of the panel agree with Mr. Harris on this, to have this public awareness campaign?

Mr. Hurwitz. Probably I will just note that it runs the risk of being called a dark pattern if the platforms are starting to label certain content in certain ways. So there is a cross current for our discussion to note there.

Ms. Matsui. Okay. Well, we don't come to any solutions now, but I appreciate it. And I have run out of time. Thank you very much.

Ms. Bickert. Congresswoman, I would just point to the ads library that we have

put in place over the past few years, which has really brought an unprecedented level of openness to political advertising. So people can now see who is behind an ad, who paid for it, and we verify the identity of those advertisers.

Ms. Matsui. I think it is difficult for most people out there to really do that, unless it is right in front of them. But I am glad that that is happening. But I think we should have much more exposure about this.

Thank you.

Ms. Schakowsky. I now recognize Mr. McNerney for 5 minutes.

Mr. McNerney. I thank the chair.

And I thank the witnesses. You testimony has been helpful and I appreciate it. But I have to say, with big power comes big responsibility, and I am disappointed, in my opinion, that Facebook hasn't really stepped up to that responsibility.

Back in June, I sent a letter to Mr. Zuckerberg, and I was joined by nearly all the Democrats on the committee. In this letter we noted that we are concerned about the potential conflict of interest between Facebook's bottom line and addressing misinformation on its platform. Six months later, I remain very concerned that Facebook is putting its bottom line ahead of addressing misinformation.

Ms. Bickert, Facebook's content monetization policy states that content that depicts or discusses subjects in the following categories may face reduced or restricted monetization, and misinformation is included on the list. It is troubling that your policy doesn't simply ban misinformation.

Do you think there are cases where misinformation can and should be monetized? Please answer yes or no.

Ms. Bickert. Congressman, no. If we see somebody that is intentionally sharing misinformation, and we make this clear in our policies, they will lose the ability to

monetize.

Mr. McNerney. Okay. Well, that sounds different than what is in your company's stated policy.

But the response I received from Facebook to my letter failed to answer many of my questions. For example, I asked the following question that was left unanswered and I would like to give you a chance to answer it today. How many project managers does Facebook employ whose full-time job it is to address misinformation?

Ms. Bickert. Congressman, I don't have a number of PMs. I can tell you that across my team, our engineering teams, and our content review teams, this is something that is a priority. Building that network of the relationships with more than 50 fact-checking organizations is something that has taken the efforts of a number of teams across the company.

Mr. McNerney. Does that include software engineers?

Ms. Bickert. It does, because there for any of these programs you need to have an infrastructure that can help recognize when something might be misinformation, allow people to report when something might be misinformation, get things over to the fact-checking organization.

Mr. McNerney. Okay. So I am going to ask you to provide that information, how many full-time employees, including software engineers who were employed in that, to identify misinformation.

Ms. Bickert. We are happy to try to follow up and answer.

Mr. McNerney. Another question that was left unanswered is, on average, from the time a content is posted on Facebook's platform, how long does it take for Facebook to flag suspicious content to third-party fact-checkers, third-party fact-checkers to review the content, and Facebook to take remedial action once the content -- once the review is

completed?

Ms. Bickert. Congressman, the answer depends. This could happen very quickly. We actually allow fact-checking organizations to proactively rate content they see on Facebook. So they --

Mr. McNerney. You think that would be fast enough to keep deepfakes from going viral or other misinformation from going viral?

Ms. Bickert. If they rate something proactively then it happens instantly. And we also use technology and use the reporting to flag content to them and we often see that they will rate it very quickly.

Mr. McNerney. Well, moving on, I am very concerned that Facebook is not prepared to address misinformation on its platform in advance of this year's election. Will you commit to having a third-party audit conducted by June 1 of Facebook's practices for combating the spread of disinformation on its platform and for the results of this audit to be made available to the public?

Ms. Bickert. Congressman, we are very happy to answer any questions about how we do what we do. We think transparency is important. And we are happy to follow up with any suggestions that you have.

Mr. McNerney. I would request a third-party audit -- I am not talking about the civil rights audit -- an independent third-party audit be conducted at Facebook by June 1.

Ms. Bickert. Congressman, again, we are very transparent about what our policies and practices are, and we are happy to follow up with any specific suggestions.

Mr. McNerney. Mr. Harris.

