HOLDING BIG TECH ACCOUNTABLE: LEGISLATION TO BUILD A SAFER INTERNET

HYBRID HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

DECEMBER 9, 2021

Serial No. 117–61

Published for the use of the Committee on Energy and Commerce

govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

56–895 PDF WASHINGTON : 2024

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
DIANA DEGETTE, Colorado
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
PAUL TONKO, New York
YVETTE D. CLARKE, New York
KURT SCHRADER, Oregon
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois, *Vice Chair*
NANETTE DIAZ BARRAGÁN, California
A. DONALD MCEACHIN, Virginia
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona
KATHLEEN M. RICE, New York
ANGIE CRAIG, Minnesota
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas

CATHY MCMORRIS RODGERS, Washington
Ranking Member
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida
JOHN R. CURTIS, Utah
DEBBBIE LESKO, Arizona
GREG PENCE, Indiana
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania
KELLY ARMSTRONG, North Dakota

PROFESSIONAL STAFF

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

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

JAN SCHAKOWSKY, Illinois
Chair

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

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

C O N T E N T S

[1] Legislation has been retained in committee files and also is available at https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114299.

---

[2] The information has been retained in committee files and also is available at https://docs.house.gov/meetings/IF/IF17/20211209/114299/HHRG-117-IF17-20211209-SD008.pdf.

[3] The witnesses did not answer submitted questions for the record by the time of publication.

HOLDING BIG TECH ACCOUNTABLE: LEGISLATION TO BUILD A SAFER INTERNET

THURSDAY, DECEMBER 9, 2021

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 11:34 a.m. in the John. D. Dingell Room, 2123 of the Rayburn House Office Building, and remotely via Cisco Webex online video conferencing, Hon. Jan Schakowsky, (chairwoman of the subcommittee) presiding.

Members present: Representatives Schakowsky, Rush, Castor, Trahan, McNerney, Clarke, Cárdenas, Dingell, Kelly, Soto, Rice, Craig, Fletcher, Pallone (ex officio); Bilirakis (subcommittee ranking member), Latta, Bucshon, Dunn, Pence, Lesko, Armstrong, and Rodgers (ex officio).

Also present: Representatives Burgess, Carter, Doyle, Duncan, Rochester, and Walberg.

Staff Present: Parul Desai, FCC Detailee; Katherine Durkin, Policy Coordinator, Waverly Gordon, Deputy Staff Director and General Counsel; Jessica Grandberry, Staff Assistant; Tiffany Guarascio, Staff Director; Ed Kaczmarski, Policy Analyst; Zach Kahan, Deputy Director Outreach and Member Service; Hank Kilgore, Policy Coordinator; Mackenzie Kuhl, Press Assistant; Jerry Leverich, Senior Counsel; David Miller, Counsel; Kaitlyn Peel, Digital Director; Chloe Rodriguez, Clerk; Andrew Souvall, Director of Communications, Outreach, and Member Services; Michele Viterise, Counsel; Michael Cameron, Minority Policy Analyst, Consumer Protection and Commerce, Energy, Environment; Emily King, Minority Member Services Director; Bijan Koohmaraie, Minority Chief Counsel; Tim Kurth, Minority Chief Counsel, Consumer Protection and Commerce; Brannon Rains, Minority Professional Staff Member, Consumer Protection and Commerce; and Michael Taggart, Minority Policy Director.

Ms. SCHAKOWSKY. The Subcommittee on Consumer Protection and Commerce will now come to order.

Today we will be holding a hearing entitled, "Holding Big Tech Accountable: Legislation to Build a Safer Internet."

Due to the COVID-19 pandemic, this hearing will—members can participate in today's hearing either in person or remotely, via online conference.

Meanwhile—excuse me, members are—participating in person must wear masks. Such members may remove their masks when they are under recognition and speaking from a microphone.

Staff and press who are present in the committee room must wear a mask at all times.

And for members who are participating remotely, your microphones will be set on mute for the purpose of eliminating inadvertent background noise. Members participating remotely will need to—you will need to unmute your microphones each time that you wish to speak. Please note that, once you are unmuted, anything that you may say in—will be available in Webex, and it could be heard over the loudspeaker. And the—and also the—in the committee room, and subject to being heard by the livestreaming and C-SPAN.

Since members are participating from different locations, the way we are going to order the members will be by seniority within the subcommittee.

Documents for the record can be sent to—I usually get that right, yes, there it is—Kaczmarski, there we go, sorry, Kaczmarski, at the email address that we have provided to the staff. And all documents will be entered into the record at the conclusion of the meeting.

We will begin at this point with opening statements of 5 minutes by the members, and the Chair now recognizes herself for 5 minutes.

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

Bottom line, the Internet is not living up to its promises.

At its birth in the previous century, the Internet promised more social connection, new communities and experiences, and more economic opportunity. But these benefits have come with very steep consequences and costs.

Today's Internet is harming our children, our society, and our democracy. Five years ago, at the age of thirteen, Anastasia Vlasova joined Instagram, which quickly flooded her accounts with images of perfect bodies and perfect lives. She soon was spending three hours a day on the app, and developed an eating disorder. Despite public outcry, recently, as recently as—reported as yesterday, it confirmed that Instagram is still promoting pro-anorexia accounts to teens. Ms. Vlasova actually did eventually quit using Instagram, but millions of children and teens remain powerless against the addictive and manipulative algorithms and ads.

On January 6th, DC police officer Michael Fanone was grabbed, beaten, and tased, all the while being called a traitor to his country. The deadly insurrection was, at least in part, coordinated on platforms like Facebook, and exacerbated by elevating the—and amplifying algorithms that were about election disinformation.

For too long, Big Tech has acted without any real accountability. Instead, they give us excuses and apologies. The time for self-regulation is over. Today we will be discussing a number of pieces of legislation that will build a safer Internet.

Last week I introduced the FTC Whistleblower Act with my colleague, Representative Trahan. This bill protects from retaliation

current and former employees who blow the whistle to the Federal Trade Commission from retailer—from retaliation, and it incentivizes the disclosure of unlawful activity. It is a critical step toward a more safe Internet.

The Algorithm's [sic] Justice and Online Platform Transparency Act from Representative Matsui prohibits algorithms from discriminating against certain consumers.

The KIDS Act, from Representatives Castor, Clarke, Trahan, and Wexton ban online practices that exploit young people.

The Social Media Data Act from Representative Trahan and Castor prohibit—provide transparency into how digital ads target consumers.

The bipartisan DETOUR Act from Representatives Blunt Rochester and Gonzalez prohibit large, online platforms from using "dark patterns" to trick consumers.

So we can, this subcommittee can create an Internet that is better, and safer, and makes sure that consumers are protected, that we protect our children, that is transparent, and holds bad actors accountable.

And with that I want to give a hearty welcome and a thank you to this wonderful panel that is here, including one, I guess, that is here remotely with us.

Thank you very much.

[The prepared statement of Ms. Schakowsky follows:]

PREPARED STATEMENT OF HON. JAN SCHAKOWSKY

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Consumer Protection and Commerce Chair Janice D. Schakowsky

Hearing on "Holding Big Tech Accountable: Legislation to Build a Safer Internet"

December 9, 2021

Bottom line, the internet is not living up to its promise. At its birth in the previous century, the internet promised more social connections, new communities and experiences, and more economic opportunities. But these benefits have come with steep costs. Today's internet is harming our children, our society, and our democracy.

Five years ago, at age 13, Anastasia Vlasova joined Instagram which quickly flooded her account with images of perfect bodies and perfect lives. She soon was spending three hours a day on the app and developed an eating disorder.

Despite public outcry, reporting yesterday confirmed that Instagram is still promoting pro-anorexia accounts to teens. Ms. Vlasova eventually quit using Instagram, but millions of children and teens remain powerless against its addictive and manipulative algorithms and ads.

On January 6th, DC Police officer Michael Fanone was grabbed, beaten, and tased—all while being called a traitor to his country. The deadly insurrection was coordinated on platforms like Facebook and exacerbated by election disinformation they amplified.

For too long Big Tech has acted without any real accountability. Instead, they give us apologies and denials. But the time for self-regulation is over!

Today, we discuss a number of proposals intended to build a safer internet. Last week I introduced the "FTC Whistleblower Act" with my colleague Representative Trahan.This bill protects from retaliation current and former employees who blow the whistle to the Federal Trade Commission, and it incentivizes the disclosure of unlawful activity.

It's a critical step forward to restore trust online. The "Algorithmic Justice and Online Platform Transparency Act" from Representative Matsui prohibits algorithms that discriminate against certain consumers.

The "KIDS Act" from Representatives Castor, Clarke, Trahan, and Wexton bans online practices that exploit young people.The "Social Media DATA Act" from Representatives Trahan and Castor provides transparency into how digital ads target consumers.

The bipartisan "DETOUR Act" from Representatives Blunt-Rochester and Gonzalez prohibits large online platforms from using "dark patterns" to trick consumers.

We can create an internet that is better and safer—an internet that protects our children, is transparent, and holds bad actors accountable.

Each of these proposals takes important steps toward that goal.

Thank you to the witnesses for joining us today.

Ms. SCHAKOWSKY. And the Chair now recognizes the ranking member, my friend, Mr. Bilirakis, for—ranking member of the subcommittee, for his 5 minutes of an opening statement.

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

Mr. BILIRAKIS. Thank you, Madam Chair. I appreciate it so very much. Good morning to everyone.

Ms. SCHAKOWSKY. Are you on?

Mr. BILIRAKIS. Yes, yes, I am.

Ms. SCHAKOWSKY. Pull it close.

Mr. BILIRAKIS. Yes, yes. I want to thank my colleagues for their interest to improve transparency and increase protection online.

There are a lot of initiatives under consideration today, and all of them raise issues that deserve our attention.

Legislation brought forth by my friend in the majority would require the FTC to issue new rules and regulations, and would grant the FTC with additional enforcement tools to reduce dark patterns, discriminatory algorithms, as you said, Madam Chair, harmful content directed at children. It would also grant new rights for consumers to take control of their data. I hope that means this is a precursor, and not a substitute—and we have discussed this with the chairperson—for passing a national privacy and data security law. That is the best and most comprehensive way Congress can protect our constituents through these means. That is my opinion.

I think many of the issues we will be discussing today can and should be a part of that larger privacy and data security discussion, and I sincerely hope my colleagues will join me in that effort. I will say to my fellow colleagues that my door is always open, and we have a great relationship with the chairperson. Please don't hesitate to come and talk to me, and give us some input on this particular issue.

Earlier last month, Republican Leader Rodgers released draft legislative language for the Control Our Data Act, or CODA, which would create one national standard for privacy and data security, establish clear rules of the road for businesses to be able to comply, and give every American equal data protections, regardless of the location of their home. I, for one, certainly want to see rules that are clear and easy to understand for my constituents, and I am sure you do, too.

I also want to assure that the FTC Bureau of Privacy that was included in our proposal has the appropriate staff and resources to enforce the national law.

I hope the panel agrees today that there are elements of all these bills that can be incorporated in some fashion in this framework to ensure we leave behind a legacy that will benefit every American. That is the goal.

We must also take seriously the threat from China, and moving forward on these two bills today is an important step towards holding them accountable.

The legislation before us will provide Americans with greater transparency into the application and websites they use online.

H.R. 3991, the TELL Act, led by Representative Duncan, would inform users if their information is stored in China, and whether

the information is acceptable by the CCP or a Chinese state-owned entity.

H.R. 4000, the Internet Application ID Act, led by Representative Kinzinger, would require websites and online users or distributors of mobile applications that are located in China are owned by the CCP to disclose that location or ownership to users.

Both bills are very reasonable, as far as I am concerned.

For those asking why we didn't invite a witness today in today's hearing that has ties to China to share their views, you should know we absolutely did. We used one of our witness slots to invite TikTok to testify. But unfortunately, it declined. They declined the invitation.

Madam Chair, I hope we can work together to invite them before the subcommittee in the near future, just as Senators Blumenthal and Blackburn did in the Senate. There were many questions left unanswered in that hearing in the Senate last month on the stewardship of their platform. And I am confident that the panel today could shed light on our shared concerns.

Thank you so very much for being here. There are very important matters our subcommittee is examining today, so I thank the Chair for holding this hearing again, and I thank the ranking member, the full ranking member, and to the witnesses again for being here today. We really appreciate it.

I look forward to your testimony on these bills, and other proposals we have publicly circulated for this committee's review, and I yield back. Thank you.

[The prepared statement of Mr. Bilirakis follows:]

PREPARED STATEMENT OF GUS BILIRAKIS

Opening Statement for Republican Leader Bilirakis

Subcommittee on Consumer Protection and Commerce

Legislative hearing on "Holding Big Tech Accountable: Legislation to Build a Safer Internet"

December 9th, 2021

As Prepared for Delivery

Good morning everyone.

I want to thank my colleagues for their interest to improve transparency and increase protections online. There are a lot of initiatives under consideration today, and all of them raise issues that deserve our attention.

Legislation brought forth by my friends in the Majority would require the FTC to issue new rules and regulations and would grant the FTC with additional enforcement tools to reduce dark patterns, discriminatory algorithms, harmful content directed at children, and would also grant new rights for consumers to take control of their data.

I hope that means this is a precursor and not a substitute for passing a national privacy and data security law. That is the best and most comprehensive way Congress can protect our constituents through these means. I think many of the issues we will be discussing today can and should be a part of that larger privacy and data security discussion, and I sincerely hope my colleagues will join me in that effort. I'll say to my fellow colleagues that my door is always open.

Earlier last month Republican Leader Rodgers released draft legislative language for the Control Our Data Act, or CODA, which would create one national standard for privacy and data security, establish clear rules of the road for businesses to be able to comply, and give every American equal data protections regardless of the location of their home. I for one certainly want to see rules that are clear and easy to understand for my constituents. I also want to assure that the FTC Bureau of Privacy that was included in our proposal has the appropriate staff and resources to enforce the national law.

I hope the panel agrees today that there are elements of all these bills that can be incorporated in some fashion in this framework to ensure we leave behind a legacy that will benefit every American.

We must also take seriously the threat from China, and moving forward on those two bills today is an important step towards holding them accountable. The legislation before us will provide Americans with greater transparency into the applications and websites they use online. H.R. 3991, the TELL Act led by Representative Duncan, would inform users if their information

is stored in China and whether the information is accessible by the CCP or a Chinese state-owned entity. H.R. 4000, the Internet Application I.D. Act, led by Representative Kinzinger, would require websites and online sellers or distributors of mobile applications that are located in China, or owned by the CCP, to disclose that location or ownership to users.

For those asking why we didn't invite a witness to today's hearing that has ties to China to share their views, you should know we did. We used one of our witness slots to invite TikTok to testify, but unfortunately they declined our invitation. Madam Chair, I hope we can work together to invite them before the subcommittee in the near future, just as Senators Blumenthal and Blackburn did in the Senate. There were many questions left unanswered from that hearing in the Senate last month on the stewardship of their platform and I am confident that the panel today can shed light on our shared concerns.

These are all very important matters our Subcommittee is examining today, so I thank the Chair for holding this hearing, and to the witnesses for being here. I look forward to your testimony on these bills and other proposals we have publicly circulated for this committee's review.

I yield back.

Ms. SCHAKOWSKY. Thank you, Mr. Bilirakis. And before I invite our—the chairman and ranking member of the committee for their opening statements, let me just say I am very excited and optimistic. We have had a real good history of working together in this subcommittee to get legislation not only introduced and passed.

And I know last week we also sent you something on—a proffer on a privacy bill. I—again, I am very confident that we are going to be able to work together and get that done.

And I agree with the urgency that you are projecting today, and share it with you, and look forward to moving ahead rapidly.

And now let me recognize the great Chair of this full committee, Frank Pallone, for his opening statement.

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

Mr. PALLONE. Thank you, Chairwoman Schakowsky. Today's hearing is the second of two hearings on legislative reforms to hold social media companies accountable.

And following last week's hearing examining possible reforms of Section 230 of the Communications Decency Act, today's panel will discuss consumer protection-focused legislation that aims to hold these companies accountable by enhancing transparency and promoting online safety.

So these legislative hearings come after years of repeated bipartisan calls for online platforms to change their ways. Unfortunately, instead of meaningfully addressing the serious harms that these platforms can inflict on the American people and our children, social media companies continue to make minor changes only after negative press coverage, or in preparation for an executive testifying before Congress, and they also refuse to become more transparent.

In fact, we only actually learn what is really going on inside these massive corporations when a whistleblower steps forward, and those courageous actions are becoming exceedingly difficult. And even more disturbing, we are now seeing instances where these platforms are publicly shutting down efforts at transparency.

So since these companies are clearly not going to change on their own, Congress has to act. And today we will discuss seven bills that target different parts of the social media ecosystem to make platforms safer for users.

And one of the best ways to make these companies more accountable is to make them more transparent. We will discuss legislation that grants academic researchers and the Federal Trade Commission access to ad libraries, which will help to get us the data we need on how these companies are targeting users.

Another bill will prohibit the use of algorithms that discriminate based on race, age, gender, ability, and other protected characteristics, or methods that manipulate users into providing consent when they wouldn't, otherwise. And this legislation will help prevent people using social media from losing rights protected under the law.

We are considering a bill that will protect whistleblowers like former Facebook employee Frances Haugen, who testified at last week's legislative hearing. Whistleblowers help bring truth to light,

and are another way of helping ensure that companies are held accountable.

And finally, we will examine how to better protect our children online by banning certain design features directed at children, and prohibiting the amplification of harmful content that is targeted at them. Legislative measures that protect our children are critically important, and have bipartisan support on this committee.

Now, Republicans and Democrats also agree that we do not want to see our data or our children's data surveilled or used in a manner that could risk their safety. And that is why we are also discussing bills that attempt to force websites and apps to be transparent about their interactions with China. We all understand the danger the Chinese Government poses to the United States economy and national security, and we must take meaningful steps to address that danger from China.

After multiple hearings, letters, and discussions with stakeholders, the members of this committee have developed legislation to address the harms caused by Big Tech. There is no silver bullet to fix the Internet. The proposals that we are discussing today are important steps to improving the online ecosystem.

Another part of tech accountability is protecting people's privacy, and the chairwoman already mentioned that, significantly, because she is so much involved with it. But I think every member of this committee agrees that more must be done on privacy. And that is why we have been working since last Congress on a bipartisan staff discussion draft. Updates to that draft were made last week to address stakeholder feedback, and have been shared with the minority.

I continue to believe that there is a bipartisan path forward on privacy, and our work continues to get there. But today we are focused on proposals to make these platforms more transparent and safer.

So I just thank the witnesses, and thank Chairwoman Schakowsky for being out front on so many of these issues, particularly the privacy issue, which I know is not an easy one, but you are determined. And I yield back.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Committee on Energy and Commerce

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

Hearing on "Holding Big Tech Accountable: Legislation to Build a Safer Internet"

December 9, 2021

Today's hearing is the second of two hearings on legislative reforms to hold social media companies accountable. Following last week's hearing examining possible reforms to Section 230 of the Communications Decency Act, today's panel will discuss consumer protection-focused legislation that aims to hold these companies accountable by enhancing transparency and promoting online safety.

These legislative hearings come after years of repeated, bipartisan calls for online platforms to change their ways.

Unfortunately, instead of meaningfully addressing the serious harms that these platforms can inflict on the American people and our children, social media companies continue to make minor changes only after negative press coverage or in preparation for an executive testifying before Congress.

They also refuse to become more transparent. In fact, we only actually learn what is really going on inside these massive corporations when a whistleblower steps forward, and those courageous actions are becoming exceedingly difficult. Even more disturbing, we are now seeing instances where these platforms are publicly shutting down efforts at transparency.

Since these companies are clearly not going to change on their own – Congress must act. Today, we will discuss seven bills that target different parts of the social media ecosystem to make platforms safer for users.

One of the best ways to make these companies more accountable is to make them more transparent. We will discuss legislation that grants academic researchers and the Federal Trade Commission (FTC) access to ad libraries which will help us get the data we need on how these companies are targeting users. Another bill will prohibit the use of algorithms that discriminate based on race, age, gender, ability, and other protected characteristics or methods that manipulate users into providing consent when they wouldn't otherwise. This legislation will help prevent people using social media from losing rights protected under the law.

We're considering a bill that will protect whistleblowers, like former Facebook employee Frances Haugen who testified at last week's legislative hearing. Whistleblowers help bring truth to light and are another way of helping ensure that companies are held accountable. Finally,

we'll examine how to better protect our children online by banning certain design features directed at children and prohibiting the amplification of harmful content that is targeted at them. Legislative measures that protect our children are critically important and have bipartisan support on this committee.

Republicans and Democrats also agree that we do not want to see our data or our children's data surveilled or used in a manner that could risk our safety. That is why we are also discussing bills that attempt to force websites and apps to be transparent about their interactions with China. We all understand the danger the Chinese government poses to the U.S. economy and national security, and we must take meaningful steps to address that danger.

After multiple hearings, letters, and discussions with stakeholders, the members of this Committee have developed legislation to address the harms caused by Big Tech. There is no silver bullet to "fix the Internet." The proposals that we are discussing today are important steps to improving the online ecosystem.

Another part of tech accountability is protecting people's privacy. I think every member of this Committee agrees that more must be done on privacy, and that's why we have been working since last Congress on a bipartisan staff discussion draft. Updates to that draft were made last week to address stakeholder feedback and have been shared with the Minority. I continue to believe that there is a bipartisan path forward on privacy and our work continues to get there, but today we are focused on proposals to make these platforms more transparent and safer.

I thank the witnesses for their testimony and look forward to the discussion.

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

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

Mrs. RODGERS. Thank you, Madam Chair. And to our witnesses, thank you for being here.

Last week we discussed many examples of Big Tech companies failing to be good stewards of their platforms. Big Tech has used its power to censor Americans, control what we see, manipulate us through the use of harmful algorithms. Big Tech must be held accountable, and that is why, from day one of this Congress, Republicans have been exploring legislative solutions through our Big Tech accountability platform.

As a part of our platform, we released a number of proposals to focus on content moderation, transparency, and protecting our kids online, all issues that are relevant to today's hearing.

My proposal, which I am leading alongside my good friend, Congressman Jim Jordan, narrowly amends Section 230 to protect free speech. Under our proposal, Big Tech will be held accountable for censoring constitutionally-protected speech. Big Tech will no longer be able to exploit the ambiguity and the discretion we see in the current law. Big Tech will be more responsible for content they choose to amplify, promote, or suggest. Big Tech will be forced to be transparent about their content decisions, and conservatives will be empowered to challenge Big Tech's censorship decisions.

Republican policies would hold Big Tech accountable for their content moderation practices, and encourage transparency on enforcement decisions, especially when it comes to illegal drugs, counterfeit, and stolen products, terrorism, doxing, child pornography and trafficking, cyberbullying, and revenge porn.

We are also looking for new ways to improve cooperation with law enforcement, while upholding our civil liberties.

I am pleased to see some of these ideas presented today in the package that the Democrats are leading on. It is unfortunate that the majority decided not to use this hearing to discuss privacy, given many of these bills include provisions directly related to the collection and use of data, and would best be addressed in the context of a comprehensive privacy and data security framework.

The proposals also include language on protecting data from wrongful purposes, other references to the Child Online Privacy Protection Act, COPPA, and a data portability provision.

Despite our interest in continuing our work from last Congress on a bipartisan privacy framework, we have yet to have a hearing, let alone a markup. And Americans are desperate for our privacy and data security bill. It is difficult to address the goals discussed today without that national privacy framework and the data security bill. We will continue to talk. We can continue to talk, but we need a national privacy and data security bill.

Worse yet, the Democrats' tax-and-spending spree, the reconciliation package before the Senate right now, includes dramatic increases for funding and authority for the Federal Trade Commis-

sion, the FTC, that never received a bipartisan consensus. The majority suggested that this is a way to protect America's personal data. It couldn't be further from the truth. It includes no privacy and data security framework to implement or enforce.

These bills will add to the confusion in the marketplace by creating conflicting rules on how data is used, collected, and shared. This confusion only allows Big Tech to become more powerful, and it harms small businesses.

The question I have today is how do these bills fit into a comprehensive privacy and data security framework, like some of the proposals that the Republicans have released publicly?

Let me also share another reason that I am concerned, which I think we all agree on, and that is the need for a national standard because of Big Tech's troubling relationship that is being more exposed with the Chinese Communist Party. Big Tech has not been responsible with the data that they have collected, or who they share it with.

I am pleased and I am grateful that the majority included two bills, related bills, in the hearing today to help address that threat, one by Mr. Duncan and one by Mr. Kinzinger.

Big Tech companies like TikTok have an incredible amount of access and control over our data and information supply chain. Americans deserve to know if their personal information is safe, and to what extent it is being accessed by the CCP. It is our duty to uphold American values like free speech, and ensure that the United States of America continues to lead the cutting-edge technology to beat China. That starts by establishing a national privacy and data security framework and holding Big Tech accountable.

I look forward to hearing from the witnesses today.

[The prepared statement of Mrs. McMorris Rodgers follows:]

PREPARED STATEMENT OF HON. CATHY MCMORRIS RODGERS

Opening Statement of Republican Leader Cathy McMorris Rodgers
Subcommittee on Commerce and Consumer Protection
"Holding Big Tech Accountable: Legislation to Build a Safer Internet"
December 9, 2021
As Prepared for Delivery

Thank you, Madam Chair, and to our witnesses.

Last week we discussed many examples of Big Tech companies failing to be good stewards of their platforms. Big Tech has used their power to censor Americans, control what we see, and manipulate us through the use of harmful algorithms.