Mr. Harris. I was going to say, their third-party fact-checking services are massively understaffed, underfunded, and a lot of the people are dropping out of the program. And the amount of information flowing through that channel is far beyond

their capacity to respond.

More or less, fact-checking isn't even really the relevant issue. I think if you look at the clearest evidence of this is Facebook's own employees wrote a letter to Mark Zuckerberg saying: You are undermining our election integrity efforts with your current political ads policy.

That says it all to me, that letter was leaked to The New York Times about a month ago, I think that those people, because they are closest to the problem, they do the research queries, they understand how bad the issue is.

We are on the outside. We don't actually know. It is almost like they are Exxon, but they also own the satellites that would show us how much pollution there is. So we don't actually know on the outside. So all we can do is trust people like that on the inside that are saying this is far less than what we would like to do. And they still have not updated their policy.

Mr. McNerney. Thank you. I yield back.

Ms. Schakowsky. I recognize Congresswoman Dingell for 5 minutes for questions.

Mrs. Dingell. Thank you, Madam Chair.

And thank you all of you for being here today. This is a subject it that really matters to me, like it does to all of us. But in the past we have treated what little protections people have online as something that is separate from those we have in our day-to-day lives offline. But the line between what happens online and offline is virtually nonexistent. Gone are the days when we can separate one from the other.

Millions of Americans have been affected by data breaches and privacy abuses. The numbers are so large that you can't even wrap your head around them. I mean, I have talked to Members here and they don't even at times understand what has

happened or how people have collected data about us.

The resources to help folks protect themselves after the fact are desperately needed. But what is really happening is that the cost of failure to protect sensitive information is being pushed on millions of people who are being breached and not trying to do anything. It is a market externality.

And that is where the government, I believe, must step in. You go to the pharmacy to fill a prescription, you assume that the medicine you are going to get is going to be safe, it is not going to kill you. If you go outside, you assume that the air you breathe, you assume, is going to be safe or we are trying to make it that way.

And that is because we have laws that protect people from have a long list of known market externalities and the burden isn't placed on their ability to find out is the medicine you are taking okay, safe, and is the air you are breathing clean. We are still working on that, but it is one we have identified. It shouldn't be any different for market externalities that are digital.

Ms. Bickert, I will admit I have sent a letter to Facebook today which has a lot of questions that didn't lend themselves to answer here, so I hope that they will be answered.

But I would like to get yes-or-no answers from the panel on the following questions. And I am going start this way, with Mr. Harris, because we always start with you, Ms. Bickert, and we will give you a little -- and thank you for being here even though you are sick.

Do you believe that the selling of real-time cell phone location without users' consent constitutes a market externality?

Mr. Harris?

Mr. Harris. I don't know with that specific one, but the entire surveillance

capitalism system produces vast harms that are all on the balance sheets of societies, whether that is the mental health of children, the manipulation of elections, the breakdown of polarization.

Mrs. Dingell. But it is a market externality.

Mr. Harris. Absolutely, all market externality.

Mrs. Dingell. Okay, let's go down.

Mr. Hurwitz?

Mr. Hurwitz. Based on the economic definition of an externality, no, it is not. However, it can be problematic.

Mrs. Dingell. Dr. Donovan?

Dr. Donovan. I am in line with Gus.

Mrs. Dingell. Ms. Bickert?

Ms. Bickert. I am not an economist, but we do think user consent is very important.

Mrs. Dingell. Second question, yes or no, do you believe that having 400 million pieces of personally identifiable information made public, including passport numbers, names, addresses, and payment information, is a market externality?

Mr. Harris?

Mr. Harris. Similarly, on sort of classic economic definition, I don't know if that would specifically qualify, but it is deeply alarming.

Mr. Hurwitz. Same answer.

Dr. Donovan. Agreed.

Ms. Bickert. Same answer.

Mrs. Dingell. So are you all agreeing with Mr. Harris?

Mr. Hurwitz. Same answer as I gave previously. It is not the technical

economic definition.

Mrs. Dingell. I just wanted to see if we had gotten you to understand what a bother it is.

Three, do you believe that having 148 million individuals' personally identifiable information, including credit card numbers, driver's license, and Social Security numbers, made public is a market externality?

Mr. Harris?

Mr. Harris. I can see it is sort of like an oil spill externality.

Mrs. Dingell. Mr. Hurwitz?

Mr. Hurwitz. The same answer.

Mrs. Dingell. So you don't think it is a problem.