Big Tech must be held accountable. That is why from day one of this Congress, Republicans have been exploring legislative solutions through our Big Tech Accountability Platform. As part of our Platform, we released a number of proposals to focus on content moderation, transparency, and protecting our kids online all issues that are relevant to today's hearing.

My proposal—which I am leading alongside my good friend Congressman Jim Jordan – narrowly amends Section 230 to protect free speech.Under our proposal:

- Big Tech will be held accountable for censoring constitutionally protected speech.
- Big Tech will no longer be able to exploit the ambiguity and discretion we see in the current law;
- Big Tech will be more responsible for content they choose to amplify, promote, or suggest;
- Big Tech will be forced to be transparent about their content decisions; and
- Conservatives will be empowered to challenge Big Tech's censorship decisions.

Republican policies would hold Big Tech accountable for their content moderation practices and encourage transparency on enforcement decisions, especially when it comes to illegal drugs, counterfeit and stolen products, terrorism, doxing, child pornography and trafficking, cyberbullying and revenge porn.

We are also looking at new ways to improve cooperation with law enforcement while upholding our civil liberties.

Some of the ideas presented in the Democrat-led bills on today's agenda do merit consideration. It is unfortunate, however, that the majority decided not to use this hearing to discuss privacy, given many of their bills include provisions directly related to the collection and use of data, and would be best addressed in the context of a comprehensive privacy and data security framework.

The proposals also include language on protecting data from wrongful purposes, other references to the Child Online Privacy Protection Act (COPPA) and a data portability provision. Despite our interest in continuing our work from last Congress on bipartisan privacy discussions, we have yet to have a hearing - let alone a markup - this year on something the American people desperately need and deserve.

How can we expect to achieve the goals discussed today when we continue to drag our feet? When we continue to talk, but never deliver on a national privacy and data security bill? Worse still, the Democrats tax and spending spree includes dramatic increases for funding and authority for the Federal Trade Commission (FTC) that never received bipartisan consensus.

The majority sold this as a way to protect Americans' personal data. This couldn't be further from the truth. It includes no privacy and data security framework to implement or enforce. These bills will add to the confusion in the marketplace by creating conflicting rules on how data is used, collected, and shared.

This confusion will only help Big Tech become more powerful and harm small businesses. The question I have to my Democrat colleagues is how would your bills fit into a comprehensive privacy and data security framework like the proposal Republicans released publicly in the absence of a comprehensive strategy from the majority?

Let me share another reason—which I'm sure we can all agree on—for why we need a national standard: Big Tech's troubling relationship with the Chinese Communist Party (CCP). Big Tech has not been responsible with the personal data they collect or who they share it with.

I am pleased that the majority included two related bills in the hearing today to help address this threat—one by Mr. Duncan and one by Mr. Kinzinger. Big Tech companies – like TikTok – have an incredible amount of access and control over our data and the information supply chain. Americans deserve to know if their personal information is safe, and to what extent it is being accessible by the CCP.

It is our duty to uphold American values like free speech and ensure the U.S. continues to lead in cutting edge technology to beat China. That starts by establishing a national privacy and data security framework and holding Big Tech accountable. I look forward to hearing from the witnesses today and I yield back.

Mrs. RODGERS. I yield back, Madam Chair.
Ms. SCHAKOWSKY. The gentle lady yields back.

And I want to remind all members of the subcommittee that, pursuant to committee rules, all members' written opening statements shall be included and made part of the record.

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

Jonathan Greenblatt is the CEO and national director for the Anti-Defamation League.

Nathalie—let's see, I am going to get it—Marshall, no, Marechal—is the senior policy and partnership manager at Ranking Digital Rights.

Rich Lane—Rick Lane is the CEO of Iggy Ventures.

Josh Golin is the executive director of Fair Play.

And Jessica Richard [sic] of counsel at—what is it, Kelley Drye, got that right? OK.

And Imran Ahmed is the CEO of the Center for Counter-Digital—Countering Digital Hate.

At the—I just want to explain the—I will recognize each of you for 5 minutes, but I want to explain the lights that are in front of you, just to make sure that you know.

When the—when your time begins, the light will be green. When there is one minute left, there will be a yellow light. And I hope at that point you will start wrapping up, so that we can keep to, as close as we can, to 5 minutes.

And we will begin now with Mr. Greenblatt.

You are now recognized for 5 minutes.

STATEMENT OF JONATHAN GREENBLATT, CEO AND NATIONAL DIRECTOR, ANTI-DEFAMATION LEAGUE; NATHALIE MARECHAL, PH.D., SENIOR POLICY AND PARTNERSHIPS MANAGER, RANKING DIGITAL RIGHTS; RICK LANE, CEO, IGGY VENTURES LLC; JOSH GOLIN, EXECUTIVE DIRECTOR, FAIRPLAY; JESSICA RICH, OF COUNSEL, KELLEY DRYE, FORMER DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; AND IMRAN AHMED, CEO, CENTER FOR COUNTERING DIGITAL HATE

STATEMENT OF JONATHAN GREENBLATT

Mr. GREENBLATT. Thank you, Madam Chair Schakowsky, Ranking Member Bilirakis, and members of the subcommittee. Good morning. It is a privilege and an honor for me to be here today.

ADL is the oldest anti-hate group in America. We have been fighting anti-Semitism and all forms of bigotry for more than 100 years, and we have been tracking online hate since the days of dial-up. This work includes partnering with law enforcement to help prevent online threats from mutating into offline incidents. We work with authorities at all levels. In the past 11 months, we have provided the FBI with more than 1,000 actionable tips. Our 25 offices across the country engage directly with individuals and institutions affected by hate.

In 2017 ADL launched the Center for Technology and Society to double down on our efforts to fight online hate. We were the first civil rights group with an operation right in the heart of Silicon Valley, and it is staffed not by longtime non-profit professionals, but by software engineers, product managers, data scientists, and

computer experts, all hired from industry. We conduct analysis, publish research, build technology, and provide recommendations to policymakers like yourselves and industry leaders.

Today there is no distinction between online and offline lives. When we say that Facebook is the front line in fighting hate, I mean that, literally. We have seen over and over again the way that hateful content online leads to violence in our communities offline. Poway, El Paso, Pittsburgh, these targeted mass shootings were motivated by extremist conspiracy theories that were spawned and spread on social media.

In addition to these tragedies, online hate affects the everyday lives of millions of Americans. Our research has found that 41 percent of users report experiencing online hate and harassment. According to ADL's most recent analysis, 75 percent of those harassed report that it happened to them on Facebook. That is nearly three times the percentage on any other platform.

And make no mistake, all of them are highly profitable companies. So this isn't a resource problem, it is a responsibility problem.

Just today, ADL released new research demonstrating how easy it is to find White supremacist, accelerationist content on Instagram, less than 24 hours after the CEO sat at another table just like this, and said they were cleaning up their mess.

But these platforms lack and neglect safety because, first and foremost, they are exempt from liability, due to the loophole of Section 230. Now, I know that isn't the topic of today's hearing, but make no mistake, Section 230 must be changed to force the companies to play by the same rules that every other media company on the landscape operates by today.

It is just not a matter of free speech. It is simply being held accountable in courts of law, when the platforms aid and abet unlawful, even lethal conduct in service of their growth and revenue.

Tech companies are complicit in the hate and violence on their platforms because, if it bleeds, it leads, and it feeds their business model and their bottom line. Hate speech, conspiracy theories, they are amplified by the algorithms, nudged to the top of their news feeds, and they addict users like a narcotic driving engagement, which, in turn, increases their profits.

With no oversight and no incentives beyond increasing revenue, tech companies will continue to do whatever they can, whatever it takes to optimize engagement, regardless of the consequences. This just can't continue.

If not for courageous whistleblowers like Frances Haugen, we wouldn't have the hard evidence to prove that Facebook knowingly—knowingly—is mainstreaming extremism, inciting violence through its algorithms and fracturing societies around the world.

What if other tech companies, tech employees felt empowered and protected to expose wrongdoing when they saw it? That is why the protections, Congresswoman Schakowsky, in your FTC Whistleblower Act are so crucial.

If platforms have no meaningful motivation to fix the harmful algorithms that amplify hate, they won't do it. That is why the Algorithmic Justice and Online Transparency Act that would protect consumers from harmful and discriminatory AI systems are really long overdue, so we applaud that legislation, as well.

Finally, to stay ahead of the curve, we have got to prioritize research. In August, ADL Belfer fellow and NYU Professor Laura Edelson was de-platformed on Facebook hours after the company realized that she and her team were studying the role that Facebook may have played in leading up to the January 6th insurrection. Platforms should not be able to thwart important third-party research at their whim. Bills like the Social Media Data Act would ensure that academics can study platforms to better inform the public.

Look, there are no silver bullets. There is no one-size-fits-all solution to repairing our internet, but there is a lot you can do right now to take action. I have highlighted three bills, and I am happy to talk about them and others in the Q and A.

But members of the committee, let me conclude by urging you to remember that what happens online has a real impact on our lives. The status quo directly threatens our kids, our communities, and our country. Now is the time for you to legislate and act.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Greenblatt follows:]

Congressional Testimony

Holding Big Tech Accountable: Legislation to Build a Safer Internet

Jonathan Greenblatt

CEO

ADL (Anti-Defamation League)

HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

Washington, DC

December 9, 2021

10:30 a.m.

Working to stop the defamation of the
Jewish people and to secure
Justice and fair treatment to all since 1913

I. INTRODUCTION

During the past several years, there has been a tectonic shift in the way communities across the world integrate digital and social networks into their daily lives. Whether related to education, worship, family gatherings, social entertainment, or news, the online world is integral to our way of life. The way news and current events reverberate online matters. For ADL, the spread of conspiracy theories and hate online, often leading to on the ground violence, has been shocking but not surprising. We're seeing what used to be fringe extremist and bigoted narratives become normalized and mainstreamed. Americans have increasingly become radicalized and incited to action by the nonstop drumbeat of online hate and conspiracy theories. This is in large part because of social media's toxic business model that favors growth and engagement over public safety. No industry has ever exercised the sheer power and control over how the world communicates than social media platforms do now.

Social media's amplification of extremism, disinformation, and conspiracy theories—and the complete lack of transparency and accountability about how that amplification takes place—poses one of the greatest threats to democracy in this country, and to the safety of vulnerable individuals and communities worldwide. Hatred spread online has resulted in deadly violence in this country: from Charleston to Charlottesville to Pittsburgh, to Poway and El Paso, we have seen the fatal consequences of white supremacist extremism that often has a clear nexus to social media. We cannot afford to understate the damage from social media's algorithmic amplification of misinformation and hate, and the complete lack of accountability even when platforms aid and abet unlawful activity. We need a bipartisan, "whole of government approach"—indeed, a "whole of society approach"—to interrupt the contagion of hate spread by social media companies in their pursuit of profit. We need to finally hold Big Tech responsible for their role in fracturing democracy and inciting violence. Reform must be smart and effective. It must mitigate the unintended consequence of consolidating even more power, and ability to wreak harm, into the hands of a few impenetrable actors.

These billion-and trillion-dollar social media companies have the resources to improve systems, hire additional staff, develop better products, and provide real transparency. Yet they claim it is too burdensome. We know that's simply not true. Evidence from the tens of thousands of internal Facebook documents leaked by Facebook whistleblower Frances Haugen confirms it. Research from ADL's Center for Technology and Society confirms it. Still, without a clear understanding of what is really going on inside of these companies, we cannot begin to address the real danger posed to the public by letting platforms spread antisemitism, misinformation, and hate twenty-four hours a day, at lighting speed. And without changes to their incentive systems, social media companies will continue to operate under a business model that focuses on generating record profits at the expense of the safety of the public and the security of our republic.

ADL brings unique expertise to the table in the fight against this cycle of hate online. Our Center on Extremism examines the ways extremists across the ideological spectrum exploit the online ecosystem to spread their messages, recruit adherents, finance hate, and commit acts of terrorism. We work directly with threatened communities on the ground as well as law enforcement agencies across the country. This year alone, the Center on Extremism assisted law

enforcement over 1100 times in connection with issues related to violent extremists, and helped several community institutions prevent attacks, both online and off. Our Silicon Valley-based Center for Technology and Society, which has deep policy and technical product expertise, generates research and advocacy-focused solutions to make digital spaces safer and more equitable. CTS engages directly and regularly with major social media platforms to push for policy and product changes; and this has made measurable differences in fighting online extremism. ADL's Education team provides resources for schools and parents to teach children to counter extremist recruitment. And our International Affairs Department monitors how cyberhate in other countries and other languages impacts threatened communities around the world, including vulnerable Jewish communities.

Our expertise in these spaces, presence on the ground in communities across the country, and roots in one of the most targeted communities—combined with more than a century of work fighting against hate and for civil rights—informs ADL's analysis of the online hate and extremism ecosystem and what we can do to combat it.

This testimony will explore how platforms spread hate and extremism. It will show the link between hate-filled extremist content and user engagement, and will explore how and why this content becomes favored by platforms. While we will never eradicate hate and extremism, as this testimony addresses, lawmakers can act meaningfully and significantly to push hate and extremism back to the fringes of the digital world.

II. ADL'S FIGHT AGAINST ONLINE HATE

Since 1913, the mission of ADL (the Anti-Defamation League) has been to "stop the defamation of the Jewish people and to secure justice and fair treatment to all." One of the most important ways in which ADL has fought against bigotry and antisemitism has been by investigating extremist threats across the ideological spectrum, including from white supremacists and other far-right violent extremists, which have posed the biggest domestic terrorism threat to this country over the past decade.

Since its inception over a century ago, ADL has been the leading organization fighting hate. As we have said time and time again, where people go, hate follows—including online. That is why, in the early days of dial-up, ADL anticipated the ways in which hate speech could poison the internet and made certain we were investing our time and resources to communicate to the key players in the industry the need for clear and understandable terms of service on hate speech and encouraged them to enforce these policies aggressively. In 2017, we doubled down on our efforts and launched the Center for Technology and Society (CTS). CTS is a leader in the global fight against online hate and harassment. In a world riddled with antisemitism, bigotry, and extremism, ADL has worked with the tech industry and elected leaders to promote best practices that can effectively address and counter these threats.

ADL has become a leader in fighting online hate and disinformation. CTS acts as a fierce advocate for making digital spaces safe, respectful, and equitable for all people. We have created product interventions to slow down or stop viral hate, and have launched our own Artificial Intelligence tool to measure hate on social media platforms and evaluate policy enforcement. We

are also deeply committed to working in coalition in order to build a more equitable internet. In 2020, ADL teamed up with the NAACP, Color of Change, LULAC, Common Sense Media and other partners to launch Stop Hate for Profit, a campaign targeting Facebook because of the hate, racism, and misinformation reverberating across its platform. Joining the Stop Hate for Profit campaign, over a thousand companies worldwide pulled their advertising spends on the platform for a month, and celebrities and sports stars staged an Instagram walkout.

CTS also plays a unique role among civil society organizations working on fighting online hate in five key areas: policy, research, advocacy, incident response, and product development. It recommends policy and product interventions to elected officials and technology companies to mitigate online hate and harassment; drives advocacy efforts to hold platforms accountable and push hate back to the peripheries of society; produces data-driven applied research by analysts and a network of fellows; sheds new light on the nature and impact of hate and harassment on vulnerable and marginalized communities; brings to market technical tools and products that meet the crucial need for independent data measurement and analysis to track identity-based online hate and harassment; and empowers targets of harassment by responding to online incidents and pushing platforms to create safer online spaces for all. Our combination of technical and policy expertise—and decades of lived experience embedded in a community that has been targeted, often lethally, by bigots and extremists—informs our approach to fighting online hate, protecting targets of online harassment, and holding platforms accountable.

III. PLATFORMS SPREAD HATE AND EXTREMISM

There is no question that the prevalence and impact of online extremism is growing. The spread of QAnon and its consistent elevation of antisemitism, the mainstreaming of the foundational white supremacist "Replacement Theory," #StoptheSteal, and COVID conspiracies all are examples of extremism and hate that have become increasingly normalized and mainstreamed—in large part because of their viral spread online. Last fall, for example, a single "Stop the Steal" Facebook group gained more than 300,000 members within 24 hours. Thousands of new members joined this group by the minute and some of them openly advocated for civil war.

Discovery in civil cases, like the lawsuit against the neo-Nazi and white supremacist organizers of the 2017 Unite the Right rally in Charlottesville, which recently resulted in a $25M+ verdict for nine people injured during the rally, provide still more chilling examples. Extremists' online presence has reverberated across a range of social media platforms. This content is intertwined with hate, white supremacy, racism, antisemitism, and misogyny—all through the lens of extreme ideologies. Such content is enmeshed in conspiracy theories and explodes on platforms that are themselves tuned to spread disinformation.

We need to look no further than the deadly insurrection at our Capitol, which ADL has repeatedly called the most predictable terror incident in American history because it was planned and promoted out in the open on mainstream platforms such as Facebook, Twitter, Instagram, YouTube, and Reddit as well as fringe platforms such as Parler, Gab, 4Chan, and Telegram. As confirmed by leaked internal Facebook documents, the insurrectionists' actions were the product of weeks, months, and years of incitement, spread across the social media ecosystem that

services nearly 300 million people in the U.S. and billions around the world. This was an act of domestic terrorism that was plotted, publicized, recruited for, and financed online.

Finally, ADL considers the dramatic increase in cyberhate in recent years to be one major contributor to the domestic and international spike in antisemitic incidents in the physical world. This was especially the case during the brief war between Israel and the terrorist group Hamas this past May, which had a sharper uptick in on-the-ground antisemitic incidents targeting Jewish communities in America and around the world as compared to previous conflicts in the Middle East—such as in 2014 when Israel and Hamas fought a much more protracted war. The proliferation of antisemitism and other forms of hatred online threatens our communities around the world, including with increased physical attacks.

A. Hate and Extremism on Mainstream Social Media Platforms

Big Tech platforms are not unwitting accomplices or merely tools for bad actors to spread hateful, racist, extremist or conspiracy-related content. On the contrary, Big Tech companies know their platforms' product features are problematic and some have acknowledged it. At a congressional hearing in March 2021, former Twitter CEO Jack Dorsey admitted that his platform had "contributed to the spread of misinformation and the planning of the attack" on the U.S. Capitol on January 6, 2021. In the same hearing, however, Facebook's CEO Mark Zuckerberg disagreed with the assessment that Facebook had profited from the spread of disinformation and touted his platform's efforts to combat it.

Importantly, documents disclosed to the SEC by Facebook whistleblower Frances Haugen—who testified last week before the Communications and Technology Subcommittee for House Energy and Commerce—make clear that Facebook was aware of both the specific role its platform played in the insurrection and the broader role the platform plays in the spread of disinformation, extremism, and hate. The SEC disclosure includes statements from Facebook's internal documents. These documents acknowledged Facebook's role in augmenting "combustible election misinformation," noting "we amplify them and give them broader distribution." Internal Facebook documents also stated that the company had "evidence from a variety of sources that hate speech, divisive political speech, and misinformation on Facebook and the family of apps are affecting societies around the world . . . Our core products' mechanics, such as virality, recommendations, and optimizing for engagement, are a significant part of why these types of speech flourish."

Over the last few years, TikTok—a social media app that allows users to create and share short videos—has also hosted hate and extremism. As ADL's Center on Extremism (COE) documented in August 2020, while much of the content on TikTok is lighthearted and fun, extremists have exploited the platform to share hateful content and recruit new adherents. A recent review of the platform found that antisemitism continues to percolate across the app, including content from known antisemitic figures as well as posts perpetuating age-old antisemitic tropes and conspiracy theories. Earlier this year ADL's CTS released a report that

showed TikTok continues to be far too slow in taking down antisemitism reported by ordinary users and it still has plenty of work to do to ensure that hate is adequately remediated.

B. Gaming Platforms

Online video games share many of the attributes of social media platforms, including spreading hate and extremism. According to the Entertainment Software Association, there are approximately 227 million gamers in the United States. Gaming analytics firm NewZoo's global market report put the gaming industry's revenue at approximately $176 billion globally. With those figures in mind, the importance of addressing hate and extremism in gaming is critical.

ADL's 2021 study of hate, harassment, and positive social experiences in online games explored players' in-game exposure to topics such as extremism and disinformation. Alarmingly, 8 percent of adult gamers (18-45) and 10 percent of teen gamers (13-17) witnessed discussions about white supremacist ideology in online multiplayer games. Seventeen percent of adult gamers saw hateful messaging linking the COVID-19 pandemic to the Asian community, and 13 percent of adult gamers saw hateful anti-immigrant messages spread in online games. The survey also showed that nearly one-in-ten online multiplayer gamers (7 percent) come across Holocaust denial discussions while playing. As we continue to pay deeper attention to the impact social media's algorithms and business models have on hate and extremism, we must consider the way online video games have similar consequences.

C. Cyberhate around the World

Many of these problems are compounded when you broaden the aperture to look outside of America's borders or content in languages other than English. Facebook whistleblower Frances Haugen recently testified that an estimated 87 percent of Facebook's spending to address misinformation was on English-language content when only 9 percent of users are English speakers. For example, ADL recently identified 39 separate Arabic-language Facebook groups or pages with hundreds or thousands followers or likes that had titles specifically aimed at promoting The Protocols of the Elders of Zion, an infamously anti-Jewish hoax. In another recent ADL study, we found 25 Spanish-language antisemitic posts on Facebook that were from groups with a total of 666,728 followers and viewed 55,911 times.

Further, antisemitic content seems to be given even more of a free pass when it comes from foreign leaders or when it is couched in language that makes passing allusion to Israel or Zionists. In light of this, Twitter enables accounts that are attributed to major media outlets for U.S.-designated terrorist groups, such as Hamas, Hezbollah and Palestinian Islamic Jihad, to have a platform before thousands of followers. They use their accounts to glorify terrorism and spread absolutely horrendous antisemitic hate and conspiracies. Ayatollah Ali Khamenei, the Supreme Leader of Iran and the head of the number one state sponsor of antisemitism and terrorism in the world today, has well over a dozen current accounts on Twitter that he uses to

promote Hamas and Hezbollah terrorists and spread hateful antisemitic tropes across a broad array of world languages.

IV. HATE AND EXTREMISM ARE GOOD FOR PLATFORMS' BUSINESS MODELS

Big Tech's fundamental business model, targeted advertising, maximizes profits by keeping its users engaged on the platform for as long as possible to sell as many advertisements as possible. Platforms keep users engaged by optimizing product mechanics like how often and on which posts we click, share, like, and comment—whether in support, opposition, otherwise. Data from tracking user behavior is analyzed to build detailed advertising profiles and find as many opportunities as possible to serve users targeted ads. AI and algorithms, surveillance advertising, subscription models, and other product affordances work together to increase user engagement—positioning these companies as some of the most profitable businesses in the world. What is problematic, however, is that the goal of the platforms, and the algorithms they deploy as a result, is to exploit people's predilection for engaging with incendiary and controversial content and sharing misinformation and divisive material. This user behavior is core to the revenue model.

Hate speech, conspiracy theories, and misinformation—amplified and recommended by platform algorithms—put corrosive and false content at the tops of personalized news feeds, right next to pictures of our families and friends. As mentioned above and detailed below, platforms benefit from the existence and spread of this content because it drives their engagement metrics. It motivates users to spend as much time on the platform as possible, increasing the amount of data that can be extracted about users and, in turn, enabling platforms to serve more and more targeted advertising to users—ultimately increasing revenue. In this way, social media is the most successful extraction industry the world has ever known. When critics say that the existence and viral amplification of hate content and disinformation is a feature, not a bug, of social media platforms, this is what they mean. And until the incentives are changed, we cannot meaningfully mitigate the threat of mainstreamed hate and extremism.

A. Surveillance Advertising and Political Advertising

Like other industries, social media platforms profit from delivering advertisements to users. Tech platforms are distinct from other advertising-based businesses, however, because of the specific and unprecedented way these platforms collect data and target ads. As mentioned above, social media platforms are so successful because they collect and analyze enormous troves of user data based on user activity on the platforms and across the internet. As many experts have noted, Big Tech knows more about us than we know about ourselves.

User data is collected for two key purposes: first, to learn and constantly improve how to keep users engaged on platforms (e.g., viewing and interacting with content) for as long as possible, so that users see as many advertisements as possible; and second, to ensure that the advertisements the platforms deliver are highly targeted to users based on the huge volume of

information that platforms know about each users' behaviors, habits, and preferences (and that of their families and friends). Platforms use this data to develop highly specific advertiser-focused user segments. Then, algorithms deliver ads to specialized demographic segments through personalized content feeds.

While some user data is provided directly by users to platforms (e.g., age and location), social media companies also surveil users to gather extensive information from their profiles (e.g., friends/followers, contacts, connections, groups) as well as their online activity—both on the specific platform and across the internet. Platforms track "likes," shares, comments, navigation paths, hover time, watch time, purchases, and other user engagement actions. Some platforms also collect additional customer data from activities off the platform and combine it with their own data. This practice has been referred to as surveillance advertising, which is described as closely tracking and profiling individuals and groups in detail and then narrowly targeting ads at them based on behavioral history, relationships, and identity and the astounding predictive power that data offers. Surveillance advertising allows platforms to dominate the digital advertising market by offering both big and small businesses an extremely efficient and effective form of advertising—far more than other options such as newspaper or local TV advertising.