Mr. Hurwitz. I don't -- I don't not think it is a problem. I wouldn't characterize it as an externality and use it as a --

Mrs. Dingell. Do you not think we have got to protect people from that?

Mr. Hurwitz. No, that is not what I am saying. I have an economics background. I rely on a more technical definition of an externality.

Mrs. Dingell. Dr. Donovan?

Dr. Donovan. It is an incredibly important problem.

Mrs. Dingell. Ms. Bickert?

Ms. Bickert. Yes, I would echo Dr. Donovan.

Mrs. Dingell. Do you believe that having the data of 87 million users taken and used for nefarious and political purposes is a market externality?

Mr. Harris?

Mr. Harris. I think it is the same answer as before.

Mr. Hurwitz. If I break into your house and steal your stuff and sell it on the

black market, that is not an externality, however it is a problem.

Mrs. Dingell. Dr. Donovan?

Dr. Donovan. Well, I wouldn't characterize it as a break-in. It was facilitated by the features built into the platform and it is a huge problem.

Mrs. Dingell. Thank you.

Ms. Bickert?

Ms. Bickert. Again, we think that user control and consent is very important.

Mrs. Dingell. Last question, I am out of time, so you are going to have to be fast.

And finally, do you believe that simply asking whoever took it to please delete it is an appropriate response?

Mr. Harris?

Mr. Harris. It is very hard to enforce that. And once the data is out there, it is distributed everywhere. So we have to live in a world where now we assume that this is just out there.

Mr. Hurwitz. You need to solve the problem on the front end.

Mrs. Dingell. Dr. Donovan?

Dr. Donovan. That never should have been allowed in the first place.

Mrs. Dingell. Ms. Bickert?

Ms. Bickert. Again, we think that it is very important to give people control over their data and we are doing our best to make sure that we are doing that.

Mrs. Dingell. So I am out of time. Thank you, Madam Chair.

Ms. Blunt Rochester. [Presiding.] Thank you. The gentlewoman yields. And I recognize myself for 5 minutes.

Thank you to the chairwoman in her absence, and thank you to the panelists.

This is a vitally important conversation that we are having. What I have noticed

is that technology is outpacing policy and the people. And so we are feeling the impacts in our mental health, we are feeling it in our economy, we are feeling it in our form of government. And so this is a very important conversation.

And I would like to start with a few questions that are kind of off of the dark patterns and those issues but really do deal with the idea of deceptive and manipulative practice. And it is just a basic question, so yes or no, and it is really surrounding the platforms that we have and the ability for people with disabilities to use them.

Are each of you or any of you familiar with the term universal design? And I will just ask Mr. Harris.

Mr. Harris. Vaguely, yes.

Ms. Blunt Rochester. Mr. Hurwitz?

Mr. Hurwitz. Vaguely, yes.

Dr. Donovan. Yes.

Ms. Blunt Rochester. Yes.

Ms. Bickert. Vaguely, yes.

Ms. Blunt Rochester. Vaguely. Okay. So there have a lot of vaguelies, and I don't have time to really talk about what is universal design is. But I think as we look at how people are treated in our society, universal design and looking at people with disabilities is one of the areas that I would like to follow up with each of you on.

I would now like to turn my time to a discussion about dark patterns. And every single Member of Congress and every one of our constituents, virtually everyone, has been affected by this in some respect. Every day, whether it is giving up our location data, or manipulated into purchasing products that they don't need, or providing sensitive information that enables scams, many of us are targeted.

And while the failure to address dark patterns harms individuals, one of the areas

that is of deeper concern to me is the challenge for us as a society as a whole. Cambridge Analytica, that scandal in and of itself was a great example for all of us of it wasn't just an individual that was harmed, it was our society, and we see some of the remnants of it to this day.

And so I heard someone say to me yesterday that they hoped that this hearing was not just a hearing, but a real wakeup call, a wakeup call to our country. And so my first question is to Mr. Harris.

Do you believe that oversight of dark patterns and the other deceptive and manipulative practices discussed here are well suited for industry self-regulation?

Mr. Harris. No, absolutely not.

Ms. Blunt Rochester. And I would like to follow up with Ms. Bickert.

Does Facebook have a responsibility to develop user interfaces that are transparent and fair to its users?

Ms. Bickert. We definitely want that. And, yes, I think we are working on new ways to be transparent all the time.