Surveillance advertising, which sometimes allows for microtargeting of sliced-and-diced demographic segments, can become even more problematic when used for political and "social issue" advertising. Political advertising often disseminates disinformation and fuels hate by narrowly targeting particular user segments and infuriating and activating them with outrageous, divisive content. Unlike a newspaper or TV spot, where everyone sees the same ad, these campaigns often fall under the radar and are not disclosed to users, researchers, or the public at large. Therefore, no one can meaningfully evaluate the harm of these targeted misinformation campaigns.

Misinformation is considered a key source of political advertising, according to Laura Edelson, ADL Belfer Fellow and PhD candidate in computer science at New York University. Edelson and her team have specifically focused on how misinformation spreads on Facebook. Facebook made promises to be transparent about all of the U.S. political ads on its platform—and about who paid for them. The platform, however, routinely misidentifies political ads and also fails to disclose important information about these ads. Facebook does not have humans overseeing every ad that is published on the platform—even though ads must be submitted for review. Instead, the company uses artificial intelligence (AI), including machine learning (ML) models, and also heavily relies on voluntary compliance. This makes it really easy for bad actors to slip through enforcement gaps. At the same time, biased AI systems can result in over-enforcing against (e.g., removing) legitimate ads. Alarmingly, Edelson and her colleagues have been able to demonstrate that extreme, unreliable news sources get more engagement on Facebook. This, in turn, has the doubled impact of increasing reach and, thus, becoming less expensive to bad-actor advertisers. Edelson and her colleagues also found that the archive of political ads that Facebook makes available to researchers is missing more than 100,000 ads.

As an ADL Belfer Fellow, Edelson is currently working to measure misinformation and hate speech aimed at U.S. Spanish-speaking and Asian American communities by analyzing political advertising on Facebook from the platform's Ad Library and from CrowdTangle, a research and data collection tool owned by Facebook. This research is part of a broader investigation into misinformation in political advertising on Facebook by Edelson and her team at NYU's Cybersecurity for Democracy project.

On August 3, 2021, Facebook placed an enormous obstacle in Edelson and her team's path when it suspended Edelson and her colleagues from accessing its data. The suspension occurred after Edelson and her colleagues started studying whether Facebook was contributing to vaccine hesitancy and sowing distrust in elections, and considered what role the platform may have played leading up to the January 6 insurrection. Facebook cited privacy concerns based, in part, on an FTC order. The federal agency itself disputed this concern publicly. In any case, the careful privacy protocols of the research, which only sought information about advertisers, clearly showed Facebook's ostensible justifications to be pretext. As ADL said at the time, one wonders what Facebook didn't want the public to know.

It's no surprise Facebook attempted to block Edelson's access to data seeking to uncover Facebook's role in the insurrection. According to reports, based on internal documents submitted to the SEC by the Facebook whistleblower, analysis of the January 6 insurrection illustrated that the company was fundamentally unprepared to manage the "Stop the Steal" movement, which turned violent and played a pivotal role in the insurrection. Facebook's own internal analysis found that the policies and procedures put in place were not strong enough to prevent the growth of groups related to "Stop the Steal." The report noted that Facebook treated each piece of "Stop the Steal" content individually, rather than as part of a greater whole. The result of this decision was that only some "Stop the Steal" content or groups were taken off the platform. Much of the content and many of the groups were left up and, ultimately, amplified by Facebook's own algorithms.

On September 28, 2021, Edelson testified before the House Science, Space, and Technology Committee's Investigations and Oversight Subcommittee. At the hearing, titled "The Disinformation Black Box: Researching Social Media Data," she spoke about the harms caused by misinformation on social media and the difficulties researchers face in trying to study this threat to the public. Platforms like Facebook provide independent researchers little access to advertising data, so it is difficult to understand the full impact of political and "social issue" advertising. We need more transparency about Facebook and other platforms' data collection, ad targeting, and algorithmic systems. As discussed in more detail below, proposals like the Social Media DATA Act would ensure academic researchers like Edelson have access to data related to the targeting of online digital advertisements in order to study discrimination, manipulation of youth, election interference, and other consumer harms. Additionally, proposals like the FTC Whistleblower Act of 2021 would ensure whistleblowers can safely disclose wrongdoing at social media companies, including when the companies make dangerous business decisions that harm consumers.

B. AI and Algorithms

AI and machine learning algorithms play a powerful role in the dissemination of extremism and online harm. As referenced in a report co-authored by ADL and other organizations fighting disinformation, "AI can be understood as machines that predict, automate, and optimize tasks in a manner that mimics human intelligence, while [machine learning] algorithms, a subset of AI, use statistics to identify patterns in data." Social media platforms use algorithms, largely fueled by AI and ML systems, to deliver, rank and moderate content, to determine what content should be recommended to a user, and to serve advertisements to users. Algorithms make these highly personalized decisions by collecting and synthesizing vast amounts of user data.

One primary reason algorithms amplify harmful online content on social media is that platforms optimize them for user engagement. They are tuned to keep eyeballs on the screen. Algorithms feed users tailored content based on factors including browsing activity. When a user interacts with a piece of content, algorithmic systems take note of the user's behavior to find and recommend similar content to the user. For example, if someone watches a video about an election, algorithmic systems will recognize that the user may be interested in political content and will continue to recommend related content. If someone has viewed or searches for hateful content, algorithms learn to serve the same user similar or more extreme content.

In addition to personalized recommendations, algorithmic systems focus on what pieces of content are likely to attract a wide range of users. Algorithms do this by recognizing signals—including which pieces of content are watched, shared, commented on, or replied to—and then combining those signals to show that content to more users almost immediately. These algorithms predict if the piece of content will increase engagement, and thus increase advertising revenue. Highly engaging topics such as extremism, hate, and conspiracies are known to generate engagement and thus drive profit. ADL has reported on research that controversial, hateful, and polarizing information and misinformation are often more engaging than other types of content and, therefore, receive wider circulation. Platforms' algorithmic tools significantly boosted extremist content, from white supremacist groups and Holocaust denial to COVID-19 hoaxes and misinformation. Platforms privilege and heavily promote this type of incendiary content to create a stimulus–response loop. In fact, reports of a Facebook researcher who explored how the social media platforms deepened political divides illustrated the speed with which platform algorithms get to work to recommend content rife with misinformation and extremism: less than a week.

The persistent presence and amplification of hate, bigotry, and conspiracy theories on social media platforms has created an environment for extremism to flourish. Today, extremists are enmeshed in online communities where content designed to increase their propensity for hatred and violence often circulates freely. Extremist content boomerangs from fringe websites to mainstream platforms—in part because of social media's immense power, amplification of "engaging" content, and sophisticated recommendation algorithms. However, extremism and hate that start on social media do not always stay there. This content has inspired individuals to commit acts of violence and domestic terrorism.

While an individual who naturally engages with innocuous content (e.g., cat videos, makeup tutorials, or music videos) may not be pushed toward extremist content, individuals who engage with political content, seek to understand conspiracy theories, or have existing gender/racial resentment can quickly become trapped in a negative feedback loop. For example, exposure to videos from extremist or white supremacist channels on YouTube remains disturbingly common. In February 2021, Brendan Nyhan, an ADL Belfer Fellow and professor at Dartmouth College, published a report that collected comprehensive behavioral data measuring YouTube video and recommendation exposure among a diverse group of survey participants. Using browser history and activity data, the report examined exposure to extremist and white supremacist YouTube channels as well as to "alternative" channels that can serve as gateways to more extreme forms of content. Though some high-profile channels were taken down by YouTube before the study period, approximately one in ten participants viewed at least one video from an extremist channel (9.2%) and approximately two in ten (22.1%) viewed at least one video from an alternative channel.

Moreover, the ADL/Nyhan study found that when participants watched the videos, they were more likely to see and follow recommendations to similar videos. Consumption was concentrated among a highly engaged subset of respondents. Among those who watched at least one video of a given type, the mean numbers of videos watched were 64.2 (alternative) and 11.5 (extremist). Moreover, consumption of these videos was most frequent among people with negative racial views.

Currently, platforms have no meaningful incentive to fix problematic algorithms and the public has little understanding of just how dangerous platforms' algorithms can be. As discussed in more detail below, proposals like the Algorithmic Justice and Online Platform Transparency Act, would prohibit discriminatory algorithmic processes, establish a safety standard for algorithms, and require increased transparency from platforms about the types of algorithmic processes they employ and the categories of information they collect to power their AI/ML tools.

C. Policymaking due to Public Relations Issues

As of 2021, almost every major social media platform has a stated public policy prohibiting extremism, terrorism, incitement-to-violence and hate on their platform. For instance, Facebook has a policy prohibiting dangerous individuals and organizations, while Twitter has a policy prohibiting violent organizations. The path to the creation and implementation of these policies, however, was not a direct one. Platforms are too often motivated not by harm prevention but, instead, by avoiding negative public perception. For example, despite repeated demands from ADL and civil society organizations to create a policy prohibiting white nationalism, Facebook only took action to implement a policy prohibiting white nationalist content following public outcry after the 2019 massacre of 51 Muslim people by a white supremacist in Christchurch, New Zealand. This is a pattern that repeats itself over and over again: Big Tech refuses or fails to take action in the face of repeated demands—by civil society, Congress, and their own employees and researchers—then a horrific tragedy occurs, and the companies apologize and pledge to do better. This inspires some action—usually a policy change—but lack of

enforcement, lack of transparency, lack of independent verification, and exceptions to policy changes make platform actions hollow and futile…and the cycle continues. This is the playbook.

For example, in June 2020, after deep frustration with the PR-first focus of policymaking by tech platforms, a number of civil society organizations (ADL, Color of Change, Common Sense, Free Press, LULAC, Mozilla, NAACP, National Hispanic Media Coalition, Sleeping Giants) formed the Stop Hate for Profit Coalition. The coalition called on businesses who ordinarily advertise on Facebook to engage in a month-long advertising pause. Over 1,200 companies joined the July 2020 pause. Additionally, Stop Hate for Profit had a September 2020 week of action, which involved celebrities and influencers calling out hate and extremism on Facebook. Content from the September week of action had an estimated 1 billion views. In January 2021, the Stop Hate for Profit Coalition asked Facebook, Twitter, Google, and other social media platforms to #BanTrumpSaveDemocracy by permanently removing Donald Trump from their platforms.

Policy changes long demanded by civil society around militia activity, the "boogaloo" movement, and Holocaust denial were finally made by Facebook following the Stop Hate for Profit Coalition's public pressure. The campaign's success clearly demonstrates the degree to which policymaking at social media companies is too frequently driven by attempts to shift public perception—only when the companies feel they have absolutely no other choice. Other platforms, also motivated by public pressure, took similar measures in the wake of Stop Hate for Profit. Twitter banned links to hateful content on their platform, which led to the deplatforming of noted white supremacist David Duke. Reddit—which has done a better, if still an incomplete job addressing hate online than many other big platforms—released its first ever hate policy and deplatformed R/TheDonald, a forum of 800,000 users known to house hate and conspiracy theories. YouTube banned six prominent white supremacists, including Stefan Molyneux, David Duke, and Richard Spencer.

Still, social media companies' reactive practices of creating policies for public relations purposes in response to tragic events remained in full effect following the attack on the U.S. Capitol on January 6, 2021. Despite Twitter's July 2020 policy against content related to the hateful QAnon conspiracy, ADL was able to find numerous examples of QAnon on Twitter following the attack on the Capitol. It was only after increased public pressure—in light of the nexus between QAnon and the January 6 attack—that Twitter took more decisive action. After the insurrection, Twitter removed 70,000 QAnon accounts, which greatly reduced the spread of this hateful conspiracy theory on the platform. In fact, ADL found that immediately following the suspension of QAnon-related accounts on January 8, the use of QAnon-related hashtags plummeted by 73 percent.

The actions taken by tech companies—both to update their policies to better prohibit hate and extremism and to better enforce their existing policies to remove such content from their platforms—were helpful but insufficient. The fact that it took such intense public pressure for platforms to create policy and enforcement improvements is unacceptable and, frankly,

dangerous. And we're still seeing lackluster enforcement of important policy changes. For example, ADL recently found that one year after Facebook banned Holocaust denial, the majority of violative posts still accessible were posted prior to the October 2020 ban, yet never subsequently removed. These posts are located in public and private groups as well as on personal profiles, and many contain links to external, explicit Holocaust denial sources. When viewed through the lens of social media companies as primarily optimizing their business models, and generating profit, the justification for public-relations-focused decision making and subpar policy enforcement is clear. This illustrates why self-regulation will never work to solve this pernicious issue. What is needed is the establishment of a set of clear disincentives that will discourage platforms from prioritizing profit over people's safety; put differently, platforms need incentives to make changes that will significantly diminish the amount, and impact, of hate and extremism on their platforms.

*D. **Product Features***

Social media platform policies are only one part of the equation when it comes to mitigating online hate and extremism. Platform products, like groups/pages, ad targeting tools, reporting systems, and other features, often interact to create an environment ripe for bad actors to exploit.

i. **Design Features**

Manipulative design features are one significant way platforms take advantage of consumers. In November, ADL introduced its Social Pattern Library, a collection of design principles and user experience patterns intended to mitigate hateful content on social media platforms developed collaboratively with leading user experience designers. We encourage platforms to consider this living resource as it provides codified product recommendations that will help break the cycle in which hateful content is amplified through algorithms or similar features. Efforts like the Deceptive Experiences to Online Users Reduction (DETOUR) Act recognize the dangers of dark patterns and must be considered when thinking about how to repair our internet.

ii. **Groups and Pages**

"Groups" is one Facebook product feature that may have had innocent origins, but for hate and extremist groups has been foundational to offline violence and domestic terrorism. Facebook claims that it is effectively addressing hate groups on its platforms. ADL and others, however, have continued to expose egregious examples of online hate, misinformation, and extremism across the company's products.

Perhaps most concerning, Facebook algorithms have recommended pages and groups connected to the "boogaloo" conspiracy theory to like-minded users long after the company's assertion last June that it would no longer do so. That assertion was followed by broader statements (in September 2020) that the platform would not recommend groups tied to violence, and an even broader March 2021 statement that Facebook would be ending all recommendations for "civic and political groups, as well as newly created groups." A recent review found that among groups sharing violent memes and a group simply named "Let's Overthrow the Government," Facebook

was recommending groups with names like "The Hawaiian Hootenanny," "Boogaloonia," and "The Chaplain of the Redacted." In addition, after one boogaloo page was "liked," our investigation's user received suggestions of other pages with similar content, showing how opportunities are created for users to get further steeped in the ideology.

And Facebook's own internal reports show that their recommendation systems are powerful ways to drive engagement and that small signals—even as small as a profile showing a woman in a southern state who liked Donald J. Trump and also Fox News, got recommendations for QAnon and other conspiracy groups within 48 hours of creating the profile, even with no other interactions on the site.

iii. Content Moderation and Reporting Systems

Today, most social media companies engage in content moderation to enforce content policies. These systems enforce the policies, sometimes called Community Guidelines or Terms of Service, that determine what content, individuals, and groups are permitted on their services. Beyond having clear and comprehensive policies (which many platforms do not), platforms also communicate with their users about content management decisions. Users deserve to know that platforms will thoughtfully review their reports, especially when reporting hateful, racist, or extremist content, and deserve timely and fair decisions from those systems. Generally, companies rely on a combination of human moderators and AI and ML-based tools to carry out their content moderation efforts, which include flagging, reviewing, making determinations about content and users, and appeals. Additionally, users report violative content to platforms. Importantly, across the industry, it is hard for users to trust that their reports are being addressed.

This year, CTS developed report cards on Holocaust denial and antisemitic platform content to determine the efficacy of platforms' reporting systems. Report cards have focused on a few different aspects of the reporting process. For ADL's Holocaust Denial Report Card, we assessed a platform's response time and whether the platform explained the reason for their decision. One noteworthy finding from this exercise is that platforms with explicit Holocaust denial policies did not necessarily do better enforcing those policies against our reported content, despite years of advocacy from civil society and researchers. Additionally, despite calls for greater transparency, another notable result is the opacity surrounding how platforms reported on the enforcement of their policies. The results of the investigation can be seen in the image below.

PLATFORM	EXPLICIT HOLOCAUST DENIAL POLICY?	GENERAL HATE POLICY?	EFFECTIVE PRODUCT LEVEL EFFORTS TO ADDRESS HOLOCAUST DENIAL?	RESPONSE WITHIN 24 HOURS?	NOTIFICATION OF POLICY REASON FOR ENFORCEMENT?	ACTION TAKEN AGAINST HOLOCAUST DENIAL?	GRADE
Twitch	Yes	Yes	Yes	Yes	No	Yes	B
Twitter	No	Yes	No	Yes	No	Yes	C
YouTube	Yes	Yes	Yes	No	No	No	C
TikTok	Yes	Yes	Yes	No	No	No	C
Roblox	Yes	Yes	Yes	No	No	No	C
Facebook (including Instagram)	Yes	Yes	No	Yes	No	No	D
Discord	No	Yes	No	Yes	No	No	D
Reddit	No	Yes	No	No	No	No	D
Steam	No	Yes	No	No	No	No	D

Note: In creating this framework for evaluating the efforts of digital social platforms, we weighted enforcement more heavily than policy and explicit policies more heavily than general policies. Additionally, because no platform had affirmative results in every category, we did not award any platform an "A."

Image: ADL Holocaust Denial Report Card

For ADL's Antisemitism Report Card, ADL investigators found that no platform performed above a B- in addressing antisemitic content reported to it. Also, no platform provided information or a policy rationale for why it did or did not remove flagged content. Facebook and TikTok got a "D" and "F" respectively when it came to data accessibility. The results of the investigation can be seen in the images below:

Online Antisemitism Report Card

PLATFORMS	HATE POLICY THAT EXPLICITLY MENTIONS RACE, RELIGION, OR ETHNICITY?	RESPONSE WITHIN 24-72 HOURS?	NOTIFICATION OF POLICY REASON FOR ENFORCEMENT?	ACTION TAKEN AGAINST A/S?	TRUSTED FLAGGER PROGRAM?	ACTIONED UPON TRUSTED FLAGGER REPORT?	EFFECTIVE PRODUCT-LEVEL EFFORTS TO ADDRESS ANTISEMITISM?	DATA ACCESSIBILITY GRADE	TOTAL GRADE
Twitter	Yes	Yes	No	No	Yes	Yes	Yes	B	B-
YouTube	Yes	No	No	Yes	Yes	No	Yes	C	B-
Reddit	Yes	No	No	No	No	N/A	Yes	B	C
Twitch	Yes	Yes	No	Yes	No	N/A	No	C	C
TikTok	Yes	No	No	No	Yes	Yes	Yes	F	C-
Facebook (including Instagram)	Yes	No	No	No	Yes	No	No	D	C-
Discord	Yes	Yes	No	No	No	N/A	No	C	C-
Roblox	Yes	No	No	No	No	N/A	No	D	D-

Image: ADL Antisemitism Report Card

Data Accessibility Report Card

PLATFORMS	PUBLIC API FOR PUBLIC CONTENT	RESEARCH/ NGO ACCESS TIER	REPORTING API	RETROACTIVE SEARCH FUNCTIONALITY	STREAMING SEARCH FUNCTIONALITY	RATE LIMITS	QUALITY DOCUMENTATION	GRADE
Twitter	Yes	Yes	No	Yes	Yes	High	Yes	B
Reddit	Yes	Yes	No	Yes	Yes	High	No	B
Discord	Yes	No	No	No	No	High	Yes	C
Twitch	Yes	No	Yes	No	No	High	Yes	C
YouTube	Yes	No	No	Yes	No	Low	Yes	C
Facebook/ Instagram	No	Yes	No	No	No	-	-	D
Roblox	Yes	No	No	Yes	Yes	-	No	D
TikTok	No	No	No	No	No	-	-	F

Image: ADL Antisemitism Report Card

Users deserve more transparency and greater protection from platforms than companies are inclined to provide. Such reluctance has consequences in the form of economic, emotional, mental, political, and physical abuses that affect many people's lives, as repeatedly shown in ADL's research. It is irresponsible at best, and deeply complicit and culpable at worst, for platforms to take, piecemeal approaches that do little to address the rapidity and depth of online hate and harassment.

V. POLICY RECOMMENDATIONS

We need a whole-of-government approach to address the hate and extremism on social media—especially because it can fracture democracy and lead to offline acts of hate-fueled violence. ADL calls for urgent action to prevent and counter domestic violent extremism.

ADL's Repair Plan

ADL has consistently stated that there is no single fix to the phenomenon of online hate. Whether it is in the dark corners of the internet, on the chats used by hundreds of millions of people on online multiplayer games, or a social media post that goes viral, the impact of online hate reverberates both on and offline. This is especially true for those targeted by extremists, who are disproportionately women and members of marginalized communities. The public agrees: according to 2021 ADL data, 77 percent of Americans think new laws are needed to hold social media platforms accountable for recommending that users join extremist groups. ADL's REPAIR Plan presents an integrated agenda to fight hate online and push hate, violence, and extremism back to the fringes of the digital world.

R Regulation and Reform

E Enforcement at Scale

P People Over Profit

A Access to Justice

I Interrupting Disinformation

R Research and Innovation

Congress has an important role in reducing the prevalence, impact and virality of online hate by holding social media companies accountable for their role in fomenting violence, racism, discrimination, and other harms.

Regulation and Reform

Platforms provide the means for transmitting hateful, violent, and abusive content—and, frequently, by more active enabling functions—in inciting violence, polarizing societies, spreading conspiracies, and facilitating discrimination, gender-based violence, and harassment. At the same time, tech companies have no accountability through third-party audits, no transparency requirements, and are almost completely shielded from legal liability due to Section 230 of the Communications Decency Act (CDA 230). Today, there is a complete lack of oversight and independent verification of the claims tech companies make, whether via Congressional testimony, in their transparency reports, or in related communications.

- Congress must **effectively reform, not eliminate, CDA 230** to hold social media platforms accountable for their role in fomenting violence, disinformation, and other forms of hate leading to harm—especially because of Big Tech's algorithmic amplification of dangerous content. Reform, however, must prioritize both civil rights and civil liberties concerns and not result in an overbroad suppression of free speech, nor unintentionally cement the monopolistic power of Big Tech by making it too costly for all but the largest platforms to ward off frivolous lawsuits and trolls. It is important to focus reform on targeted advertisements, egregious harms, and unlawful activity resulting in violence that has been facilitated, or actively abetted, by algorithms. This would be particularly powerful if accompanied by other laws and regulations that focus on anti-discrimination measures, increased transparency, and other means of ensuring accountability.

- Many tech policy experts have focused their efforts on reforming CDA 230 in pursuit of a non-existent one-stop solution. Importantly, this reform is only one essential step in a much larger process. CDA 230 reform will make platforms liable for certain unlawful third-party content. It is unlikely, however, to have much impact on the "lawful but awful" hate that suffuses the internet and is often protected by the First Amendment in the United States. Therefore, policymakers must also **pass laws and undertake approaches that require regular reporting of meaningful metrics, increased transparency, and independent audits regarding content moderation, algorithms, and engagement features** while looking for other incentive-based or regulatory action.

- Additionally, Congress should encourage the Administration to **establish centers of expertise regarding online hate, violence, and severe harassment across agencies**. Within every agency, there should be cross-departmental task forces to help coordinate

the work and support the necessary research, enforcement and plans of action. Agencies should work with Congress to develop research grant programs to comprehensively assess the links between Big Tech business models and online hate and build a more detailed knowledge base of the industry role in online harms.

- In an absence of transparency and oversight, online spaces have been toxic for young teenagers and a breeding ground for extremism. Proposals such as the KIDS Act would increase protections for young people (under 16) who are exposed to manipulative marketing, amplification of harmful content, and damaging design features. The Social Media DATA Act and the Algorithmic Justice and Online Platform Transparency Act would provide the public with a deeper understanding of the parameters and impact of platforms' algorithms, paid content, and other information crucial to fighting online discrimination and extremism.

Enforcement at Scale

When something goes wrong on a major social media platform, tech companies blame scale and plead impotence. The fact that millions, even billions of pieces of content can be uploaded all over the world, shared, viewed, and commented upon by millions of viewers in a matter of seconds serves as the justification for "mistakes" in content moderation—even if those mistakes result in violence and death. But scale is not the problem here; defective policies, bad products, and subpar enforcement are the root of Big Tech's lackluster enforcement.

Today, most major social media companies only publish limited information about their content policies and enforcement. Reports end up serving as a deflection away from the truth about what content proliferates on platforms. Recent revelations from leaked documents show that this isn't just a theory—organizations like Facebook had an unannounced program called XCheck that allowed over 5 million celebrities, politicians, and influencers to effectively skirt all of the published rules and policies. That meant that none of the posts by millions of public figures went through automated systems that normally flag violating content. The most influential accounts got a free pass for posting almost anything they wanted whenever they wanted. We only know about this because of a whistleblower. None of this was disclosed in a single platform report. This is why we need increased protection for whistleblowers. Proposals like the FTC Whistleblower Act of 2021 would protect whistleblowers who disclose wrongdoing at their current and former employers for issues under FTC jurisdiction.

Social media companies have little to no legal or financial incentives to give consumers comprehensive information. There is a strong need for systematized, regulated, and easily accessible transparency efforts from social media platforms. Platforms claim to have strong policies against hate, violence, and extremism, when in fact, most are unclear, hard to find, or have perplexing exceptions.

- Transparency reform would motivate platforms to be more explicit about their policies on hate, harassment, and misinformation, and apply their rules consistently. It would act as a

deterrent from making changes, exceptions, or other decisions that end up amplifying hate. It would create an environment where social media companies can compete on how well they are protecting users, not on how they can optimize the most corrosive content to keep us scrolling for as long as possible to sell as many ads as possible. Proposals like the transparency requirements offered in California's AB 587, which would require large social media companies to report on their content management policies and enforcement behaviors on a quarterly basis, can provide necessary information on how platforms are determining, codifying, and implementing their policies.

- Transparency reports must evaluate success and provide evidence that independent researchers can use; such independent researchers must be granted uninterrupted access to data, and Congress must continue an oversight role. Companies can and should increase transparency related to their products. At present, technology companies have little to no transparency in terms of how they build, improve, and fix the products embedded into their platforms to address hate and harassment. In addition to transparency reports, technology companies should allow third-party audits of their work on content moderation on their platforms. Audits would also allow the public to verify that the company followed through on its public commitments and to assess the effectiveness of company efforts across time.

- **Platforms must mitigate harm to consumers through products, designs, algorithms, and policies that further discrimination, bias, and hate.** Platforms should ensure that their design, user agreements, and policies counter the potential for bias-based discrimination and civil rights violations on the platform. To do this, platforms must regularly evaluate the way product features and policy enforcement fuel discrimination, bias, and hate and make product/policy improvements based on these evaluations. Platforms need an understanding of which populations are targeted or impacted most egregiously and why, the nature of hate content, and the path of spread; tech companies should create and maintain diverse teams to mitigate bias when designing consumer products and services, drafting policies, and making content moderation decisions. Proposals like the Deceptive Experiences to Online Users Reduction (DETOUR) Act would ensure platforms are not designing, modifying, or manipulating a user interface in a way that impairs users from making educated decisions before consenting and giving companies access to their personal data. Importantly, this proposal would also make it illegal to segment consumers of online services for the purposes of behavioral or psychological experiments without informed consent.

- A whole-of-government approach means that a wide range of legislative and regulatory bodies must exercise oversight to ensure tech companies adopt and consistently enforce policies and community guidelines designed to identify and combat violence, hate, and harassment. While there is not likely to be a one-size-fits-all set of guidelines or enforcement, incentives for effective standards and guidelines, transparency regarding them and their impact, and independent research evaluating these efforts can be imposed or supported by the government. **The FTC, State AGs, and other enforcement**

authorities also should increase consumer protection efforts, especially when tech companies engage in unfair and deceptive practices.

People Over Profit

The rapid and massive spread of extremism and hate on social media is a product feature, not a bug. Inflammatory mis- and disinformation and hate content generates growth and greater user engagement. Many tech company algorithms are wired to optimize for user engagement because the companies' business models are built around growing users and keeping people on the platform for as long as possible, to see as many ads as possible, because that is what generates revenue. As many former and current Big Tech employees have acknowledged, platforms like Facebook build and employ algorithms designed to promote engagement, thus inevitably amplifying the most corrosive content.

- **Platforms need to adjust their algorithms** and stop recommending or otherwise amplifying organizations or content from groups associated with extremism, hate, misinformation, or conspiracies to users—even if it results in less engagement from users. Platforms must invest in both AI improvements and adequately trained and resourced human content moderators—with training focused on particular cultural contexts and languages. The Algorithmic Justice and Online Platform Transparency Act and KIDS Act should be carefully considered as we look to accomplish goals of making algorithms safer for all users—especially young people.

- Platforms **also must put more resources toward protecting victims and targets of online harassment**, countering disinformation, and improving content moderation instead of prioritizing the bottom line. Platforms should provide effective, expeditious resources and redress for victims of hate and harassment. For example, users should be allowed to flag multiple pieces of content within one report instead of creating a new report for each piece of content. They should be able to block multiple perpetrators of online harassment at once instead of undergoing the laborious process of blocking them individually. Preventing users who repeatedly engage in hate and harassment from accessing a platform even if they create a new profile, known as IP blocking, helps protect victims.

- Platforms also need to pay more attention to online hate and misinformation in languages other than English. They need to invest in human content moderators who are well-trained in all of the major languages that their platforms service, and also need to devote major resources to improving AI detection of violative content in languages other than English. Leaders of state sponsors of terrorism shouldn't be given a free pass to incite Jew-hatred or glorify terrorism simply because they post in a language other than English.

- We urge Congress to focus on how consumers—and advertisers—are impacted by a business model that optimizes for engagement. Congress must focus on how both algorithmic amplification and monopolistic power can fuel hate. **They should ensure**

algorithms are ethical and fair and consider regulating surveillance advertising and increasing data privacy, so companies cannot exploit consumers' data for profit—a practice that inevitably results in greater online hate.

Access to Justice

A safer internet starts with protecting targets of harassment, not perpetrators. This means changing laws, policies, and practices that currently deny victims meaningful access to the courts and other effective avenues of redress. When tech platforms host harassing content and enable perpetrators to abuse their targets, victims of extremist violence, gender-based violence, hate, and harassment have no place to go in the face of physical threats, emotional injury, and financial and reputational harm. Victims and targets have been denied access to justice because our cyberharassment laws are outdated or don't exist at all.

According to ADL's latest data, 1 in 3 Americans who are harassed online attribute the harassment in whole or in part to their identity, referring to race, religion, gender, sexual orientation, gender identity, ethnicity, ability, and the like. More specifically, women experienced harassment disproportionately, as 35 percent of female-identified respondents felt they were targeted because of their gender. This abuse also happens in online games spaces. According to ADL's recent online gaming survey exploring the social interactions, experiences, attitudes, and behaviors of online multiplayer gamers nationwide, for the third year in a row gender was the most frequently cited reason for abuse.

Harassment intrudes into users' lives and hampers their ability to communicate, unfairly impacting marginalized communities' ability to work, socialize, learn, and express themselves online.

- We urge Congress and executive agencies to provide more resources and pressure agencies to pursue investigations and enforcement actions of bias-based cyberstalking, doxing, and swatting. Also, **Congress should update gaps and loopholes in cyber harassment laws** and the reporting of bias-based digital abuse in order to better protect victims and targets, including enacting legislation related to doxing, swatting, and non-consensual distribution of intimate imagery. One way to achieve this is by improving and passing the Online Safety Modernization Act at the federal level while also encouraging states to pass anti-cyberharassment legislation.

- According to ADL's ethnographic study of online hate and harassment, "some of the most widely reported incidents of campaign harassment (the ability of harassers to use online networks to organize campaigns of hate) and networked harassment (the weaponization of a target's online network) have been waged against women and the LGBTQ+ community." Victims and targets of cyberhate need more resources and support. Congress and the Administration should work together to create a resource center to support targets of identity-based online harassment. This center could provide tools to victims and targets seeking to communicate with social media platforms, report unlawful behavior to law enforcement, and receive extra care. Additionally, creating a hotline for victims and targets of cyberhate and harassment and requiring the platforms to

regularly report on the quantity and types of hate and harassment reported and actioned can help us tackle this issue.

Interrupting Disinformation

Hatemongers and extremists spread disinformation to harm targets and terrorize vulnerable communities; they amplify conspiracy theories to advance political aims; radicalize followers; and incite violence either intentionally as a tool to meet their goal or as a predictable outcome. Their content becomes further normalized when influential people, including high-level officeholders, spread this content further, often claiming that they are only "passing on" information they did not create for their followers to "evaluate." Hatemongers and extremists find ways to engage on mainstream social media platforms (Twitter, Facebook, YouTube), fringe platforms (Parler, Telegram, 4chan/8kun) and the Dark Web (Gab, DLive, america.win). It is a vicious cycle: this extraordinary spread is both made possible by, and helps further increase, the profound distrust of government and institutions.

The mainstreaming and normalization of hateful and extremist beliefs (including virulently misogynist, antisemitic, and racist conspiracy theories) is the foundation of much of the disinformation proliferating online. This is made evident by the fact that millions of Americans believe in QAnon conspiracies and other extremist ideologies.

Interrupting disinformation and finding/encouraging off-ramps and effective mitigation strategies to counter radicalization is no longer a marginal issue. It now requires a whole-of-government and society approach. There is a clear connection between online extremist, antisemitic, misogynist, racist, and hateful images and tropes reverberating on social media and offline hate and violence directed at marginalized communities. Further, the deadly insurrection at the United States Capitol is a key example of the violence that can erupt when extremist disinformation spreads on social media.

- The continuing spread of baseless and dangerous conspiracy theories will continue to find fertile ground. Social media algorithms recommend content to extremist-leaning users, including related groups and pages that contain harmful content. Government must join with civil society and industry to find ways to undermine, interrupt, and mitigate disinformation without undermining civil rights and liberties. **Congress should fund research on the impact of social media platforms' recommendation systems and algorithmic amplification mechanisms** on the intersection between algorithmic amplification of disinformation, misogyny, and gender-based violence.

- Congress and the executive branch must provide resources to civil society organizations working to counter online disinformation. We strongly urge you to **support widespread media literacy, digital literacy, and anti-disinformation education.** Congress should investigate the nature and impact of product designs that allow hatemongers and extremists to exploit digital social platforms and spread antidemocratic, violent, and hate-based disinformation. It should also support concerted research to identify new ways of countering dangerous disinformation that leads to violence—especially gender-based

violence. It is simultaneously vital not to abuse this imperative to surveil vulnerable communities or to crack down on its non-violent critics and adversaries.

Research and Innovation

Government actors, civil society, and the tech sector must stay ahead of the curve as emerging threats will inevitably contribute to the impact of online hate. There must be a concerted effort to focus on technology research and innovation aimed at combating online hate. Just as privacy-by-design has been promoted, with some notable success, "anti-hate by design" must be promoted and widely incorporated into social media platforms and made a fundamental consumer expectation.

Government actors and platforms must focus on research and innovation to slow the spread of online hate, including, but not limited to: (1) measurement of online hate; (2) the extent of sexism, hate and extremism in online games; (3) methods of off-ramping vulnerable individuals who may be going down a path to commit extremist and gender-based violence; (4) the connection between online hate speech and hate crimes; (5) new methods of disinformation; (6) the role of internet infrastructure providers and online funding sources in supporting and facilitating the spread of hate and extremism; (7) the role of monopolistic power in spreading online hate; and (8) audio content moderation. Congress can play a key role in this innovation to invest in improving our understanding of how hate impacts communities. Those community members are also individuals who have the most credibility in communicating with friends, family, etc. to prevent hate from taking root. Congress can invest in prevention, community engagement, and other tools to better understand how communities are dealing with the challenge.

CONCLUSION

Thank you for the opportunity to testify before this body and for calling a hearing on this urgent topic. It is long past time to acknowledge the threats social media platforms fuel and the need for increased accountability. These companies will tell you that it's too hard to address hate, extremism, and racism on the internet. They will claim the legal framework will prevent us from regulating their platforms. That is simply untrue. Time and time again, lawmakers have crafted good policies to protect consumers and industry alike—from regulation for automobiles, food, prescription drugs, and securities. There is a lot we can and must do to push hate and extremism back to the fringes of the digital world. We must address these threats holistically rather than piecemeal. This is precisely what ADL's **REPAIR** plans do, applying a whole-of-government and whole-of-society approach to fight online hate and extremism. On behalf of ADL, we look forward to working with you as you continue to devote your attention to this critical issue.

Ms. SCHAKOWSKY. I thank the gentleman. And now we have, remotely with us today, Dr. Marechal.

And you are recognized now for 5 minutes.

STATEMENT OF NATHALIE MARECHAL

Dr. MARECHAL. Thank you, Congresswoman. Good morning, and thank you to all of you for inviting me to testify today.

I am Natalie Marechal, senior policy and partnerships manager at Ranking Digital Rights.

As Congress crafts legislation to hold Big Tech accountable for its negative impacts on society, I urge you to focus on upstream structural reforms by regulating online advertising, mandating transparency and research access to data, and encouraging the Securities and Exchange Commission to use its existing regulatory authority to do what its shareholders are unable to: get Big Tech to comply with the same laws as all other public companies, and to improve their corporate governance.

The tenor and substance of congressional hearings on the tech industry has come a long way in the past few years, thanks to a growing recognition that the harms users experience through social media platforms are connected to business models centered on maximizing revenue from targeted advertising. This business model incentivizes rapid growth; anti-competitive behavior like predatory acquisitions of would-be competitors and vertical integration across the ad tech value chain; mass commercial surveillance; and data collection without our knowledge or consent; reliance on automation to perform tasks that actually require human nuance and contextual judgment to be done correctly; and consolidation of corporate power that thwarts any internal attempt at reform.

The company now known as Meta is the most brazen example of these dynamics. But the basic point that how a company makes money plays a determinate role in its products and its behavior is true across the tech sector and beyond. A business model that relies on the violation of rights will necessarily lead to products that create and amplify harms.

So what should Congress do about it? First, regulate the tech—the online advertising industry. Transpose the basic principles that govern offline advertising to the online world, and pursue antitrust enforcement in the ad tech sector. These measures will directly address consumer and civil rights harms related to privacy, discrimination, and fraud in online advertising. They will also shift the incentive structures that contribute to product design and corporate decisions that harm consumers and destabilize democracies around the world.

Further, increased competition in the ad tech market will undercut the Alphabet and Meta duopoly, and enable greater accountability for these two mega-corporations that often behave as though they are above the law.

Second, create the conditions for evidence-based policy-making by mandating specific types of transparency for information that can safely be made public, and by creating mechanisms for qualified, trustworthy, industry-independent researchers to verify companies' claims about users' experiences, and expand knowledge and under-

standing about how these platforms impact societies and democracy around the world.

The RDR methodology and the Santa Clara Principles on Transparency and Accountability and Content Moderation both provide granular recommendations for the data that companies should disclose publicly.

And third, Congress should encourage the SEC to use its authority to do what shareholders have been trying to do, and have been unable to do for reasons I will explain: get Big Tech to comply with the same laws as all other publicly-traded companies. Numerous whistleblower disclosures to the SEC indicate that several Big Tech companies are violating securities laws. But because of their dual-class share structure, shareholders are unable to hold corporate management accountable. When the CEO is also the chair of the board of directors, this means that person is accountable to no one.

I am talking about Mark Zuckerberg. No one should have this much power.

The SEC must address the private market exemptions that have allowed Big Tech companies to become so large, and with concentrated governance. Because Meta was able to obtain significant private market funding before going public, the company was able to impose this dual-class share structure, and a governance structure that allows Mark Zuckerberg to unilaterally make decisions that impact billions of people without any accountability. This loophole must be closed so that shareholder democracy of the future Facebooks can take hold.

To address the excesses of today's Big Tech firms, the SEC should ensue—should issue an enforcement policy declaring that it will not grant bad actor waivers to, and will seek increase enforcement penalties for companies with class B shares, or those in which a single person serves as CEO and share of the company's board of directors.

The bills under consideration today all seek to shine a light on Big Tech's secretive business practices, and hold them accountable when they harm their users, their competitors, or society more broadly, whether through deliberate action or through their failure to proactively identify and mitigate potential harms ahead of time.

The Republican Big Tech Accountability Platform also contains many provisions that Ranking Digital Rights has long called for: transparency into how Big Tech develops its content policies and regular, periodic disclosures about content policy enforcement, including the types of content taken down, and why, and clearly understood appeals processes.

Big Tech accountability is not a partisan issue. Americans may disagree about how social media companies should govern content on their platforms, but there is strong bipartisan agreement that Big Tech is not above the law and that, whatever companies do, they should be transparent about it, and they should be accountable to their users, their shareholders, and the American people. Legislation should start there.

Thank you again for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Dr. Marechal follows:]

Written Testimony of

Nathalie Maréchal, PhD

Senior Policy & Partnerships Manager

RANKING DIGITAL RIGHTS

An independent research program housed at New America

Before the
U.S. Congress
House of Representatives
Energy & Commerce Committee
Subcommittee on Consumer Protection & Commerce

Hearing on **Holding Big Tech Accountable: Legislation to Build a Safer Internet**

December 9, 2021

Good morning and thank you for inviting me to testify. I am Nathalie Maréchal, Senior Policy & Partnerships Manager at Ranking Digital Rights (RDR).

RDR is an independent research program housed at the New America think tank. We promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect the rights of internet users and their communities. We do this by ranking the world's most powerful digital platforms and telecommunications companies on international human rights standards. Our methodology is recognized in our field as the "gold standard" of corporate norms for tech and human rights, setting a high but achievable bar for a wide range of global tech and telecom companies. Our Corporate Accountability Index evaluates 26 publicly-traded companies headquartered in 15 countries. Among them are the U.S. "Big Tech" giants: Alphabet, Amazon, Apple, Meta, Microsoft and Twitter, but also large digital platforms based in China, Russia and South Korea, and global telecom operators. All told, these companies hold a combined market capitalization of more than USD $11 trillion. Their products and services affect a majority of the world's 5.1 billion internet users.

As Congress crafts legislation to hold Big Tech accountable for its negative impacts on society, I urge you to focus on upstream structural reforms by regulating online advertising, mandating transparency and researcher access to data, and encouraging the Securities and Exchange Commission (SEC) to act within its existing regulatory authority to do what shareholders are unable to: Get Big Tech to comply with the same laws as all other public companies.

In 2020, our two-part report, "It's the Business Model," took a critical look at what drives profits at Facebook, Twitter, and Google.[1] All three companies have built their business models on targeted advertising and algorithmic systems that can drive the reach of a message by targeting it to people who are most likely to share it, and thus influence the viewpoints of thousands or even millions of people. Companies' failures to staunch the flow of problematic content and disinformation online are rooted in these systems and the surveillance-based business models that they serve.

---

[1] Maréchal, Nathalie, & Ellery Roberts Biddle. *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge - A Report from Ranking Digital Rights*. New America. March 17, 2020, http://newamerica.org/oti/reports/its-not-just-content-its-business-model/
Maréchal, Nathalie, Rebecca MacKinnon & Jessica Dheere. *Getting to the Source of Infodemics: It's the Business Model*. New America. May 27, 2021, https://www.newamerica.org/oti/reports/getting-to-the-source-of-infodemics-its-the-business-model/

Social media platforms will never be able to rid the internet of problematic speech, even if we could all agree on what speech is problematic. So instead of seeking to hold them liable for content posted by their users, Congress and advocates should focus on how content is amplified and targeted by regulating the surveillance-based business model that incentivizes platforms to collect massive amounts of personal information without meaningful consent, to optimize product design for virality and engagement, and to make business decisions without adequately considering the negative impact on society, much less put proper measures in place to mitigate harms. We think it's bad in the United States, but Facebook cares even less about its negative impact on society in parts of the world less valuable for serving its business model, like Ethiopia[2] and Myanmar.[3] Facebook's documented failure to implement robust content moderation systems in languages other than English is particularly egregious, but it's hardly an outlier.

Last week, the Subcommittee on Communications and Technology held a hearing on potential reforms to the Section 230 intermediary liability shield. Reforming Section 230 could enable those who have been harmed by online speech or conduct to sue the platform hosting the content in question, but only if said content was already illegal. This would not address hate speech, false statements about political candidates, public health misinformation, and other types of content that members of Congress are rightly concerned about but are nonetheless protected by the First Amendment. Nor would it help us understand the inner workings of the "black box" platforms whose algorithmic decision-making holds so much power over our lives. Evidence-based policymaking requires industry-independent research, which in turn requires access to platform data. The Social Media DATA Act takes a necessary first step in that direction by compelling greater transparency about online advertising, including targeting parameters, and by creating a mechanism for the FTC to provide qualified, industry-independent researchers access to non-advertising platform data for research purposes.

The tenor and substance of Congressional hearings on the tech industry has come a long way in the past few years, thanks to a growing recognition that the harms users experience through social media platforms are connected to platform business models centered on maximizing revenue from targeted advertising. This business model incentivizes rapid growth; anti-competitive behavior, such as predatory acquisitions of would-be competitors and vertical integration across the ad tech value chain; mass data collection without knowledge or consent; reliance on automation to perform tasks that

---

[2] Zelalem, Zecharias and Peter Guest. "Why Facebook Keeps Failing in Ethiopia." Rest of World, November 13, 2021, https://restofworld.org/2021/why-facebook-keeps-failing-in-ethiopia/.
[3] Wodinsky, Shoshana. "Rohingya Sue Meta for $150 Billion Over Facebook's Alleged Role in Myanmar Genocide." Gizmodo, December 7, 2021, https://gizmodo.com/rohingya-sue-meta-for-150-billion-over-facebooks-alleg-1848172791.

require human nuance and contextual judgment; and consolidation of corporate power that thwarts any internal attempt at reform. The company now known as Meta is the most brazen example of these dynamics, but the basic point that how a company makes money plays a determinant role in its products and behavior is true across the tech sector and beyond. A business model that relies on the violation of rights will necessarily lead to products/behaviors that create and amplify harms.

So what should Congress do about it?

First, regulate the online advertising industry. Transpose the basic principles that govern offline advertising to the online world, and pursue antitrust enforcement in the ad tech sector. These measures will directly address consumer and civil rights harms related to privacy, discrimination, and fraud in online advertising. They will also shift the incentive structures that contribute to product design and corporate decisions that harm consumers and destabilize democracies around the world. Further, increased competition in the ad tech market will undercut the Alphabet and Meta duopoly and enable greater accountability for two mega-corporations that often behave as though they are above the law.

Second, create the conditions for evidence-based policymaking by mandating specific types of transparency for information that can safely be made public and by creating mechanisms for qualified, trustworthy, industry-independent researchers to verify companies' claims about users' experiences and expand knowledge and understanding about how these platforms impact societies and democracy around the world.[4] The RDR methodology and the Santa Clara Principles on Transparency and Accountability in Content Moderation both provide granular recommendations for the data that companies should disclose publicly.[5]

Third, Congress should encourage the Securities and Exchange Commission (SEC) to act within its existing regulatory authority to do what shareholders are unable to: Get Big

---

[4] Carter, Daniel, Amelia Acker, and Dan Sholler. "Tech Companies are Secretive; Researchers Need to Get Investigative." Information Matters, December 2, 2021, https://informationmatters.org/2021/10/tech-companies-are-secretive-researchers-need-to-get-investigative/.
Whittaker, Meredith. "The Steep Cost of Capture." *ACM Interactions* 28, no. 6 (November-December 2021): 50, https://interactions.acm.org/archive/view/november-december-2021/the-steep-cost-of-capture.
Benesch, Susan. "Nobody Can See Into Facebook." *The Atlantic.* October 30, 2021, https://www.theatlantic.com/ideas/archive/2021/10/facebook-oversight-data-independent-research/620557/.

[5] "2020 Indicators." Ranking Digital Rights, accessed December 6, 2021, https://rankingdigitalrights.org/2020-indicators/.
"The Santa Clara Principles." The Santa Clara Principles, accessed December 6, 2021, https://santaclaraprinciples.com/.

Tech to comply with the same laws as all other public companies. Numerous whistleblower disclosures to the SEC indicate that several Big Tech companies are violating the securities laws, but because of their dual-class share structure, shareholders are unable to hold corporate management accountable.

The SEC must address the private market exemptions that allowed Big Tech companies to become so large and with concentrated governance. Because Meta was able to obtain significant private-market funding before going public, the company was able to impose a dual-class share structure and a governance structure that allows Mark Zuckerberg to unilaterally make decisions that impact billions of people without any accountability. This loophole must be closed so that shareholder democracy of the future Facebooks can take hold. To address the excesses of today's Big Tech firms, the SEC should issue an enforcement policy declaring that it will not grant bad actor waivers to, and will seek increased enforcement penalties for, companies with Class B shares or those in which a single individual serves as CEO and Chair of the company's Board of Directors.

The bills under consideration today all seek to shine a light on Big Tech's secretive business practices and hold them accountable when they harm their users, their competitors, or society more broadly, whether through deliberate action or through their failure to proactively identify and mitigate potential harms ahead of time. The Republican Big Tech Accountability Platform also contains many provisions that Ranking Digital Rights has long called for: transparency into how Big Tech develops its content policies and regular disclosures about content policy enforcement, including the types of content taken down and why, and clearly understood appeals processes.[6]

Big Tech accountability is not a partisan issue. Americans may disagree about how social media companies should govern content on their platforms, but there is strong bipartisan agreement that Big Tech is not above the law, and that whatever companies do, they should be transparent about it, and they should be accountable to their users, their shareholders, and the American people. Legislation should start there.

Thank you again for the opportunity to testify today, and I look forward to your questions.

---

[6] Republican Leader McMorris Rodgers to Energy and Commerce Committee Republican Members. "Big Tech Accountability Platform," accessed December 7, 2021, https://republicans-energycommerce.house.gov/wp-content/uploads/2021/01/Big-Tech-Accountability-Platform-Memo.pdf.

Ms. SCHAKOWSKY. Thank you so much. And now let me recognize Mr. Lane.

You are recognized for 5 minutes.

STATEMENT OF RICK LANE

Mr. LANE. Chair Schakowsky, Ranking Member Bilirakis, Chairman Pallone, Ranking Member McMorris Rodgers, and members of the subcommittee, thank you for inviting me to testify. My name is Rick Lane, and I am the CEO of a strategic advisory firm, Iggy Ventures. I also volunteer my time to help child safety organizations combat sex trafficking and other online threats to children.

Over the past 30 years I had the opportunity to work on almost every major piece of technology-related, consumer protection, privacy, and cybersecurity legislation that has moved through Congress. I testify today in my personal capacity.

Building a more safe, secure, and sustainable internet will require Congress to focus on four main issues: one, reforming Section 230; two, creating more transparency in the way internet platforms operate, while protecting internet users' privacy; three, restoring access to the WHOIS data; and four, updating the Child Online Privacy Protection Act. These issues do not necessarily need to be addressed in the single comprehensive piece of legislation, but they should be discussed in a comprehensive fashion. All the pieces must fit together.