Ms. Blunt Rochester. Does Section 230 of the Communications Decency Act provide immunities to Facebook over these issues?

Ms. Bickert. Section 230 is an important part of my team being able to do what we do. So, yes, it gives us the ability to proactively look for abuse and remove it.

Ms. Blunt Rochester. But does it provide immunities? You would say yes?

Ms. Bickert. I am sorry, what is the specific -- Section 230 does provide us certain protections. The most important from my standpoint is the ability for us to go after abuse on our platform. But separately it is also an important mechanism for people who use the internet to be able to post to platforms like Facebook.

Ms. Blunt Rochester. I guess one of my concerns here for asking that question is

we are having a big conversation about the balance of freedom of speech, in addition to the ability for people to yell fire in a crowded place. And so I am going to turn back to Mr. Harris.

How do you think that we in Congress can develop a more agile and responsive response to the concerning trends on the internet? You mentioned a digital update of Federal agencies. Can you talk a little bit but that as well?

Mr. Harris. Just as you said, that the problem here is we have -- this is E.O. Wilson -- the problem of humanity is we have paleolithic emotions, Medieval institutions, and accelerating God-like technology. When your steering wheel goes about a light year behind your accelerating God-like technology, the system crashes.

So the whole point is we have to give a digital update to some of the existing institutions -- Health and Human Services, FCC, FTC, you can imagine every category of society -- and saying where do we already have jurisdiction about each of these areas and ask them to come up with a plan for what their digital update is going to be and put the tech companies in a direct relationship where every quarter there is an audit and there is a set of actions that are going to be taken to ameliorate these harms.

That is the only way I can see scaling this absent creating a whole new digital Federal agency which will be way too late for these issues.

Ms. Blunt Rochester. I know I am running out of time, but my other question really was going to be to Ms. Bickert on the role that you see of government. I think we are having a lot of conversations here about freedom of speech and also the role of government.

And so as a follow-up, I would like to have a conversation with you about what you see as that role of government versus self-regulation, and how we can make something happen here. The bigger concern is for us to make sure that we are looking

at this both as an individual level, but also as a society.

And I yield my time and recognize the gentlewoman from New York, Ms. Clarke.

Ms. Clarke. Thank you very much, Madam Chair.

And I thank our ranking member, I thank our panelists for their expert witness here today.

Deepfakes currently pose a significant and an unprecedented threat. Now more than ever we need to prepare for the possibility that foreign adversaries will use deepfakes to spread disinformation and interfere in our election, which is why I have successfully secured language in the NDAA requiring notification be given to Congress if Russia or China seek to do exactly this.

But deepfakes has been and will be used to harm individual Americans. We have already seen instances of women's images being superimposed on fake pornographic videos. As these tools become more affordable and accessible, we can expect deepfakes to be used to influence financial markets, discredit dissidents, and even incite violence.

That is why I have introduced the first House bill to address this threat, the DEEPFAKES Accountability Act, which requires creators to label deepfakes as altered content, updates our identity theft statutes for digital impersonation, and requires cooperation between the government and private sector to develop detection technologies. I am now working on a second bill specifically to address how online platforms deal with deepfake content.

So, Dr. Donovan, cheap fakes. We have often talked about deepfakes where the technology footprint of the content has changed. But can you talk a bit more about the national security implications of cheap fakes, such as the Pelosi video, where footage is simply altered instead of entirely fabricated?

Dr. Donovan. One of the most effective political uses of a cheap fake is to draw attention and shift the entire media narrative towards a false claim. And so particularly what we saw last week with the Biden video was concerning because you have hundreds of newsrooms kick into gear to dispute something, a video, and platforms have allowed it to scale to a level where the public is curious and are looking for that content, and then are also coming into contact with other nefarious actors and networks.

Ms. Clarke. What would you say can be done by government to counteract the threat?

Dr. Donovan. There has to be -- I think you are moving very much in the direction I would go to where we need to have some labels, we need to understand the identity threat that it poses, and that there needs to be broader cooperation between governments.

As well I think that the cost to journalism is very high, because all of the energy and resources that go into tracking, mapping, and getting public information out there, I think the platform companies can do a much better job of preventing that harm up front by looking at content when it does seem to go wildly out of scale with the usual activity of an account and to proactively look at things where if you do see an uptick of 500,000 views on something maybe there needs to be proactive content moderation.

Ms. Clarke. Very well.