I recognize that Section 230 reform is the province of another subcommittee, and was the focus of last week's hearing. I would be remiss, however, if I didn't take this opportunity to take a few—to make a few observations on the topic.

I believe we need to restore to platforms the ordinary duty of care that would apply, but for courts' current and overbroad application of Section 230. Social media companies are rife with offers to sell illegal drugs, yet the former CEO of TikTok stated at a 2020 technology event that he had never been told of illicit drug transactions on the platform, and doubted their very existence. That was a surprising statement, since others knew, including the drug dealers that were using TikTok's platform.

TikTok could also increase the threat of espionage and cyber attacks, in light of the influence the Chinese Government has over both it and ByteDance, the Chinese company that owns TikTok. Indeed, we are confronted with a social networking site that is, A, susceptible to manipulation by a Communist regime with a record of human rights abuses; B, growing more rapidly than any U.S. competitor; and C, collecting massive amounts of data on our youngest and most easily influenced demographic, in an arms race to develop more sophisticated artificial intelligence.

It is for these reasons that both H.R. 3991 Telling Everyone the Location of data Leaving the U.S. Act, introduced by Rep. Duncan, and H.R. 4000, the Internet Application ID Act, introduced by Rep. Kinzinger, are so important. These two bills, together, will provide the American people with the information they need to know exactly where these types of companies are headquartered, where their data is being stored, and to fully understand the risks they and their children are taking when using these apps, apps that can be used to undermine our democracy.

Another transparency issue that Congress needs to address is access to accurate, WHOIS domain name registration, which contains basic contact details for holders of internet domains, and is fundamental to protecting consumer privacy, promoting lawful commerce, ensuring public safety, and protecting our national security. Indeed, a Department of Justice report states that the first step in online reconnaissance often involves use of ICANN's WHOIS database.

In 2018, registries and registrars like GoDaddy, VeriSign, Namecheap increasingly began restricting access to WHOIS data, based on an overlap—application of the European Union GDPR. Yet almost after five years of "trying to fix the WHOIS GDPR problem," ICANN has failed. The time has, therefore, come for this committee and Congress to pass legislation requiring domain name registries and registrars to once again make WHOIS information available, and that will be zero cost to consumers.

No other area of consumer protection is more important than establishing reasonable policies to protect children in the marketplace. This is especially true in the area of online privacy and market-dominant digital payment apps and debit cards that target children, and collect and exploit a shocking amount of their data. COPPA, enacted in 1998, creates an opt-in parental consent privacy regime for websites directed at children under 13.

By contrast, Gramm-Leach-Bliley, enacted in 1999, created an opt-out privacy regime for financial institutions. That privacy space between COPPA and GLBA creates a FinTech child privacy protecting—protection gap in existing law. This gap is especially harmful as we move toward a cashless society, a trend accelerated by the pandemic.

The good news is that one company, FinTech digital company which I am involved with, Rego Payment, is the only COPPA-compliant digital wallet.

Thank you again for giving me this opportunity to participate today. I look forward to your questions, and continue to work with you and your staff. We must all work together to fix these important problems because, at the end of the day, it is the right thing to do.

Thank you.

[The prepared statement of Mr. Lane follows:]

U.S. House of Representatives
Committee on Energy & Commerce
Subcommittee on Consumer Protection & Commerce

Hybrid Hearing on:
"Holding Big Tech Accountable: Legislation to Build a Safer Internet"

Prepared Testimony of Rick Lane
Founder & CEO of Iggy Ventures, LLC
and Child Safety Advocate

Dec. 9, 2021

Chair Schakowsky, Ranking Member Bilirakis, Chairman Pallone, Ranking Member McMorris Rodgers, and Members of the Subcommittee:

Thank you for inviting me to testify. My name is Rick Lane. I am the founder and CEO of strategic advisory firm Iggy Ventures. I also volunteer my time to help child safety organizations combat sex trafficking and other online threats to children. My prior experience includes five years working for House Appropriations Committee Member Rep. Joseph Early (D-MA), five years at a major law firm, two years as director of congressional affairs and e-commerce for the U.S. Chamber of Commerce, and 15 years as SVP for government affairs at 21st Century Fox. Over the past 30-plus years, I had the opportunity to work on almost every major piece of technology-related consumer protection, privacy, and cybersecurity legislation that moved through Congress. I testify today in my personal capacity. My views should not be attributed to any other individual or entity.

Building a more safe, secure, and sustainable Internet will require Congress to focus on four main issues: 1) reforming section 230; 2) creating more transparency in the way Internet platforms operate, while protecting Internet users' privacy; 3) restoring access to WHOIS data; and 4) updating the Children's Online Privacy Protection Act (COPPA). These issues do not necessarily need to be address in a single, comprehensive piece of legislation. But they should be *discussed* in a comprehensive fashion. All the pieces must work together. Attachment 1 includes a slide I created in 1998 that illustrates the way technology policy issues interconnect and cut across jurisdictional lines.

We are also running out of time. Web 2.0 was built on top of a Web 1.0 that we now know has cracks in the foundation. And if you believe the latest chatter, we are on the precipice of Web 3.0. Unless we address the Internet's structural issues, I fear a virtual "metaverse" that occupies even more of our and our children's lives and collects even more information about us will exponentially exacerbate today's problems. The status quo works no longer. We need clear rules of the road that promote accountability.

Democrats and Republicans share concerns about the spread of illegal activity online, including identity theft, fraud, illicit sale of opioids, and dissemination of child sexual abuse materials. They share concerns over cybersecurity. And they share concerns over privacy. My hope is that the House and Senate can come together in a bipartisan and bicameral fashion to address those issues, no matter what partisan differences may exist on other issues.

Section 230 Reform

I recognize that section 230 reform is the province of the Communications & Technology Subcommittee and was the focus of a hearing last week. I would be remiss, however, if I didn't take this opportunity to make a few observations on that topic—which concerns the most fundamental form of consumer protection that we have, keeping people safe from harm.

We must return the rule of law to the Internet. I appreciate Congress's decision in 1996 to treat the Internet differently in its nascent years, which I not only supported, but worked to ensure. At this point, however, e-commerce is so ubiquitous as to be just commerce. Until we hold online platforms and other Internet intermediaries such as Cloudflare, Verisign, GoDaddy, the Internet Society, Namecheap, and even the Internet Corporation for Assigned Names and Numbers equally accountable as brick-and-mortar businesses, people will be less safe online.

For that reason, I agree with Prof. Danielle Citron, former House Commerce Committee Counsel Neil Fried, and the Alliance to Counter Crime Online. We need to restore to platforms the ordinary duty of care that would apply but for courts' current, overbroad application of section 230. Congress should amend section 230 to require that platforms and other Internet intermediaries take reasonable steps to curb illegal conduct online as a condition of receiving the section's protections. I further explain the need to restore the duty of care in an article I recently co-wrote in *Tech Policy Press*, provided in Attachment 2.

I am heartened to see how much effort this Committee is putting into reforming section 230. Unfortunately, none of the bills the Communications & Technology Subcommittee considered last week would restore the duty of care, as a recent letter to the Subcommittee from Victims of Illicit Drugs points out. VOID represents parents who have tragically lost children to the illegal sale of drugs over social media. "These children were not killed by misinformation, bias, hate speech, or algorithms," the letter explains. "They were killed, in part, because platforms negligently, recklessly, or knowingly facilitated illegal activity: in this case, an unlawful drug sale."

Social media such as Facebook, Instagram, YouTube, Twitter, Snapchat, and TikTok are rife with offers to sell illegal drugs. Although algorithms can exacerbate the problem, transactions often occur without amplification and posts peddling illicit substances are easy to find. Some platforms have taken helpful steps to address this issue, but other platform operators frequently have their heads in the sand. A former CEO of TikTok, for example, stated at a 2020 Technology Policy Institute event that he had never been told of illicit drug transactions on the platform and doubted their existence. That was a surprising statement since many others knew, including the drug dealers that were using TikTok's platform. Researcher Eric Feinberg and Professor Tim Mackey have over the years documented such illegal drug sales.

If platforms could be held civilly liable for irresponsibly enabling such transactions, they'd be much more likely to pay attention and curb the activity. By making simple language changes to section 230 that restore the duty of reasonable care, Congress could help combat not just Internet opioid sales but all current and future illegal activity online. And in a non-regulatory, pro-free market way that both conservatives and liberals should be able to support: creating meaningful incentives for platforms to find the most effective and efficient ways to prevent online harm.

TikTok could also increase the threat of espionage and cyberattacks in light of the influence the Chinese government has over both it and ByteDance, the Chinese company that owns TikTok. Indeed, we are confronted with a social networking site that is: a) susceptible to manipulation by a Communist regime with a record of human rights violations; b) growing more rapidly than any U.S. competitor; and c) collecting massive amounts of data on our youngest and most easily influenced demographic in an arms race to develop more sophisticated artificial intelligence. Moreover, TikTok has been proven to have security flaws, as well as agreed to pay a record-setting $5.7 million in 2019 to settle FTC allegations that it illegally collected personal information from children.

Yet section 230 limits TikTok's liability for any nefarious activity by the Chinese government or other third party that the platform might enable. Combining the interests underlying TikTok's surveillance-based business model with the interests underlying China's surveillance-based and oppressive governance model creates an even more dangerous threat in an online world that lacks basic accountability. I include in Attachment 3 an article I wrote addressing the unique problems presented by TikTok.

Transparency

Online platforms and their defenders often hide behind the First Amendment, arguing that section 230 reform proposals will violate constitutional protections for free expression. Although the First Amendment protects platforms' editorial discretion over "awful but lawful" *content*, that protection does not extend to non-expressive and unlawful *conduct*. That is true as applied to the conduct of the platforms' users as well as the conduct of the platforms themselves in negligently managing such user behavior.

The section 230 reform proposal I recommend above focuses on conduct and so does not run afoul of the First Amendment. In fact, by producing a safer, more lawful online space, it advances core First Amendment interests. Limiting harassment and abuse that can silence different perspectives and communities will increase participation, enhancing transparency and information available to all.

One way, however, to address misinformation, bias, hate speech, or other concerns that would promote free expression rather than hamper it would be for Congress to enact transparency requirements. Indeed, Democrats and Republicans alike have expressed frustration with the opaque and inconsistent way platforms engage in content moderation.

The Supreme Court has held that the First Amendment allows the government to require that commercial enterprises provide "purely factual and uncontroversial information about the terms under which [their] services will be available," where the "disclosure requirements are reasonably related to the State's interest in preventing deception of consumers." Congress could thus adopt transparency provisions that require each platform to: 1) publicly disclose its content moderation policies; 2) create a process by which users can file a complaint with the platform arguing it did not follow its own policies; 3) create a process by which users can appeal a platform's decision to take down or leave up specific content, or to terminate or not terminate service to a user; and 4) publicly disclose information about the decisions the platform has made to take down or leave up certain content, or to terminate or not terminate service to a user.

Platforms that violate these transparency requirements or their own policies would lose the section 230 shield and might be culpable for breach of contract or a deceptive trade practice. These transparency requirements would also better enable individuals and businesses to decide what platforms to use—potentially prompting new entrants and existing providers to compete based on content moderation practices, thereby promoting innovation. In addition, the public disclosure requirements would allow policymakers, law enforcement, and researchers to track problematic trends—either with users' online misbehavior or the platforms' moderation practices—and develop strategies to address them.

WHOIS and Know Your Customer

WHOIS Access

The availability of accurate WHOIS data—which contains basic contact details for holders of Internet domain names—is also critically important and was core to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN). WHOIS data has been public since the founding of the commercial Internet and forms the basis of online transparency, security, and accountability. Access to that information is necessary to protect consumer privacy, promote lawful commerce, and ensure public safety. Indeed, a DOJ cyber report states that "[t]he first step in online reconnaissance often involves use of the Internet Corporation for Assigned Names and Numbers' WHOIS database."

Domain name providers (registries and registrars) often fail to verify WHOIS information from registrants, however, and in 2018 providers increasingly began restricting access to WHOIS data based on an overapplication of the European Union's General Data Protection Regulation. This is hindering efforts by cybersecurity firms, public interest groups, the private sector, federal agencies, and law enforcement authorities to protect consumers online by stopping abuses like identity theft, fraud, illegal sale of opioids, human trafficking, state-sponsored espionage, and terrorism.

A 2018 survey of 55 global law enforcement agencies by the ICANN Public Safety Working Group, for example, revealed that 98 percent found the WHOIS system aided their investigative needs before domain name providers took these unnecessary restrictive measures, as compared to 33 percent after. More recently, a 2021 survey by the two leading cybersecurity working groups found that restricted access to WHOIS data is impeding investigations of cyberattacks. Two-thirds of the 277 respondents said that their ability to detect malicious domains has decreased, 70 percent indicated that they can no longer address threats in a timely manner, and more than 80 percent reported that the time it takes to address abuse has increased, which means that cyberattacks—and harm to victims—last longer. As the working groups explain:

> [C]hanges to WHOIS access following ICANN's implementation of the EU GDPR … continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattacks.
>
> * * *
>
> Criminals regularly register large numbers of domains in bulk, often in batches of hundreds or thousands of names at the same time. … To fight crime and abuse, large datasets are

> particularly powerful. … For this data-driven approach to work, however, high-volume, real-time access to WHOIS records is essentially required. Wait times, rate limiting, inconsistent responses, redacted data … all decrease response times and data quality.
>
> * * *
>
> Many users in law enforcement, public safety, and cybersecurity of the WHOIS [data] require timely and predictable access to accurate records. This is not only true for those attributing attacks but also for parties relying on bulk data analysis to map cybercriminal infrastructures and detect patterns of abuse. *The survey responses corroborate or are consistent with other studies that have concluded that the changes to WHOIS have undermined cybersecurity and impeded cyber investigations generally* (emphasis added).

The Department of Homeland Security has similarly identified the lack of access to WHOIS data as a significant and growing problem. The DHS stated in a July 16, 2020, letter to Rep. Bob Latta, then chairman of the House Commerce Committee's Consumer Protection Subcommittee, that if the agency "had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain."[1] The FTC and FDA have also expressed concern.[2]

The Department of Commerce has been outspoken about the United States' concern over the removal of public access to accurate WHOIS information. The Department sent a letter as far back as April 4, 2019, directing ICANN "to deliberately and *swiftly* create a system that allows for third parties with legitimate interests, like law enforcement, IP rights holders, and cybersecurity researchers to access non-public data critical to fulfilling their missions."[3] The letter observed that "[w]ithout clear and meaningful progress, alternative solutions such as calls for domestic legislation will only intensify and be considered."[4]

Yet after almost five years, ICANN has failed to solve the problem. The time has therefore come for this Committee to pass legislation requiring domain name providers to once again make WHOIS information available for legitimate purposes. Such legislation would help solve cyber issues at zero cost to taxpayers. Even the European Union's proposed 2.0 version of its Directive on Security of Network and Information Systems included language to address the problem of a "dark" and inaccurate WHOIS. I have included in Attachment 4 an article I wrote discussing how

---

[1] Letter from Raymond Kovacic, Assistant Director, Office of Congressional Relations, DHS, to Rep. Bob Latta (July 16, 2020).

[2] *See* Letter from Joseph Simons, FTC Chairman, to Rep. Bob Latta (July 30, 2020) (expressing concern over new domain name provider policies "that significantly limit the publicly available contact information relating to domain name registrants" and stating that "[t]he FTC would benefit from greater and swifter access to domain name registration data."); Letter from Karas Gross, Associate Commissioner for Legislative Affairs, FDA, to Rep. Bob Latta (Aug. 13, 2020) (stating that "[a]ccess to WHOIS information has been a critical aspect of FDA's mission to protect public health" and that the reduced availability of WHOIS data "has had a detrimental impact on FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients.").

[3] Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherine Chalaby, Chair, ICANN Board of Directors (April 4, 2019).

[4] *Id.*

the lack of WHOIS access is hindering anti-espionage and anti-terrorism efforts, and in Attachment 5 a letter from the Coalition for Online Accountability discussing the pressing need to solve the WHOIS problem. Congress and the Department of Commerce can no longer continue to put ICANN's multistakeholder process over the health, safety, and cyber security of the American people.

Know Your Customer Requirements

Online intermediaries other than domain name providers also have a role to play. The failure of many intermediaries to verify their customers' identities aggravates today's growing epidemic of harmful and illegal conduct online in two ways. First, people are more likely to engage in antisocial and unlawful conduct if they believe their identities are hidden. Second, holding individuals and entities accountable becomes harder if no one knows who they are.

That is why I helped submit comments on behalf of thirteen online safety organizations asking the Department of Commerce to adopt Know Your Customer-type obligations for Internet intermediaries as the Department implements Executive Order No. 13984 on "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities." People often have good reasons for protecting their identities, such as securing their safety from those who would cause them harm and avoiding retribution for whistleblowing. Verifying identities for use of Internet services can occur, however, while maintaining safeguards that prevent disclosure except in appropriate circumstances.

FinTech Child Privacy Protection Gap

No area of consumer protection is more important than establishing responsible policies to protect children in the marketplace. Yet while platforms and other Internet intermediaries have made it more difficult to deter or track individuals engaged in unlawful activity online, they have been even less steadfast in protecting our children.

This is especially true in the area of online privacy and market dominant digital payment apps that target children and collect and exploit "a shocking amount of" their data. That data can potentially lay the foundation for profiling and targeting child victims or identity theft and fraud that can undermine a child's financial future – especially if a company is hacked or breached and this information ends up in dark web data trading markets.

The Children's Online Privacy Protection Act, enacted in 1998, makes it unlawful for a "website or online service" to collect personal information from a child under thirteen—whether for the service's own use or to sell to others—without first obtaining parental consent.[5] This is essentially an opt in. By contrast, the Gramm-Leach-Bliley Act, enacted in 1999, makes it unlawful for a "financial institution" to disclose to a non-affiliated third party (but not to use itself) any non-public personal information about someone without offering them an opportunity to opt-out.[6] That space between ages 12 and 18 is the FinTech Child Privacy Protection (FTCPP) gap where young

[5] *See* Omnibus Consolidated Appropriations, Pub. L. No. 105-277, div. C, tit. XIII, 112 Stat. 2681, at 728-35 (1998) (codified at 15 U.S.C. §§ 6501-06).

[6] *See* Pub. L. No. 106-102, tit. V, 113 Stat. 1338, 1436-45 (1999) (codified at 15 U.S.C. §§ 6801-09).

consumers are not adequately protected but existing law does not empower parents to give them meaningful oversight and support.

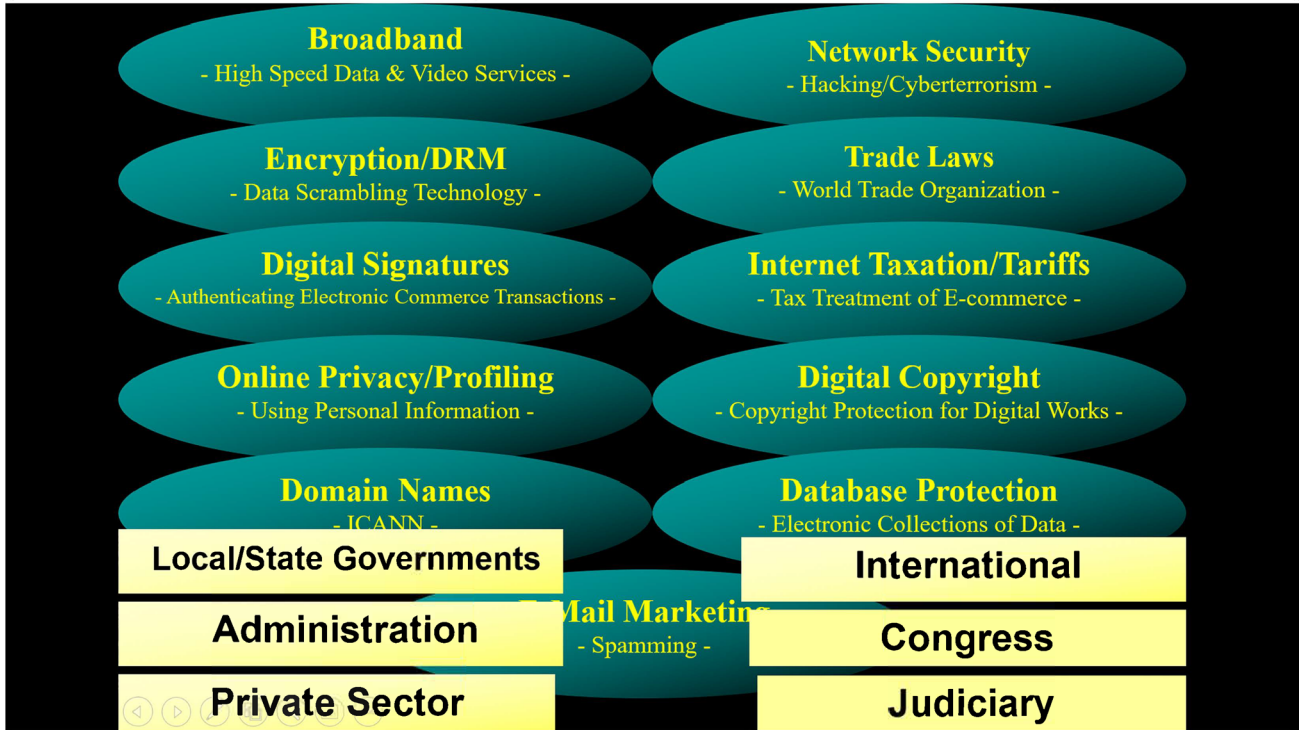
This FTCPP gap is especially harmful as we move toward a cashless society, however—a trend accelerated by the pandemic. Children today are more frequently engaging in financial transactions with digital wallets, both online and in stores. The parental opt-in requirements of COPPA certainly do not apply to children that use these digital services if they are 13 or older. Indeed, in some cases the FTCPP gap may even reach down to children who are younger than 13 depending on whether the entity doing the collecting qualifies as a financial institution as opposed to a website or online service. Unfortunately, some operators of financial applications may be exploiting this gap to use or sell the data of the kids they are currently courting to their services, as *Vice* reported earlier this year. That also means data on children is becoming more susceptible to data breaches.

The good news is that at least one FinTech provider is going above and beyond the legal requirements. Rego Payment Architectures—a company I provide strategic advice to and in which I am an investor—has incorporated COPPA privacy by design into its Mazoola financial application and pay button, producing the only COPPA certified digital payment app on the market. Mazoola allows parents to create digital accounts for their children but collects no personally identifiable information about the kids. All Mazoola knows is that the account is attributable to the parents and even there the company collects the bare minimum needed to comply with existing Know-Your-Customer and banking laws. The parents can then set chores or other tasks, pay allowances, set limits on the amount of money the kids may spend and where, and even reject specific purchase attempts in real time.

Rego is doing all this voluntarily. Which raises another point. The House and Senate Judiciary Committees' antitrust efforts may inadvertently harm such voluntary efforts by forcing technology companies to open their platforms. Without taking a position on the need for new antitrust legislation or the competitive impact of closed systems, it is true that closed systems are easier to keep safe. I do believe this Committee should keep an eye on the antitrust debates to make sure legislative efforts there do not make your job here harder. I have similar concerns about the impact of end-to-end encryption on the ability to keep children safe, absent creation of a lawful mechanism to access information for legitimate purposes. In this area, we should be wary of unintended consequences.

Thank you again for giving me the opportunity to participate today. I look forward to your questions and to continue working with you on these issues. We all must work together to fix these problems because, at the end of the day, it is the right thing to do.

Attachment 1



Tech Policy Press

TECHNOLOGY, POWER, POLICY AND PEOPLE

Section 230 Reform Naysayers Ignore Clear Problems Online-and the Clear Solutions

PUBLISHED OCTOBER 13, 2021

Skeptics of reforming Section 230 of the Communications Act, which limits platform liability, routinely diminish the unlawful and harmful conduct that online platforms facilitate through their own irresponsible behavior, as well as constitutional proposals that can help address this problem.

Take, for example, Jeff Kosseff and Daphne Keller's Oct. 9 *Washington Post* Perspective, "Why outlawing harmful social media content would face an uphill legal battle." In it, the authors focus on the "misinformation, toxicity, and violent content" that social media amplify. They point out that algorithmic amplification of awful but lawful speech is protected by the First Amendment, making many proposed legislative responses potentially unconstitutional.

This sidesteps, however, not only the platform carelessness highlighted in the recent series of four Senate hearings on protecting consumers and kids, but also the constitutional approach that Professor Danielle Citron and we have each put forward to address it: amending Section 230 so that platforms cannot invoke the liability shield unless they take reasonable steps to curb *unlawful conduct* on their services.

Ordinarily, businesses have a duty of care to protect one customer from harming another customer or the public. A hotel can be held civilly liable if it doesn't do enough to limit prostitution on its premises. A nightclub can be held civilly liable if it doesn't do enough to limit drug trafficking on its dance floor. A pawn shop can be held civilly liable if it doesn't do enough to limit fencing in its store.

These and many other situations have analogs in the online world. But a 1997 court interpretation of Section 230 granting platforms overbroad immunity for their irresponsible behavior has had the effect of preventing application of the duty of reasonable care in such situations. That decision further enables the platforms' "move fast and break things" culture, to borrow a phrase from Mark Zuckerberg.

As more of our social, economic, and political lives have moved online, this dereliction of the rule of law makes the public less safe and removes judicial recourse. Adding insult to injury, it gives online platforms an inappropriate competitive advantage over their brick-and-mortar rivals, which rightfully must expend resources to ensure their own behavior does not facilitate illegal or harmful activity.

Restoring the duty of care for online platforms, as we suggest, does not require repeal of Section 230. Nor does it involve government restriction of lawful speech. It simply gives victims access to the courthouse steps when a platform irresponsibly facilitates *unlawful or harmful conduct*. The victims still must prove their cases, but at least they can be heard.

The reasonableness standard has been developed over more than 100 years of judicial precedent that courts, victims, and platforms can rely on. It provides a mechanism that can account for platform size and the amount of harm, so that smaller platforms and startups are not treated as if they are Facebook or YouTube. And it can adjust as online problems and potential solutions evolve. If the platforms and their

defenders are worried about abusive litigation, they should join the tort reform movement, not defend a distortive, harmful, and unjust carve-out for social media.

There is also a constitutional way to address awful but lawful misinformation, toxicity, and violent content on social media—as well as platforms' erratic and opaque content moderation practices: transparency requirements.

Congress cannot require or prohibit platforms to take down or leave up lawful speech. The First Amendment leaves those decisions to the platforms' discretion.

But the Supreme Court has held that the First Amendment *does* allow the government to require that commercial enterprises provide "purely factual and uncontroversial information about the terms under which [their] services will be available," where the "disclosure requirements are reasonably related to the State's interest in preventing deception of consumers."

Congress could adopt transparency requirements that require platforms to: 1) publicly disclose their content moderation policies; 2) create a process by which users can file a complaint with the platform arguing it did not follow its own policies; 3) create a process by which users can appeal a platform's decision to take down or leave up specific content, or to terminate or not terminate service to a user; and 4) publicly disclose, subject to certain privacy protections, information about the decisions the

platform has made to take down or leave up certain content, or to terminate or not terminate service to a user.

Platforms that violate these transparency requirements or their own policies would lose the Section 230 shield and might be culpable for breach of contract or a deceptive trade practice. That would give users a venue when the platforms moderate in an inconsistent way.

These transparency requirements would also better enable individuals and businesses to decide what platforms to use—potentially prompting new entrants and existing providers to compete based on content moderation practices, promoting innovation.

In addition, the public disclosure requirements would allow policymakers, law enforcement, and researchers to track problematic trends—either with users' online misbehavior or the platforms' moderation practices—and develop strategies to address them.

Focusing on platforms' careless facilitation of unlawful or harmful conduct, along with these two constitutional approaches, would allow Congress to advance a freer, safer, more transparent internet. The platforms shift focus to lawful but awful speech because that problem is harder to solve. Entertaining that misdirection only benefits tech firms, the central beneficiaries of the status quo.

Neil Fried

Neil Fried launched DigitalFrontiers Advocacy in January 2020, bringing more than 25 years of experience in the public and private sectors, and testified before Congress on section 230 reform in June of that year. From 2013 to 2020, Neil was senior vice president for congressional and regulatory a!airs at the Motion Picture Association. He joined the MPA in 2013 from the House Energy & Commerce Committee, where he served as counsel and ultimately chief counsel on media and technology law issues for close to 10 years. Prior to working on the Hill, Neil represented clients before Congress and the Federal Communications Commission while at the D.C. o"ces of two law firms: Verner, Liipfert, Bernhard, McPherson and Hand; and Paul Hastings. He helped implement the 1996 Telecommunications Act as an attorney with the FCC from 1996 to 2000. Before coming to the FCC, he was a John S. and James L. Knight Foundation law fellow at the Reporters Committee for Freedom of the Press.

Rick Lane

Rick Lane is a tech policy expert, child safety advocate, and the founder and CEO of Iggy Ventures. Iggy advises and invests in companies and projects that can have a positive social impact. Prior to starting Iggy, Rick was the Senior Vice President of Government A!airs of 21st Century Fox/News Corporation. Rick was responsible for coordinating the development and implementation of the Company's public policy activities. Before joining 21st Century Fox, Rick was the first Director of Congressional A!airs focusing on E-Commerce and Internet public policy issues for the United States Chamber of Commerce. Prior to working at the Chamber, Rick was employed by the international law firm of Weil, Gotshal & Manges LLP (WG&M) as the Director of Legislative A!airs. While at Weil, he advised and represented clients before Congress on a variety of legislative matters a!ecting the technology and telecommunications industries. From 1988 to 1993, he worked as an Associate Sta! member to the House Appropriations Committee. His primary responsibilities involved technology, telecommunications, tax, education, labor and related issues.

Gretchen Peters

Gretchen Peters is Executive Director of the Alliance to Counter Crime Online. She conducts complex research and investigations of organized crime and corruption.

The Trichordist

Artists For An Ethical and Sustainable Internet #StopArtistExploitation

Tag: Tik Tok Drug Dealers

Crouching Tiger, Hidden Dragon: Broad and Antiquated CDA 230 Immunity for TikTok Could Aid China's Secret Efforts to Undermine U.S. Cyber-Security: Guest Post by Rick Lane

I believe there are only two public policy issues that President Trump and Vice President Biden agree upon: The status quo of Section 230 of the 1996 Telecommunication Act is no longer acceptable; TikTok is a threat to our cyber and national security.

Interesting enough, these two issues are interlinked. Section 230 of the Communications Decency Act (CDA 230) gives free reign to Internet platforms operating in the United States to act with impunity as it relates to user generated content. Predictably, this has led to unintended and destructive consequences. But, left unsaid is what Big Tech doesn't want anybody to realize – CDA 230 also unwittingly shields China as America's top geopolitical adversary challenges U.S. national and economic security right here at home.

According to Bloomberg, Chinese-controlled "ByteDance/TikTok, led by Zhang Yiming, is becoming a viable rival to the dominant American online behemoths, Facebook Inc. and Alphabet Inc.." Last year, TikTok's net profit was approximately $3 billion and the company estimates that it has about 80 million monthly active users in the United States, 60% of whom are female and 80% fall between the ages of 16 and 34. Of particular concern is that 60% of TikTok users are Gen Z, which is the largest generational cohort in American history and will include 74 million people next year.

As a champion of free markets, I would normally be among the first to applaud an upstart bringing a competitive "A" game to challenge dominant incumbent players no matter where they are based. But we have learned from experience that homegrown social networking companies like Facebook/Instagram, Google, and Twitter exert dominant and controversial influence in U.S. public policy debates – what sort of foreign influence should we expect TikTok to exert on this year's election.

Lately, I've found myself asking should I really be concerned?

A recent article by Larry Magid was the tipping point for me in this debate. The headline of the article was, "How A 51-Year-Old Grandmother and Thousands of Teens Used TikTok to Derail A Trump Rally & Maybe Save Lives." Magid lays out the series of events illustrating how attendance at a Trump rally was manipulated by a viral video of a grandmother from Iowa. It sounds innocent enough until you realize that the inflated numbers of expected attendees started when fans of K-pop, the popular Korean music genre, ordered free rally tickets from the Trump campaign with no intention of actually attending. Next, according to the article, the "grandmother from Iowa" posted a video on TikTok urging her mostly young viewers to "Google two phrases, 'Juneteenth' and 'Black Wall Street,'" before also suggesting that they register for two free tickets to the Trump rally. Her video post went viral and motivated young TikTok users to request hundreds of thousands of tickets.

After reading this, I was left with a simple question: Whether Trump or Biden, doesn't it bother anyone else that a Chinese-controlled social network was used to interfere with an American presidential campaign event at the same time that tensions between our two countries are escalating? Even Vice President Biden has banned TikTok from campaign phones and computers. As Mr. Magid's article acknowledges, "(i)t's long been known that social media can have a huge impact on politics. That's why Russia tasked a state-run agency to flood social media with posts and ads to get Donald Trump elected."

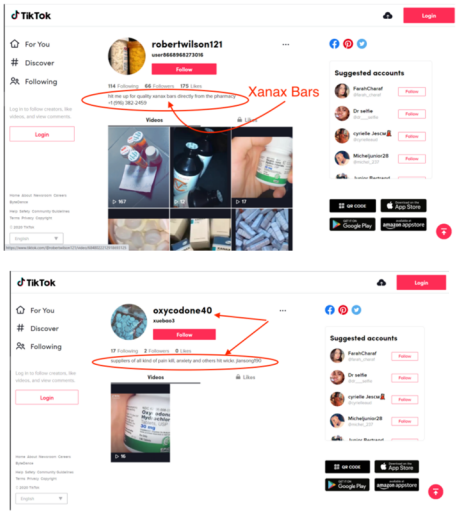
Two additional facts build on the story told by Magid. Another recent article, titled "Anonymous Hackers Target TikTok: 'Delete This Chinese Spyware Now," states that TikTok is "a data collection service that is thinly veiled as a social network. If there is an API to get information on you, your contacts, or your device, they're using it." The other fact to connect is that the key driver for algorithms and artificial intelligence, especially when dealing with human behavior, is vast data on human interaction. It is one of the main reasons that Microsoft is so interested in buying TikTok.

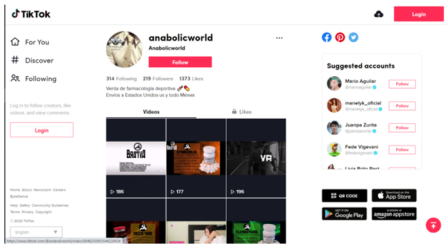
So now we are confronted with a Chinese based "social networking" site growing more rapidly than any homegrown US competitor and collecting more data on our youngest and most easily influenced demographic at the same time that China, Russia, and Iran are using social networks to undermine our democracy. Let's not forget that this social networking site has been proven not to be secure and agreed to pay $5.7 million to settle Federal Trade Commission (FTC) allegations that it illegally collected personal information from children, the largest civil penalty ever obtained by the FTC in a children's privacy case.

But most alarming is that TikTok is protected by CDA 230 and cannot be held accountable for the actions of its "users" even if those "users" happen to be foreign governments. For example, if the Chinese government is leveraging TikTok for its own strategic advantage, the US government has no recourse against TikTok for these activities. The impunity provided by CDA 230 to TikTok, as well as Chinese and other hostile governments, directly threatens our democratic process. Even more troubling is the fact that TikTok, along with Facebook and other social networking sites, cannot be held responsible for illegal conduct occurring on their platforms – even when they know about it.

Besides the potential of interfering with our elections, TikTok also continues to facilitate the sale of illegal drugs. Below are three screenshots of illicit activity being perpetrated on TikTok. The first two images show illegal drug sales of opioids and the other shows illegal drug sales of steroids. Remember, TikTok's core demographic and the intended audience for these posts consists primarily of members of Gen Z, those born between 1995 and 2012 –our children. [Similar to Google's near-indictment and $500,000,000 fine for violating the Controlled Substances Act (https://musictechpolicy.files.wordpress.com/2010/09/google-agreement.pdf).]

(Screenshots Provided by Eric Feinberg)





I will leave you with a quote from a recent speech (https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states) at the Hudson Institute by FBI Director Christopher Wray. He stated:

> "The Chinese government is engaged in a broad, diverse campaign of theft and malign influence, and it can execute that campaign with authoritarian efficiency. They're calculating. They're persistent. They're patient. And they're not subject to the righteous constraints of an open, democratic society or the rule of law… China, as led by the Chinese Communist Party, is going to continue to try to misappropriate our ideas, influence our policymakers, manipulate our public opinion, and steal our data. They will use an all-tools and all-sectors approach—and that demands our own all-tools and all-sectors approach in response."

For addressing this clear and present danger, the United States must modify CDA 230 and ensure that we have all the tools necessary to hold TikTok accountable for criminal activity that occurs by "others" on their platform. Importantly, this includes illegal actions taken by the Chinese government to misappropriate the site, and the massive amounts of data it collects, in order to inflict harm on the US and its allies. Finally, we must avoid inadvertently making this problem worse by spreading the excessively broad and antiquated immunity of CDA 230 through trade agreements with other countries.

Rick Lane is the founder and CEO of IGGY Ventures (https://www.worldwithoutexploitation.org/bios/rick-lane). IGGY advises and invests in technology startups and public policy initiatives that can have a positive societal impact. Rick served for 15 years as the Senior Vice President of Government Affairs of 21st Century Fox. Before joining Fox, Rick was the Director of Congressional Affairs focusing on e-Commerce and Internet public policy issues for the United States Chamber of Commerce.

September 20, 2020September 20, 2020 by Trichordist Editor

Attachment 4

Home My Network

CONGRESS MUST ACT NOW!

Published on December 22, 2020

Rick Lane
Strategic Advisor

9 articles ✓ Following

On January 10, 2020, the President issued an executive order strengthening the economic sanctions against Iran. While the Iranian government announced that the ballistic missile attacks on Iraqi bases

used by U.S. forces concluded their response to the killing of General Soliemani, increased tensions between the U.S. and Iran are expected to continue and Iran's cyber capabilities will continue to pose a threat to U.S. interests. Director of National Intelligence John Ratcliffe said both Iran and Russia have obtained US voter registration information in an effort to interfere in with the 2020 Presidential election. The Cybersecurity and Infrastructure Security Agency (CISA) recently announced the compromise of U.S. government agencies, critical infrastructure entities, and private sector organizations, most likely by Russia, beginning in at least March 2020. Recognizing those threats, the U.S. must ensure that it has the tools necessary at its disposal to defend itself – including access to WHOIS data.

WHOIS data is the registration information for *who is* behind a particular website. Much like public land and title records that demonstrate ownership of a physical location, WHOIS records had been publicly available since the inception of the Internet. WHOIS records have been used by law enforcement, cyber security experts and consumer advocates to identify malicious websites and either block, isolate or take additional action. Unfortunately, the recent, and overly broad, interpretation of the European Union's General Data Protection Regulation (GDPR) has resulted in this information being redacted and going almost entirely dark. No longer can law enforcement or cyber security firms quickly identify registration information behind a website and link that information to other, potentially harmful website.

Concerns around WHOIS information going dark have been well documented. In a survey of law enforcement agencies from around the world presentation to the Public Safety Working Ground at ICANN, 98 percent of respondents indicated that WHOIS information at least partially met their investigative needs prior to implementation of the EU GDPR. Since then, only 8 percent of those same respondents said that WHOIS still meets their investigative needs. At a 2019 briefing on Capitol Hill, Jason Gull, Senior Counsel in the Department of Justice's Computer Crime and Intellectual Property Section said, "We are finding that WHOIS is turning into 'WHO WAS.' We have historical information about WHOIS from a year ago and that information is like having an old phonebook.' Other agencies, including the Food & Drug Administration and Drug Enforcement Administration, have also expressed their frustration with this resource going dark.

Russia, Iran, China and its surrogate forces are well-known to be expert cyber-warriors. In a very short period of years, cyber warfare has gone from being an element of science fiction to a grim reality. Because it is highly asymmetric (very few expert hackers can cause widespread effects) and deniable (forensic attribution is not easy) many experts believe that cyber will become a preferred method attack and disruption that countries will use.

That is certainly true of countries like Russia, Iran and China. They have a history of using cyber tools effectively. In fact, several Iranians have been indicted in the U.S. justice system for their roles in cyber

activities targeting America and American entities. In 2018, an investigation by FireEye (using registration data) discovered over 2,800 inauthentic social media accounts originating from Iran that were ultimate removed from social media platforms. These accounts were designed to impersonate U.S. political candidates and influence media campaigns involving Iranian interests.

Dealing with the WHOIS problem is vital, and the urgency to do so is only increasing. Unfortunately, current estimates for regaining access to WHOIS by correcting the interpretation of the GDPR won't be available for three years or more. Now is the time for Congressional leadership. Without WHOIS, our vulnerabilities will continue to persist and investigations into not only cyber-frauds and cyber-warfare, but drug cases, intellectual property cases and other problems will be hurt.

As was stated by the U.S. Department of Homeland Security in a July 16, 2020 letter to Representative Robert Latta, "HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations… Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain."

Strengthening the cyber resilience of both public and private sector organizations is a matter of national security. We should expect that adversaries will continue to focus efforts to gather intelligence and cause disruptions through cyber-activities. For Congress and the Administration to ignore the WHOIS problem, or wait for the failed ICANN process to fix it, is turning a blind eye to an extremely serious risk to our nation. Congress needs to step in and address this vital weakness in our cyber defenses. Congress needs to enact WHOIS legislation now that will ensure that those who are protecting our national cyber infrastructure have all the tools they need to make America and the world more safe.

Attachment 5

Coalition for Online Accountability

November 30, 2021

The Honorable Maria Cantwell
Chairman
The Honorable Roger Wicker
Ranking Member
Senate Committee on Commerce, Science and Transportation
512 Dirksen Senate Building
Washington, D.C. 20510

Re: Nomination of Alan Davidson as Assistant Secretary of Commerce for Communications and Information

Dear Chairman Cantwell and Ranking Member Wicker:

We at the Coalition for Online Accountability ("COA")[1] have been deeply involved with ICANN related matters including those related to domain registrant information—often referred to as WHOIS data—and abuse in the Domain Name System ("DNS") for nearly twenty years. In light of the National Telecommunications and Information Administration ("NTIA")'s letter last year of December 23, 2020[2] to then Chairman Wicker and the developments at ICANN and the significant growth of cybercrime and DNS abuse since that time, we are writing to request that the information set forth below and the questions posed at the end of this letter be made part of the official record in connection with the hearing on December 1, 2021 to consider Alan Davidson as Assistant Secretary of Commerce for Communications and Information and head of NTIA.

As set forth in President's May 2021 Executive Order on Improving the Nation's Cybersecurity *"The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, and ultimately the American people's security and privacy"* and that *"the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."*[3]

[1] COA consists of seven leading copyright industry companies, trade associations and member organizations of copyright owners, all of them deeply engaged in the use of the internet to disseminate creative works. The COA members are Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association (MPA); the Recording Industry Association of America (RIAA); NBCUniversal; The Walt Disney Company; and WarnerMedia. COA's main goal since its founding nearly two decades ago (as the Copyright Coalition on Domain Names) has been to preserve and enhance online transparency and accountability.
[22] https://secureandtransparent.org/wp-content/uploads/2021/01/NTIA-Senate-Letter-12-23-20.pdf
[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

A specific component of this challenge concerns the current lack of access to domain name registration data (also called "WHOIS data")—the information that identifies the organization or individual that owns a website operating under a particular domain name. From the earliest days of the Internet until May 2018, WHOIS data was publicly accessible and used for investigating and mitigating illegal online activity by both public and private sector organizations, including law enforcement agencies, cybersecurity investigators, network technology professionals, child protection organizations, patient safety organizations, consumer welfare organizations, and anti-counterfeiting and anti-piracy organizations.[4]

Yet since the enactment of policies by the Internet Corporation for Assigned Names and Numbers ("ICANN") in May 2018 to attempt to comply with the European Union's General Data Protection Regulation ("GDPR"), the WHOIS system has essentially gone dark. As noted in a recently released study by Interisle, currently "*86.5% of registrants cannot be identified via WHOIS.*"[5] Letters have been written by a number of federal agencies describing how the current lack of access to WHOIS data is interfering with their investigations of a broad array of online criminal activity and is increasing risks to public safety and welfare. For example, the Department of Homeland Security set forth a very specific example in a letter last year to Congressman Robert Latta as follows:

"As a recent example of GDPR inhibiting HSI investigations, the HSI Cyber Crime Center (C3) Cyber Crimes Unit identified several websites posing as legitimate coronavirus disease 2019 (COVID-19) fundraising organizations, but are actually fraudulent. These websites claim to be sites for entities such as the World Health Organization, United Nations' foundations, and other non-governmental organizations, and appear to be legitimate. When HSI conducted WHOIS queries for these domains, most of the subscriber information was redacted as a result of GDPR. Having increased and expedient access to domain name registration information would have allowed HSI to identify the registered owners of the domains expeditiously in order to prevent further victimization by these illegitimate fundraising websites."[6]

As stated by NTIA in its letter of December 23, 2020 to this Committee, "the importance of this [WHOIS] data cannot be overstated." Furthermore, we support NTIA's conclusion that the policy, which has been under development by ICANN's multi-stakeholder process for now over three years, falls drastically and unacceptably short of meeting the public interest, particularly in the areas of safety, security, consumer welfare and protection of intellectual property. These difficulties and obstacles were further highlighted in a recent report published in June 2021 by the Messaging Malware Mobile Anti-Abuse Working Group ("M3AAWG") and the Anti-Phishing Working Group ("APWG").[7] Based upon a survey of nearly 300 cybersecurity practitioners, the report concluded:

- *"94% of our respondents report that redaction [of WHOIS data] impairs their ability to investigate relationships between malicious domains and actors."*
- *"Two-thirds of our respondents indicate that their ability to detect malicious domains has decreased."*
- *"The solutions currently discussed at ICANN would not meet the needs of law enforcement and cybersecurity actors in terms of timelines."*
- *"Changes to WHOIS access following ICANN's implementation of the EU GDPR . . . continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattacks."* (emphasis added)

M3AAWG and APWG wrote to the ICANN Board and CEO at the end of September 2021 to inform them of the study and to offer detailed specific suggestions to improve the WHOIS situation in order to reduce cyberattacks and cybercrime.[8] ICANN responded in November with a terse reply that stated in relevant part, *"The ICANN policy development process cannot define, correct ambiguities under, or change international law."*[9]

---

[4] Before May 2018, WHOIS data had been a public directory since the early 1980s. For a brief history of WHOIS, see: https://whois.icann.org/en/about-whois#field-section-3

[5] http://www.interisle.net/ContactStudy2021.html

[6] https://secureandtransparent.org/wp-content/uploads/2020/09/20-02497-ICEs-Signed-Response-to-Representative-Latta.pdf

[7] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

[8] https://www.icann.org/en/system/files/correspondence/cadagin-cassidy-to-marby-et-al-30sep21-en.pdf

[9] https://www.icann.org/en/system/files/correspondence/marby-to-cadagin-cassidy-04nov21-en.pdf

The 170+ member Governmental Advisory Committee ("GAC") to ICANN stated in June 2020 with respect to WHOIS data, *"[A]ccess to this information is essential to allow public authorities and other relevant entities to serve objectives such as law enforcement, cybersecurity, consumer protection or the protection of intellectual property. Such access remains a high priority for the GAC."*[10] Nevertheless, more than three years following the implementation of ICANN's policies to redact WHOIS data, access has been overwhelmingly unavailable and ICANN states it cannot do anything further because it cannot define the law.

QUESTION FOR NOMINEE DAVIDSON: Will you, as Assistant Secretary of Commerce and head of NTIA, work with us in Congress on legislative or regulatory measures to address this situation and restore access to WHOIS data? Given that the overwhelming majority of generic top-level domain names are administered by U.S. companies, are you willing to work with us on U.S. legislation that will require that U.S. based domain name registrars and registries: (i) verify the accuracy of the WHOIS data that they collect, and (ii) make such data publicly accessible? Such legislation will not cost the federal government a single dollar and yet it will significantly improve the ability of both government agencies and private sector cybersecurity professionals to investigate, mitigate and prevent cyberattacks and a broad array of cybercrime.

Thank you for your consideration.

Sincerely,

Dean S. Marks
Executive Director and Legal Counsel
Coalition for Online Accountability ("COA")
E-mail: ed4coa@gmail.com

[10] See ICANN67 GAC Communique at: https://gac.icann.org/contentMigrated/icann67-gac-communique at p. 7

4 November 2021

To: Amy Cadagin, Executive Director; Peter Cassidy, Secretary General
Cc: Maarten Botterman and Rod Rasmussen

Dear Ms. Cadagin and Mr. Cassidy,

Thank you for your letter dated 30 September 2021 regarding findings from the M3AAWG and APWG WHOIS Report presented to ICANN in June 2021. We acknowledge receipt of the recommendations contained in the letter. As stated in our 7 July 2021 response to your 8 June 2021 letter, the consensus policy recommendations developed by the ICANN community for a System for Standardized Access/Disclosure (SSAD) extend as far as the community determined possible, due to the ambiguity and legal constraints that exist under the GDPR. The ICANN policy development process cannot define, correct ambiguities under, or change international law.

The ICANN org appreciates M3AAWG and APWG's continued participation and engagement in the multistakeholder model and also noted your active participation in the recently completed ICANN72 Annual General Meeting.

Regards,

Göran Marby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)

Ms. SCHAKOWSKY. Thank you.
And now, Mr. Golin, the floor is yours for 5 minutes.

STATEMENT OF JOSH GOLIN

Mr. GOLIN. Thank you, Chair Schakowsky, Ranking Member Bilirakis, and distinguished members of the subcommittee for holding this important hearing. My name is Josh Golin, and I am executive director of Fairplay, the leading independent watchdog of the children's media and marketing industries.

Through corporate campaign and strategic regulatory filings, we have changed the marketing and data collection practices of some of the world's biggest companies. Currently, we are leading a campaign to stop Facebook from launching a children's version of Instagram. And last week, with other leading advocates, we launched Design with Kids in Mind, a campaign to demand regulations that require online operators put kids' interests first when designing their platforms.

Frances Haugen has shone a critical spotlight on Instagram's harmful impacts on teens, and Facebook's callous disregard for children's well-being. But it would be a mistake to view her revelations as problems limited to Facebook and Instagram. Compulsive overuse, exposure to harmful content, cyberbullying, harms to mental health, and the sexual exploitation of children are industry-wide issues that demand systemic solutions from Congress.

To put it plainly, the unregulated business model for digital media is fundamentally at odds with children's well-being.