Ms. Bickert, Facebook is a founding member of the deepfake technology challenge, but detection is only partially a technology issue. We also need to have a definition of what fake is and a policy for which kind of fake videos are actually acceptable.

Last summer you informed Congress that Facebook is working on a precise definition for what constitutes a deepfake. Can you update us on those efforts,

especially in light of your announcement yesterday? And specifically how do you intend to differentiate between legitimate deepfakes, such as those created by Hollywood for entertainment, and malicious ones?

Ms. Bickert. Thank you for the question.

The policy that we put out yesterday is designed to address the most sophisticated types of manipulated media, and this fits within the definition of what many academics would call deepfakes, so that we can remove it.

Now, beyond that, we do think it is useful to work with others in industry and civil society and academia to actually have common definitions so we are all talking about the same thing. And those are conversations that we have been a part of in the past 6 months. We will continue to be a part of those. And we are hoping that, working together with industry and other stakeholders, we will be able to come up with comprehensive definitions.

Ms. Clarke. Should the intent of the deepfake or rather its subject matter be the focus?

Ms. Bickert. I am sorry. Could you repeat that?

Ms. Clarke. Should the intent of the deepfake or the subject matter be the focus?

Ms. Bickert. From our standpoint it is often difficult to tell intent when we are talking about many different types of abuse, but also specifically with deepfakes for misinformation, and that is why if you look at our policy definition it doesn't focus on intent so much as what the effects would be on the viewer.

Ms. Clarke. Thank you very much. I yield back.

I thank you, Madam Chair, for allowing my participation today.

Ms. Schakowsky. [Presiding.] That concludes the questioning.

I have things I want to put into the record, and maybe the ranking member does as well. But I did want to make an ending comment, and I would welcome her to do the same if she wishes.

So we had a discussion that took us to the grocery store, but we are now in a new world that we are discussing that is hugely bigger when we talk about Facebook. And as you say in your testimony, Facebook is a community of more than 2 billion people spanning countries, cultures, and languages across the globe.

But I think that there is now such an incredible and justified distrust of how we are being protected. We know in the physical world we do have laws that apply and that expectations of consumers are that those will be somehow there to protect us. But in fact they aren't.

We live then in the virtual world and the digital world in a place of self-regulation. And it seems to me that that has not satisfied expectations of consumers correctly. And we don't have institutions right now, even when they have the authorities, have the funding, have the expertise, I am thinking of the Federal Trade Commission just as an example, to do what it needs to do.

But we don't have a regulatory framework at all that I think, hopefully in a bipartisan way, we can think about. And it may include things like just the kinds of audits that you were talking about, Mr. Harris, which would not necessarily create new regulatory laws, but may, but we may need to.

And to me, that is the big takeaway today. When you have communities that are bigger than any country in the entire world that are essentially making decisions for all of the rest of us, and we know that we have been victimized, that the Government of the United States of America does need to respond. That is my takeaway from this hearing.

And I would appreciate hearing from the ranking member.

Mrs. Rodgers. I thank the chair, and I thank everyone for being here. I think it is important that we all become more educated.

I wanted to bring to everyone's attention that the FTC is holding a hearing on January 28 regarding voice cloning. I think that it is important that all of us are participating, becoming better educated, and helping make sure we are taking steps as we move forward.

Clearly, this is a new era, and on one hand we can celebrate that America has led the world in innovation and technology and improving our lives in many ways. There is also this other side that we need to be looking at and making sure that we are taking the appropriate steps to keep people safe and secure.

So we will continue this important discussion and continue to become better educated. Today's hearing was a great part of that. Thank you, Chair.

Ms. Schakowsky. Thank you very much.

I would like to insert into the record the -- I seek unanimous consent to enter the following documents into the record. A letter from the SAG-AFTRA. A letter from R Street. A paper written by Jeffrey Westling of the R Street Institute. A report from the ATHAR Project on Facebook. And so I seek unanimous consent.

Without objection, so ordered.

[The information follows:]

******** COMMITTEE INSERT ********

Ms. Schakowsky. So let me thank all of our witnesses today. We had good participation from members despite the fact that there were other hearings going on.

I remind members that pursuant to committee rules they have 10 business days to submit additional questions for the record to be answered by the witnesses and hopefully in a reasonably short time. We hope that there will be prompt answers.

And at this time, the subcommittee is adjourned.

[Whereupon, at 1:00 p.m., the subcommittee was adjourned.]