Digital platforms are designed to maximize revenue and, therefore, engagement because the longer they can capture a user's attention, the more money they make by collecting data and serving ads. As a result, children are subject to relentless pressure and manipulative design that pushes them to use and check platforms as often as possible. The harms young people—this harms young people in several ways, including encouraging the overuse of social media and displacing critical online activities like sleep, exercise, and face-to-face interactions. Overuse can also lead to isolation from secure family relationships, and reduced interest in academic achievement and extracurricular activities, allowing for-profit tech companies to shape children's character, habits, and future.

Design choices used to maximize engagement are also harmful, because they exploit young people's desire for social approval, and their natural tendency towards risk-taking. Displays of likes and follower counts provide an instant snapshot of whose profiles and posts are popular. Children quickly learn that the way to improve these metrics is to post risque and provocative content, creating a permanent record of their youthful indiscretions, and increasing their risk of cyberbullying and sexual exploitation.

Platforms also harm young people by personalizing and recommending content most likely to keep them engaged. One former YouTube engineer observed recommendation algorithms are designed to optimize watch time, not to show content that is actually good for kids. This means that, on platforms like Instagram and TikTok, teens interested in dieting will be barraged with content promoting eating disorders, and a depressed user will be shown content promoting self-harm.

Nearly every concern that parents, public health professionals, and children themselves have about digital media platforms can be traced to deliberate design choices. It doesn't have to be this way. Apps and online platforms could be built, instead, to reduce risk and increase safeguards for children. But that won't happen without significant action from Congress.

The only Federal law that protects children online was passed 23 years ago, long before smartphones, Instagram, and YouTube even existed. Congress's continued inaction, combined with a lack of enforcement at the FTC, has emboldened Big Tech to develop an exploitative business model without considering or mitigating its harmful effects on children and teens. It is no wonder that polls consistently show that parents want Congress to do more to protect children online.

We know the key legislative solutions. The KIDS Act, which we will discuss today, would prohibit companies from deploying design techniques like autoplay, displays of quantified popularity, and algorithmic recommendations that put children and teens at risk. The Privacy Act would expand privacy protections to teens, ban harmful uses of data, like surveillance advertising, and require platforms to make the best interests of children a primary design consideration. Together, these bills would create the safeguards children need, and transform the online experience for young people.

Over the last year I have watched several hearings like this one, and was heartened to hear Members of Congress speak, first and foremost, not as Republicans and Democrats, but as parents and grandparents with firsthand knowledge of what is at stake.

But the American people need more than your understanding and justified anger at companies like Facebook. Big Tech is banking on the fact that partisan divisions will keep you from taking action. I hope you will prove them wrong, and advance legislative solutions that better protect children while they are online, and make it easier for them to disconnect and engage in the offline activities they need to thrive.

There is simply too much at stake for children and their futures to allow the status quo to continue.

Thank you for having me here today, and I look forward to your questions.

[The prepared statement of Mr. Golin follows:]

Written Testimony of Josh Golin

Executive Director, Fairplay

Before the House Energy and Commerce
Subcommittee on Consumer Protection

Hearing on "Holding Big Tech Accountable: Legislation to Build a Safer Internet"

December 9, 2021

My name is Josh Golin and I am Executive Director of Fairplay.

I would like to thank Chairman Pallone, Ranking Member McMorris-Rodgers, Chairwoman Schakowsky, Ranking Member Bilirakis, and the Distinguished Members of the Subcommittee for holding this important hearing of critical importance to America's families, and for inviting me to testify.

The courageous whistleblowing of Frances Haugen has shone a critical spotlight on Instagram's harmful impacts on teens and Facebook's callous disregard for children's wellbeing.[1] But it would be a mistake to view her revelations as problems limited to Facebook and Instagram. Compulsive overuse, exposure to harmful content, cyberbullying, harms to mental health, and the sexual exploitation of children are industry-wide issues that demand systemic solutions from Congress.

To put it plainly, the unregulated business model for digital media is fundamentally at odds with children's wellbeing. Digital platforms are designed to maximize revenue, and design choices that increase engagement and facilitate data collection put children at risk.

It doesn't have to be this way. Instead of prioritizing engagement and data collection, apps, websites, and online platforms could be built in ways that reduce risks and increase safeguards for children.

But tech companies won't make these changes on their own. It is past time for Congress to enact new online protections for children that require online operators to prioritize children's wellbeing in their design choices. Without meaningful Congressional action, children and teens will continue to be harmed by Instagram, TikTok, Snap, YouTube, and thousands of lesser known apps, websites, and platforms.

My testimony today will describe how many of the most serious issues facing children and teens online are a direct result of design choices made to further companies' bottom lines. I will also describe how a failure to regulate digital media for children and teens has led to today's harmful online environment. Finally, I will explain why we need a design code – a set of regulations that prioritize children's rights and needs – to ensure that young people can reap the benefits of the internet without being exposed to manipulation or harm.

---

[1] Wells, Georgia, et al. "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show." *The Wall Street Journal* (14 Sept. 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

I. About Fairplay

Fairplay (formerly Campaign for Commercial-Free Childhood) is the leading independent watchdog of the children's media and marketing industries. We are committed to building a world where kids can be kids, free from the false promises of marketers and the manipulations of Big Tech. Our advocacy is grounded in the overwhelming evidence that child-targeted marketing – and the excessive screen time it encourages – undermines kids' healthy development.

Through corporate campaigns and strategic regulatory filings, Fairplay has changed the child-targeted marketing and data collection practices of some of the world's biggest companies. Most notably, our 2018 Federal Trade Commission complaint against Google for violating the Children's Online Privacy Protection Act (COPPA) led to the 2019 FTC settlement that required Google to pay a record fine and to limit data collection and targeted advertising on child-directed content on YouTube.[2] We have filed other requests for investigation at the FTC that remain pending. We have documented, for example, that Google Play recommends apps for young children that violate COPPA and uses unfair monetization techniques;[3] that TikTok has not complied with the 2019 FTC Consent Decree that it was violating COPPA;[4] and that Prodigy, a popular online math game assigned by tens of thousands of elementary schools across the country uses manipulative design to unfairly promote expensive subscriptions to children.[5]

Our current campaigns include leading a large international coalition of parents, advocates, and child development experts to stop Facebook from launching a kids' version of Instagram.[6] And just last week, we introduced Designed with Kids in Mind, a multi-faceted campaign to demand regulations that would require operators to make the best interests of children a primary consideration when designing apps, websites, and platforms likely to be accessed by young people.[7]

Fairplay is also home to the Children's Screen Time Action Network, a global coalition of practitioners, educators, advocates, activists, parents, and caregivers working to promote a healthy childhood by

---

[2] Campaign for a Commercial-Free Childhood (now Fairplay) and Center for Digital Democracy. "Request to Investigate Google's YouTube Online Service and Advertising Practices for Violating the Children's Online Privacy Protection Act." *Counsel for Center for Digital Democracy and Campaign for a Commercial-Free Childhood before the Federal Trade Commission*. (2 April 2018). https://fairplayforkids.org/advocates-say-googles-youtube-violates-federal-childrens-privacy-law/

[3] Campaign for a Commercial-Free Childhood (now Fairplay) and Center for Digital Democracy. "Request to Investigate Google's Unfair and Deceptive Practices in Marketing Apps for Children." *Counsel for Center for Digital Democracy and Campaign for a Commercial-Free Childhood before the Federal Trade Commission.* (12 Dec. 2018), https://fairplayforkids.org/apps-which-google-rates-safe-kids-violate-their-privacy-and-expose-them-other-harms/

[4] Campaign for a Commercial-Free Childhood (now Fairplay) and Center for Digital Democracy. "Complaint and Request for Investigation of TikTok for Violations of the Children's Online Privacy Protection Act and Implementing Rule." *Counsel for Campaign for a Commercial-Free Childhood and Center for Digital Democracy before the Federal Trade Commission.* (14 May 2020). https://fairplayforkids.org/wp-content/uploads/2020/05/tik_tok_complaint.pdf

[5] Campaign for a Commercial-Free Childhood (now Fairplay). "Request for Investigation of Deceptive and Unfair Practices by the Edtech Platform Prodigy." *Campaign for a Commercial-Free Childhood before the Federal Trade Commission.* (19 Feb. 2020). https://fairplayforkids.org/wp-content/uploads/2021/02/Prodigy_Complaint_Feb21.pdf

[6] Fairplay. "Facebook's bait and switch on surveillance advertising to children." *Open Letter to Mark Zuckerberg.* (16 Nov. 2021). https://fairplayforkids.org/wp-content/uploads/2021/11/fbsurveillanceletter.pdf

[7] Fairplay. "Designed with Kids in Mind." (Accessed 7 Dec. 2021). https://designedwithkidsinmind.us/

reducing the amount of time kids spend with digital media. The Action Network hosts seven work groups, such as the Cyberbullying and Online Safety group whose members include parents who have experienced the worst types of social media-related tragedies.

II. Children and teens are spending more time with digital media than ever before, and the pandemic has accelerated the trend.

Research conducted prior to the pandemic found that nearly half of 2- to 4-year-olds and more than two-thirds of 5- to 8-year-olds have their own tablet or smartphone. By age 11, a majority of kids have their own smartphone, meaning they are potentially connected to the internet every waking moment regardless of location.[8]

That same research found preschool children average 2.5 hours of screen time per day, while pre-teens average almost 5 hours per day, and teens almost 7.5 hours per day. Importantly, these figures only count entertainment screen usage and not the time children spend on digital devices for school or homework. Children in lower-income households spent nearly two hours more with screens than children from higher-income households, and Black and Hispanic children spend significantly more time on screens than their white peers.[9]

COVID-19 has accelerated these trends, and screen time for children is estimated to have increased by 50% during the pandemic.[10] During the same period, online messages sent and received by children increased by an incredible 144%.[11] Thirty-five percent of parents report that their children began using social media during the pandemic at a younger age than their parents had originally planned.[12]

III. The platforms where children spend the majority of their time online are designed to maximize engagement, often at the expense of children's wellbeing and safety.

Digital platforms are designed to maximize revenue and therefore engagement because the longer they can capture a user's attention, the more money the platforms make. As a result, children are subject to relentless pressure and manipulative design that pushes them to use and check platforms as often as possible.

The effects of these design choices on young people are serious. Excessive screen media use and social media use is linked to a number of risks for children and adolescents, including obesity,[13] lower

---

[8] Rideout, V., and Robb, M. B.. The Common Sense census: Media use by tweens and teens." *San Francisco, CA: Common Sense Media.* (2019), https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-census-8-to-18-full-report-updated.pdf

[9] *Ibid.*

[10] Fischer, Sara, et al. "Kids' screen time up 50% during pandemic." *Axios.* (17 Jan. 2021), https://www.axios.com/kids-screen-time-pandemic-112650a6-743c-4c15-b84a-7d86103262bb.html

[11] Kelly, Heather. "Growing up on screens: How a year lived online has changed our children." *Washington Post*. (5 March 2021), https://www.washingtonpost.com/technology/2021/03/05/screen-time-one-year-kids/

[12] Munzer T., Torres C., Domoff S., Levitt K., Weeks H., Schaller A., Radesky J. "Media use practices of elementary-aged children during the COVID-19 pandemic." *In preparation.*

[13] Robinson, T. N., Banda, J. A., Hale L., Lu, A. S., Fleming-Milici, F., Calvert, S. L., Wartella, E. "Screen media exposure and obesity in children and adolescents." *Pediatrics,* 140 (Supplement 2), S97-S101. (2017), doi:10.1542/peds.2016-1758K

psychological wellbeing,[14] decreased happiness,[15] decreased quality of sleep,[16,17] increased risk of depression,[18] and increases in suicide-related outcomes such as suicidal ideation, plans, and attempts.[19] Fifty-nine percent of US teens have reported being bullied on social media,[20] an experience which has been linked to increased risky behaviors such as smoking and increased risk of suicidal ideation.[21]

The pressure to spend more time on digital media platforms and maximize interactions with other users also puts children at risk from predation. Twenty-five percent of 9- to 17-year-olds report having had an online sexually explicit interaction with someone they believed to be an adult.[22] In 2020, 17% of minors – including 14% of 9- to 12-year-olds – reported having shared a nude photo or video of themselves online. Of these children and teens, 50% reported having shared a nude photo or video with someone they had not met in real life and 41% reported sharing with someone over the age of 18.[23]

Below are just some of the tech features designed to increase user engagement that put children at risk:

Autoplay and Endless Scroll

One objective of persuasive design is to reduce friction so that platforms are easier to use and keep young people using them. Autoplay on video platforms like YouTube and TikTok's endless scroll mean that once children start watching, they are automatically served video after video with no action required. While these features are great for platforms' bottom lines because they increase engagement,

---

[14] Twenge, J., Campbell, K. "Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets," *Psychiatric Quarterly* 90, no. 2. 311–31, (1 June 2019), https://doi.org/10.1007/s11126-019-09630-7.

[15] Twigg, L., Duncan, C., Weich, S. "Is Social Media Use Associated with Children's Well-Being? Results from the UK Household Longitudinal Study," *Journal of Adolescence* 80: 73–83, (1 April 2020), https://doi.org/10.1016/j.adolescence.2020.02.002.

[16] Carter, Ben et al. "Association Between Portable Screen-Based Media Device Access or Use and Sleep Outcomes: A Systematic Review and Meta-Analysis." *JAMA Pediatrics* 170, no. 12: 1202–8, (1 Dec. 2016), https://doi.org/10.1001/jamapediatrics.2016.2341.

[17] Lemola, Sakari et al. "Adolescents' Electronic Media Use at Night, Sleep Disturbance, and Depressive Symptoms in the Smartphone Age." *Journal of Youth and Adolescence* 44 (1 Feb. 2014), https://doi.org/10.1007/s10964-014-0176-x.

[18] *Ibid.*

[19] Twenge, Jean et al. "Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time." *Clinical Psychological Science* 6, no. 1, 3-17, (1 Jan. 2018), https://doi.org/10.1177/2167702617723376.

[20] Anderson, Monica. "A Majority of Teens Have Experienced Some Form of Cyberbullying," *Pew Research Center: Internet, Science & Tech* (blog), (27 Sep. 2018), https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/.

[21] Van Geel, M., Vedder, P., Tanilon, J.. "Relationship Between Peer Victimization, Cyberbullying, and Suicide in Children and Adolescents: A Meta-Analysis," *JAMA Pediatrics* 168, no. 5: 435–42, (1 May 2014), https://doi.org/10.1001/jamapediatrics.2013.4143.

[22] Thorn. "Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking." (May 2021), https://info.thorn.org/hubfs/Research/Responding%20to%20Online%20Threats_2021-Full-Report.pdf.

[23] Thorn. "Understanding sexually explicit images, self-produced by children." (9 Dec. 2020), https://www.thorn.org/blog/thorn-research-understanding-sexually-explicit-images-self-produced-by-children/.

they make it more difficult for parents to set limits and for children to disengage, thereby increasing the risk of overuse.

Quantified Popularity

A defining feature of social media is that popularity of individuals and what they post is quantified and displayed publicly for other users to see in the form of friend and follower counts, and tabulated likes, shares, and views. This quantification exploits young people's tendency for social comparison and desire for acceptance, and recreates, on a 24/7 basis, the high school cafeteria experience where everyone can instantly see who the popular and unpopular kids are.

Quantified popularity is extremely effective at getting users to post on platforms, which is essential for maximizing engagement not only for the poster but for everyone in their networks.[24] Children and teens, who are already prone to oversharing, quickly learn that the way to improve these metrics is to post frequently, and to post particularly provocative and risqué content. Adolescent girls report feeling pressure to post sexualized selfies as a means of generating attention and social acceptance from their peers.[25] These posts can create a permanent online record of youthful indiscretions that can limit opportunities later in life, not to mention increase the risk of cyberbullying and sexual exploitation. Similarly, the pressure to demonstrate one's popularity by displaying a high friend count can lead children to accept friend requests from strangers, thereby putting them at risk of grooming and sexual exploitation.

The pursuit of external, quantified popularity also encourages children and teens to attempt dangerous viral challenges, like when Snapchat's speed filter led young people to film themselves driving well over 100 MPH, resulting in many tragic fatal accidents.[26] This past summer, media reports documented how "the blackout challenge" on TikTok, in which young people hold their breath until they pass out, was responsible for the deaths of several children.[27] Likes and shares and the possibility of "going viral" makes attempting these stunts much more appealing to young people.

Personalized Content and Algorithmic Recommendations

Platforms such as YouTube, TikTok, and Instagram serve users content based on automated suggestions. Algorithms choose which content children and teens see based on the vast amount of data they collect on users, such as likes, shares, comments, interests, geolocation, and the videos a user watches and for how long. These algorithms are designed to extend engagement by discerning what video or other content a user is most likely to engage with.[28] For example, a recent internal TikTok document analyzed

---

[24] 5Rights Foundation. "Pathways: How digital design puts children at risk." (July 2021), https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf.

[25] Macheroni, G., Vincent, J., Jimenez, E. "'Girls Are Addicted to Likes so They Post Semi-Naked Selfies': Peer Mediation, Normativity and the Construction of Identity Online," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 9, no. 1 (1 May 2015), https://doi.org/10.5817/CP2015-1-5.

[26] Blanco, Sebastian. "Snapchat removes speed filter blamed for numerous high-speed crashes." *Car and Driver,* (20 June 2021), https://www.caranddriver.com/news/a36777379/snapchat-removes-speed-filter-crashes/

[27] Lee, Anne Marie. "Child deaths blamed on TikTok 'blackout challenge' spark outcry." *CBS News,* (19 Aug. 2021), https://www.cbsnews.com/news/tik-tok-blackout-challenge-child-deaths/

[28] 5Rights Foundation. "Pathways: How digital design puts children at risk." (July 2021), https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf

by *New York Times* columnist Ben Smith revealed that the company optimizes for "time spent" on the app, indicating its algorithms incentivize users to remain on TikTok for as long as possible.[29]

This personalization can harm children not only by driving overuse but by exposing them to content that hasn't undergone any human review. Algorithms drive 70% of viewing on YouTube.[30] As a former YouTube engineer observed: "recommendations are designed to optimize watch time, there is no reason that it shows content that is actually good for kids. It might sometimes, but if it does, it is coincidence."[31] In recent years, many parents have documented how YouTube recommends knockoff versions of cartoons to young children which often contain violent, sexualized and disturbing content.[32]

Algorithmic recommendations can be particularly dangerous when they target children and teens' greatest vulnerabilities. A *Wall Street Journal* investigation documented how TikTok users were served videos that encouraged eating disorders and discussed suicide.[33] And Frances Haugen described how Instagram's algorithm targets users with content based on their interests, even if their interests are eating disorders or self harm: "They develop these feedback cycles where children are using Instagram to self-soothe but then are exposed to more and more content that makes them hate themselves."[34] Her observations were confirmed by an experiment conducted by Senator Blumenthal's office, which created an account for a fake 13 year-old girl that "liked" content about dieting. Within 24 hours, the account was served pro-eating disorder and self-harm content. According to Facebook's own internal research, one in three adolescent girls says Instagram makes their eating disorders worse.[35]

On top of that, algorithmic recommendations have been shown to push dangerous drug content to teen users. A report by the Tech Transparency Project released just this week found that accounts for fake teen users aged 13-17 were able to connect with drug dealers in as little as two clicks.[36]

IV. Apps, websites, and platforms target children with unfair marketing and manipulative monetization techniques.

Another way in which digital platforms harm children is through unfair advertising and monetization practices. Online advertising to children is significantly less regulated than television advertising; there are no limits on the frequency or presentation of ads shown to children. As a result, the websites and

---

[29] Smith, Ben. "How TikTok Reads Your Mind." *The New York Times,* (5 Dec. 2021), https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html?partner=slack&smid=sl-share

[30] Solsman, Joan. "YouTube's AI is the puppet master over most of what you watch." *CNET,* (10 Jan. 2018), https://www.cnet.com/news/youtube-ces-2018-neal-mohan/

[31] Orphanides, K.G. "Children's YouTube is still churning out blood, suicide and cannibalism." *Wired,* (23 March 2018), https://www.wired.co.uk/article/youtube-for-kids-videos-problems-algorithm-recommend

[32] Bridle, James. "How Peppa Pig became a video nightmare for children." *The Guardian,* (17 June 2018), https://www.theguardian.com/technology/2018/jun/17/peppa-pig-youtube-weird-algorithms-automated-content

[33] Wall Street Journal Staff. "Inside TikTok's Algorithm: A WSJ Video Investigation." *Wall Street Journal,* (21 July 2021), https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477

[34] Pelley, Scott. "Whistleblower: Facebook is misleading the public on progress against hate speech, violence, misinformation." *CBS: 60 Minutes,* (4 Oct. 2021), https://youtu.be/_Lx5VmAdZSI

[35] Wells, Georgia, et al. "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show." *The Wall Street Journal* (14 Sept. 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[36] *Tech Transparency Project.* "Xanax, Ecstasy, and Opioids: Instagram Offers Drug Pipeline to Kids." (7 Dec. 2021), https://www.techtransparencyproject.org/articles/xanax-ecstasy-and-opioids-instagram-offers-drug-pipeline-kids

apps used by young children contain a high frequency of ads, often shown in manipulative ways, as well as other commercial content. In addition, online advertising is frequently harder for children to identify, making young people more vulnerable to the marketing they encounter online as compared to traditional television advertising.[37]

More than 95% of early childhood videos on YouTube contain ads, and one in five videos viewed by children 8 and under contained ads that were not age-appropriate, such as ads that featured violent or sexualized content.[38] Researchers who studied preschool apps found a high prevalence of age-inappropriate ads, and 54% of apps contained disruptive pop-up advertisements or ads that the child user couldn't easily close.[39] Another analysis found that the educational potential of children's apps is severely degraded by the high number of disruptive ads that appear, particularly in free apps more likely to be used by low-income children.[40]

Surveillance Advertising

Surveillance advertising – targeted advertising using personal data provided by websites and platforms – is the dominant form of marketing online. As Fairplay, Global Action Plan, and Reset Australia described in a recent report about Facebook, surveillance ads are inherently unfair when targeted to children:

> On the one side is a child, poorly equipped to distinguish between advertising and information, especially within digital contexts. On the other, Facebook with its vast troves of data about the child, including but not limited to their browsing history, mood, insecurities, their peers' interests, and more. This power imbalance makes surveillance advertising inherently more manipulative than contextual digital advertising, let alone traditional analogue advertising.[41]

As with personalizing content, surveillance ads can be used to target and exacerbate young people's vulnerabilities. Ads for risky "Flat Tummy Teas" and dangerous exercise routines target young women on Instagram. Researchers were able to target ads to teenagers on Facebook based on their interests in gambling, alcohol, and dieting.[42] While Facebook has since restricted advertisers' ability to target teens

---

[37] Owen, L., Lewis, C., Auty, S., Buijzen, M., "Is children's understanding of non–traditional advertising comparable to their understanding of television advertising?" *Journal Public Policy Mark.* 32(2):195–206 (2012), https://journals.sagepub.com/doi/abs/10.1509/jppm.09.003

[38] Radesky, J. S., Schaller, A., Yeo, S. L., Weeks, H. M., & Robb, M.B. "Young kids and YouTube: How ads, toys, and games dominate viewing." *Common Sense Media,* (2020), https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/research/2020_youngkidsyoutube-report_final-release_forweb.pdf

[39] Meyer M, Adkins V, Yuan N, Weeks HM, Chang YJ, Radesky J. "Advertising in Young Children's Apps: A Content Analysis." *J Dev Behav Pediatr,* (Jan. 2019), https://pubmed.ncbi.nlm.nih.gov/30371646/

[40] Meyer, M., Zosh, J.M., McLaren, C., Robb, M., McCaffery, H., Golinkoff, R.M., Hirsh-Pasek, K., & Radesky, J. "How educational are "educational" apps for young children? App store content analysis using the Four Pillars of Learning framework." *Journal of Children and Media*, (2021), https://www.tandfonline.com/doi/abs/10.1080/17482798.2021.1882516?journalCode=rchm20

[41] Yi-ching Ho, E., Farthing, R. "How Facebook still target surveillance ads to teens." *Reset Australia, Fairplay, and Global Action Plan.* (Nov. 2021), https://fairplayforkids.org/wp-content/uploads/2021/11/fbsurveillancereport.pdf

[42] Farthing, Rys, et al. "Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data." *Reset Australia,* (April 2021), https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf

based on their interests, the company's ad targeting algorithm still uses the data it collects on young people to determine who is most likely to be vulnerable to a given ad.[43]

Even in cases where the products aren't as harmful as alcohol or dieting aids, surveillance advertising exploits children. As Common Sense notes, "Kids may be profiled as gamers, impulsive purchasers, or anxious oversharers – and then unfairly targeted by ads that encourage more of these things."[44]

While the Children's Online Privacy Protection Act (COPPA) prohibits collecting and using the data of a child under the age of 13 for targeted advertising and other purposes without advance verifiable parental consent, the law is rarely enforced. In the 21 years that the COPPA Rule has been in effect, the FTC has brought only 35 enforcement actions. Often, settlements merely required the defendant to comply with the law and file periodic reports with the FTC. When the FTC has assessed civil penalties, they have been woefully insufficient to incentivize compliance with COPPA. Given this lack of enforcement, it is not surprising that COPPA violations are rampant. Studies of Android apps directed to and played by young children have found that more than 50% share children's personal information with third parties, including advertisers, in clear violation of the law.

Influencer Marketing

It has long been understood that children are better able to identify advertising when it is clearly separated from programming. That's why product placement and host selling are prohibited on children's television. Yet no such prohibitions exist on the internet and therefore influencer marketing to children and teens is ubiquitous.

Almost half of videos watched by children eight and younger on YouTube featured or promoted products for children to buy.[45] In fact, unboxing videos – where toy companies or retailers compensate a child YouTuber for excitedly talking about a toy – are among the most popular and most recommended videos on YouTube. Children have no idea that the videos they are watching, which are often more than ten minutes long, are essentially infomercials. Instead, they think they're watching a friend talk about a toy they really like. Not surprisingly, unboxing videos are incredibly effective from an advertiser's point-of-view. Children who watch unboxing videos are more likely to nag their parents for products and throw a tantrum if the answer is "no" than when they watch regular commercials.[46]

Similarly, older children and teens are targeted by influencers who post clips telling where to buy outfits like theirs. And junk food marketers like Burger King and Doritos target kids and teens with commercialized dance "challenges" on TikTok. The toy industry is also increasingly using influencers to

---

[43] *Ibid.*

[44] Jerome, Joseph and Johnson, Ariel Fox. "AdTech and Kids: Behavioral Ads Need a Time-Out" *Common Sense,* (2021), https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/AdTech%20and%20Kids.pdf

[45] Radesky, J. S., Schaller, A., Yeo, S. L., Weeks, H. M., & Robb, M.B. "Young kids and YouTube: How ads, toys, and games dominate viewing." *Common Sense, (*2020), https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/research/2020_youngkidsyoutube-report_final-release_forweb.pdf

[46] Marshall, Lisa. "Unboxing videos fueling kids' tantrums, breeding consumerism." *CU Boulder Today,* (3 Dec. 2019), https://www.colorado.edu/today/2019/12/03/unboxing-videos-fueling-kids-tantrums-breeding-consumerism

market to children on TikTok, taking advantage of the fact that TikTok does little to enforce its own terms of service that say users must be at least 13 years-old.[47]

Manipulative In-game Purchases

In addition to advertising, in-game purchases are a primary way children and teens are monetized online. Most online games and apps now use a "freemium" model where users can download a game for free or a nominal cost and then have to pay for add-ons. Some add-ons are essential to advance in the game while others are for coveted cosmetic items for game characters, such as Fortnite skins. In almost all cases, developers use unfair pressure and manipulation to get kids to make – or ask their parents for – in-game purchases. Apps targeted to teenagers are more than 3 times as likely to have in-app purchases as apps targeted to general audiences.[48]

Apps aimed at young children often leverage their parasocial relationships with the games' characters in order to promote in-game purchases. The characters directly exhort children to make purchases and express disappointment when they don't. A forthcoming analysis of apps popular with young children found that of apps that feature characters, nearly 29% use "parasocial relationship abuse" to drive purchases.[49] For example, the Buddy character in *Kick the Buddy* says "don't just stand there, buy something!" when the player is on the store page.[50] In the popular preschool app *Doctor Kids,* the main character cries if kids click away from the store without making a purchase. [51] In other words, the app developer is deliberately trying to make kids feel like they are hurting a friend if their parents are unwilling or unable to make a purchase. Parasocial relationship abuse is also used to extend engagement in nearly a quarter of apps played by young children, with characters pressuring players to keep going or expressing disapproval if they stop.

Apps popular with young children also tease players by showing them attractive game items or prizes that can't be accessed without a purchase. This practice is used extensively by the popular math game Prodigy, which has been assigned by more than 90,000 schools for homework, in order to sell pricey Premium memberships. For example, when children successfully answer a math problem, they are presented with two treasure boxes: a plain wooden one and a sparkly blue one. When kids without Premium memberships click on the sparkly blue box, their choice is denied and they are blocked from finding out what's inside. Instead, they are presented with an ad for a Premium membership, which presently costs $75 for one year, and kids who don't upgrade at that moment must settle for the wooden box.[52] To make matters worse, when they play at school, students can see who does and

---

[47] Chang, Brittany. "TikTok is quickly becoming a marketing destination for toy companies with the help of influencers and original content." *Business Insider.* (19 Dec. 2020), https://www.businessinsider.com/tiktok-quickly-becoming-marketing-destination-for-toy-companies-2020-12?utm_source=pocket_mylist

[48] BBB National Programs. "Risky Business: The current State of Tenn Privacy in the Android App Marketplace." (2020), https://industryselfregulation.org/docs/librariesprovider5/default-document-library/tapp_whitepaper.pdf

[49] Radesky, J., Hiniker, A. et al. "Design abuses in children's apps." Forthcoming.

[50] *Ibid.*

[51] Meyer M, Adkins V, Yuan N, Weeks HM, Chang YJ, Radesky J. "Advertising in Young Children's Apps: A Content Analysis." *J Dev Behav Pediatr,* (Jan. 2019), https://pubmed.ncbi.nlm.nih.gov/30371646/

[52] Campaign for a Commercial-Free Childhood (now Fairplay). "Request for Investigation of Deceptive and Unfair Practices by the Edtech Platform Prodigy." *Campaign for a Commercial-Free Childhood before the Federal Trade Commission.* (19 Feb. 2020). https://fairplayforkids.org/wp-content/uploads/2021/02/Prodigy_Complaint_Feb21.pdf

doesn't have Premium memberships and the associated perks, thereby creating a new form of educational inequity.

Platforms and games such as Roblox and Fortnite frequently require players to purchase virtual currencies in order to purchase in-game items. These virtual currencies have no fixed value to actual money (i.e. the conversion rate is better the more currency you buy). It is unrealistic to expect a child who is a concrete thinker to understand the complexities and abstractions of a currency with no fixed value. In addition, games often use dark patterns to get children to buy more virtual currency. For example, game items are priced so that children will have leftover currency but not enough to buy another item, making their remaining virtual currency worthless unless they buy more.[53] Not surprisingly, given these high levels of manipulation and abstraction, children spend lots of money on in-game purchases, with some racking up bills in the thousands of dollars.[54]

V. Congress must take action to build a better internet for children and teens.

Nearly every concern that parents, public health professionals, and children themselves have about digital media platforms can be traced to deliberate design choices. It doesn't have to be this way. Apps and online platforms could instead be built to reduce risks and increase safeguards for children.

But that won't happen without significant action from Congress. COPPA – the only federal law that protects children online – was passed 23 years ago, long before smartphones, Instagram, and YouTube even existed. Congress's continued inaction, combined with a lack of enforcement by the FTC, has emboldened Big Tech to develop an exploitative business model without considering or mitigating its harmful effects on children and teens. It's no wonder polls consistently show parents want Congress to do more to protect children online.[55]

When kids are in digital spaces for learning, socializing, and relaxing, they deserve the opportunity for the most positive experience, designed in a way that understands and supports their unique ways of seeing the world. They should be able to explore in developmentally-appropriate ways without being manipulated into spending more time online, spending more money, watching more ads, or surrendering more data. That's exactly why we need a US design code – rules and laws to ensure that any digital services children use are safe and fit for them.

A design code, like the UK's recently implemented Age Appropriate Design Code, is an upstream approach that requires making the best interests of children a primary consideration when designing an online service likely to be accessed by children and teens. It requires tech companies to think about what children need and how to reduce risks in their products. A code would prohibit harmful data

---

[53] Rosenbloom, Michael. "Request for Public Comment on the Federal Trade Commission's Request for Comments Regarding Topics to be Discussed at Dark Patterns Workshop." (27 May 2021), https://www.democraticmedia.org/sites/default/files/field/public-files/2021/ccfc-cdd_dark_patterns_comments_05-28-2021.pdf

[54] Kleinman, Zoe. "My son spent £3,160 in one game." *BBC News* (15 July 2019), https://www.bbc.com/news/technology-48925623

[55] Klar, Rebecca. "Most voters support new rules for social media companies on children, personal data: poll." *The Hill,* (18 Nov. 2021), ttps://thehill.com/policy/technology/582013-most-voters-support-new-rules-for-social-media-companies-on-children

processing and design choices and require tech companies to regularly assess how their services are impacting children.

Just as companies currently design their services to prioritize profits and engagement over children's wellbeing, these same services *could* be designed in a way that puts children first. It shouldn't be up to tech companies to decide if they want to make risky design choices for children or not.

Fortunately, there are already two legislative solutions under consideration by this Subcommittee which, taken together, would create the foundations of a design code for America's children. The KIDS Act, which we will discuss today, would prohibit companies from deploying design techniques that extend engagement on children and teens, such as autoplay, nudges, and rewards like Snapstreaks. It would ban, for children under 16, the public displays of quantified popularity that drive overuse of social media, trigger social comparison, and encourage provocative posting. It would prohibit websites from amplifying harmful content to children and young teens. It would prevent operators from manipulating children into making in-game and in-app purchases. And it would prohibit websites from recommending content that includes influencer marketing, such as unboxing videos, to children under 16.

While the KIDS Act would stop online operators from targeting children and teens with manipulative design, deceptive advertising, and harmful content, the Protecting the Information of our Vulnerable Children and Youth (PRIVCY) Act would give young people the 21st century privacy protections they deserve. It expands privacy protections to teens and bans harmful uses of data like surveillance advertising. The PRIVCY Act also incorporates key elements of the UK's groundbreaking Age Appropriate Design Code, including requiring platforms to make the best interests of children a primary design consideration and to conduct regular risk assessments. And to address the crisis of enforcement, it creates a Youth Marketing and Privacy Division at the FTC.

Together, these bills would create the safeguards children need and transform the online experience for young people.

VI. Conclusion

Over the last year, Congress has convened a number of critical hearings on children's online experiences and the responsibilities of Big Tech. It has been heartening to hear members of Congress speak first and foremost, not as Republicans or Democrats, but as parents and grandparents with first-hand knowledge of what's at stake.

But the American people need more than your understanding and justifiable anger at companies like Facebook. Big Tech is banking on the fact that partisan divisions will keep you from taking real action. I hope you prove them wrong and advance legislative solutions that better protect children while they're online *and* make it easier for them to disconnect and engage in the offline experiences they need to thrive. There is simply too much at stake for children and for their futures to allow the status quo to continue.

Thank you again for having me here today and I look forward to discussing all of this with you.

Ms. SCHAKOWSKY. Well, thank you.
And now, Ms. Rich, you are recognized for 5 minutes.

STATEMENT OF JESSICA RICH

Ms. RICH. Chair Schakowsky, Ranking Member Bilirakis, and members of this subcommittee, I am Jessica Rich, of counsel at Kelley Drye, and a distinguished fellow at Georgetown University. I am pleased to be here today testifying on holding Big Tech accountable, and building a safer internet. My remarks today are my own, based on my years of government service.

My background is as a law enforcement attorney and official. I worked for over 26 years at the Federal Trade Commission, the last 4 as director of its Bureau of Consumer Protection. Before becoming director, I was the first and longtime manager of the FTC's privacy program. I have supported stronger data privacy and security laws for over 20 years. The focus of my testimony today is on that very issue: privacy.

While I understand that privacy is not the chief focus of this hearing, I am highlighting it today because the need for privacy legislation, Federal privacy legislation, has never been stronger. This hearing is addressing many important issues, some of which are closely related to privacy. But passing a strong and comprehensive private—Federal privacy law is one of the most important things Congress can do to hold Big Tech accountable, and build a safer internet.

Consumers, businesses, regulators, and the marketplace as a whole, we all need a Federal privacy law.

First, survey upon survey shows that consumers are concerned about their privacy, and believe they have little control about how companies collect, use, and share their personal information. They continue to be the victims of massive data breaches. Data collection and abuses are everywhere. And companies make decisions affecting them every day using algorithms and profiles with built-in assumption and biases.

You can't educate consumers about their rights, because it depends on the market sector, the state they are in, and the type of company and the data involved. Often, consumers have no rights at all. And consumers can't be expected to read hundreds of privacy policies a day from companies they have never heard of. Consumers need a clear and consistent privacy law that they can understand and rely on every day, no matter where they are or what they are doing.

Businesses are similarly confused about privacy laws in this country. At the Federal level, we have the FTC Act, as well as dozens of sector-specific laws like COPPA, HIPAA, and the Fair Credit Reporting Act. We also now have three comprehensive state laws, with more on the way.

Honest companies spent enormous time and money to navigate all these laws, while the unscrupulous exploit the gaps and the loopholes. Meanwhile, large companies have benefited. That includes the platforms, because they can afford the cost of compliance, and because many existing laws favor large entities that can keep their operations in house, and not share data with third parties.

In sum, businesses too need a clear and consistent Federal privacy law to help them navigate a difficult regulatory environment, and create a more level playing field.

But there is more. For over 20 years, the FTC, my former agency, has overseen privacy using a law that is just not up to the task: the FTC Act. While the FTC has accomplished a lot, this law does not establish clear standards for everyone to follow before problems occur, and there are big gaps in its protections, creating uncertainty for the marketplace.

Many in Congress on both sides of the aisle have criticized the FTC for these problems: too strong, too weak, too much, too little. But, with respect, it is Congress that needs to fix the problems by passing a law with clear standards for the FTC and the public.

Finally, we now, all of us, understand that concerns surrounding the use of personal data reach well beyond traditional notions of privacy to issues like discrimination, algorithmic fairness, accountability, whistleblower protections, dark patterns, protecting our kids, data portability, and even, with respect to data security, our critical infrastructure. A privacy law could address many of these issues, at least in part, achieving far more than could be achieved by adding yet more sectoral requirements to the confusing mix of laws we now have in the United States.

Thank you so much for inviting me here today. I stand ready to assist the subcommittee and its members and staff with ongoing work related to consumer protection and privacy.

[The prepared statement of Ms. Rich follows:]

STATEMENT OF JESSICA L. RICH

Of Counsel, Kelley Drye & Warren
Distinguished Fellow, Georgetown Institute for Technology Law and Policy

Before the

Subcommittee on Consumer Protection and Commerce
Committee on Energy and Commerce
United State House of Representatives

On

"HOLDING BIG TECH ACCOUNTABLE:
LEGISLATION TO BUILD A SAFER INTERNET"

December 9, 2021

I. INTRODUCTION AND BACKGROUND

Chair Schakowsky, Ranking Member Bilirakis, and members of this Subcommittee, I am Jessica L. Rich, Of Counsel at Kelley Drye & Warren and a Distinguished Fellow at Georgetown University. I am pleased to be here today, testifying before this Committee on holding big tech accountable and building a safer internet. I want to thank this Committee for its leadership and ongoing efforts on consumer protection, privacy, and related issues. I also want to make clear that my remarks today are my own, based largely on my years of experience in government service.

My background is as a lawyer and law enforcement official. I worked for over 26 years at the Federal Trade Commission (FTC), the last four as Director of the Bureau of Consumer Protection overseeing the agency's efforts to protect consumers from illegal marketing, advertising, and privacy practices. Earlier in my FTC career, I launched the agency's very first work to protect consumer privacy and data security, and then led and expanded these efforts for over a decade – bringing cases against numerous companies that failed to protect consumers' personal information, and developing rules to implement the Gramm Leach Bliley Act (GLB),[1] Children's Online Privacy Protection Act (COPPA),[2] and Fair and Accurate Credit Transaction Act.[3] In 2000, I led the FTC team that wrote the first of many reports to Congress[4] seeking stronger legal authority and remedies for privacy – and I have testified, spoken publicly, and written many articles pleading the same case since.

II. THE NEED FOR A COMPREHENSIVE FEDERAL PRIVACY LAW

The focus of my testimony today is on that very issue – privacy. For over two decades, Congress has debated whether to pass a comprehensive data privacy law. Scores of bills have come and gone with no action. Meanwhile, Europe and many other countries have moved ahead to enact detailed data protection regulations, and three states (California, Virginia, and Colorado) have done the

---

1 15 U.S.C. § 6801 et seq.
2 15 U.S.C. § 6501 et seq.
3 15 U.S.C. § 1681 et seq.
4 *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (FTC, May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

same, adding to the cacophony of privacy laws that exists across jurisdictions, market sectors, and topic areas.

I understand that privacy is not the chief focus of this hearing. However, I am highlighting this issue in my testimony because the need for federal privacy legislation has never been greater; because many of the issues being considered at this hearing could be addressed, at least partially, in a privacy law; and because a privacy law would advance some of Congress' broader goals regarding the tech platforms and marketplace fairness.

Put simply (and borrowing from the title of this hearing), I believe that passing a federal privacy law is one of the most important things that Congress could do to "hold big tech companies accountable" and "build a safer internet." Further, given the progress made during the past two years on this issue – in both the House and the Senate – success should be within reach.

Here are some of the reasons why federal privacy legislation is needed now:

For Consumers

Survey upon survey shows that consumers are concerned and confused about their privacy and believe that they have little control about how companies collect, use, and share their personal information.[5] For good reason. In recent years, consumers have been the victims of massive and continuing data breaches,[6] data collection and abuses have exploded online,[7] and companies have increasingly made decisions about individuals using algorithms and profiles that predict consumers' behavior based on assumptions and stereotypes.[8]

---

[5] See *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information* (Pew Research Center, Nov. 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[6] See *The 60 Biggest Data Breaches* (Upguard, Dec. 2021), https://www.upguard.com/blog/biggest-data-breaches.

[7] See *Privacy International*, https://privacyinternational.org/examples.

[8] See *Algorithmic Bias Detection and Mitigation* (Brookings, May 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

Incredibly, as this Subcommittee knows, there is no law that protects consumer privacy nationwide. Instead, there are multiple laws that apply to certain sectors, jurisdictions, entities, and fact patterns.[9] If consumers want to decipher how companies collect and use their data, they need to read hundreds of lengthy privacy policies – often confusing, incomplete, and/or from companies they have never heard of. Further, without consistent rules governing consumer privacy, it is impossible to educate consumers about their rights, and thus enlist them in policing the marketplace, because their rights (or lack thereof) depend on the situation.

Consumers need a clear and consistent privacy law that they can rely on to protect them across jurisdictions and market sectors. Passing one would help build a safer internet.

For Businesses

Businesses are similarly confused about our privacy laws. Even as gaps in these laws leave consumers largely unprotected, they impose a huge compliance burden on companies trying to understand and follow them. At the federal level, we have the FTC Act, as well as numerous sector-specific laws – a veritable alphabet soup that includes COPPA, HIPAA, FCRA, GLBA, TCPA, FERPA, ECPA, CAN-SPAM, CPPA (the federal one), VPPA, GINA, and the CPNI rules. At the state level, there are the three state-wide laws mentioned above (with likely more to come), and yet again more sector-specific laws. For multinational companies, we have the General Data Protection Regulation (GDPR) and many other foreign laws and rules.

The lack of consistent standards allows the unscrupulous to exploit gaps and loopholes, disadvantaging honest companies. Further, the cost of navigating multiple laws and regulations benefits the tech platforms and other large companies that have the funds to afford it. So, too, does the emphasis in many existing laws on stopping third-party sharing (as opposed to stopping data abuses by everyone) because large companies have greater ability than small ones to keep their operations in-house.

---

[9] See *Data Protection: An Overview* (Congressional Research Service, March 2019), https://crsreports.congress.gov/product/pdf/R/R45631.

Businesses need a clear and consistent federal privacy law to help them navigate a difficult regulatory environment. Even if existing laws remain on the books, a federal law can create a more coherent framework for compliance. A federal law also could create a level playing field by imposing the same rules on everyone, and avoiding the pitfalls that have given advantages to the tech platforms and other large companies.

For Enforcers

The lack of clear privacy standards has undermined the FTC too – the nation's chief privacy enforcer at the federal level. Since the late 90s, most of the FTC's privacy efforts have been based on Section 5 of the FTC Act,[10] a law that was not designed for this purpose and is ill-suited for it in many ways. Among other things, the law does not establish clear standards for everyone to follow before problems occur – it is largely reactive. It does not cover non-profits, or companies engaged in common carrier activities. It does not authorize civil penalties for first time violations. And now, after the Supreme Court's ruling in the *AMG* case, the law does not even allow the FTC to seek monetary relief in federal court under Section 13(b).

Despite the shortcomings of the law, the FTC has brought hundreds of cases and obtained record-breaking settlements against companies that have misrepresented their data practices or used data in ways that impose significant harm.[11] Nevertheless, with adequate legal authority (and resources) conferred by a federal law, the FTC could be much more effective in investigating, studying, and putting a stop to harmful data practices. Empowering the State Attorneys General authority to enforce the law would enhance this effectiveness even further.

While some have suggested that the FTC simply write its own privacy rules using its Section 5 (Magnuson-Moss) rulemaking authority, such an effort is unlikely to succeed – or at least unlikely to produce the comprehensive and credible rules that are needed here. Magnuson-Moss rulemaking is an arduous process – requiring proof of deception or unfairness, as well as prevalence, for every

---

[10] 15 U.S.C. §§ 41-58.

[11] See FTC *Privacy and Security Cases and Proceedings,* https://www.ftc.gov/enforcement/cases-proceedings/terms/245%2B247%2B249%2B262.

mandate, and imposing hearings, paperwork, and other hurdles every step of the way.[12] Many rules, less complicated than privacy, have taken years to complete.[13] Further, after all of these years of debate, Congress needs to make the tough decisions to ensure acceptance (and not endless lawsuits) among the broad range of affected stakeholders.

In addition, while the Build Back Better bill would provide privacy resources that the FTC now lacks, clearer direction from Congress is needed to ensure that the FTC has sufficient authority and credibility to be the nation's lead privacy enforcer.

To Advance Related Goals Embraced by this Subcommittee and Many Others

The benefits discussed above would assist consumers and businesses, promote a level playing field in the marketplace, and strengthen the hands of the FTC and State AGs. Accomplishing these goals would be significant and historic for both data protection and competition in this country.

But there's more. In recent years, policymakers and the public have come to accept that the issues surrounding the use of personal data reach well beyond traditional notions of privacy – to issues like discrimination, algorithmic fairness, accountability, and whistleblower protections, some of the very issues being considered at this hearing. In addition, imposing data security requirements on commercial entities – a key feature in any privacy bill – is important to protecting our critical infrastructure, given its connections to commercial systems.[14] Finally, passing a federal privacy law would help strengthen the U.S.' position internationally – in negotiations about U.S.- EU data transfers and similar matters.[15]

---

[12] 15 U.S.C. § 57a.

[13] See Credit Practices Rule, 40 Fed. Reg. 16,347 (proposed Apr. 11, 1975); 49 Fed. Reg. 7740 (issued Mar. 1, 1984; codified at 16 CFR pt. 444); Sale of Used Motor Vehicles, 41 Fed. Reg. 1089 (proposed Jan. 6, 1976); 49 Fed. Reg. 45,692 (issued Nov. 19, 1984, codified at 16 CFR pt. 455).

[14] See *Critical Infrastructure Sector Partnerships*, https://www.cisa.gov/critical-infrastructure-sector-partnerships.

[15] See *U.S.-EU Privacy Shield and Transatlantic Flows* (Congressional Research Service, Sept. 2021), https://crsreports.congress.gov/product/pdf/R/R46917.

In short, this Subcommittee and Congress as a whole can achieve many important goals by enacting a federal privacy law – more than can be achieved by adding yet more sectoral requirements to the confusing mix of current laws now governing U.S. data and technology.

III. CONCLUSION

Thank you for inviting me here today. I stand ready to assist the Subcommittee and its members and staff with its ongoing work related to consumer protection and privacy.

Ms. SCHAKOWSKY. Thank you very much.

And last, but certainly not least, Mr. Ahmed, you are recognized now for 5 minutes.

STATEMENT OF IMRAN AHMED

Mr. AHMED. Chairs Schakowsky and Pallone, Ranking Members Bilirakis and McMorris Rodgers, members of the committee, thank you for this opportunity to appear before you today.

The Center for Countering Digital Hate, CCDH, is a nonprofit research in the dynamics of misinformation and hate on social media, how it undermines democracy, the rule of law, child safety, and our ability to deal with life-threatening crises such as COVID.

So why is this happening? Why are we here? The ugly truth is social media companies discovered prioritizing hate, misinformation, conflict, and anger is highly profitable. It keeps users addicted, so they can serve them ads.

CCDH's research has documented bad actors causing harm, but also bad platforms encouraging, amplifying, and profiting from that harm. The platforms have managed to successfully stop any credible action by deploying a well-worn playbook: one, initially deny there is a problem; two, admit there is a problem, but deflect responsibility; three, finally, acknowledge responsibility, but delay any action. Deny, deflect, delay. I can show you how that works in practice.

On March the 24th we released a report showing that up to 65 percent of anti-vax content circulating on Facebook and Twitter, 65 percent, originates with sites and accounts operated by just 12 anti-vaxxers, the Disinformation Dozen. Now, this committee asked Mark Zuckerberg about the report in a hearing the next day, on March the 25th. He promised to do something about it. He did not.

Six months later, after the surgeon general and the President weighed in—again, citing our report—Facebook responded, claiming our report had a faulty narrative. However, Facebook whistleblower Frances Haugen revealed that, on the very same day we released our report, March the 24th, Facebook produced an internal study confirming that a tiny number of accounts were responsible for more than half of anti-vaccine content on their platform. So they were lying, while the American public were suffering under COVID, and people were dying.

The members of this committee have seen the same tactics from social media executives time and time again. You have correctly determined, as have legislators in the UK, Australia, Germany, and other allied nations, that social media companies cannot self-regulate, and that we need new legislation.

There is no silver bullet. That is right. Section 230 shows the limitations to a single solution based on one core principle. It did not predict nor deal with the harms we are now seeing emanating from social media. There will need to be a range of approaches to transparency and accountability to nudge social media into a place that balances dialogue, privacy, safety, and prosperity.

The bills being considered today would collectively represent a big step forward to protecting children, families, society, and our democracies. The KIDS Act would put real protections in place for our children.

Transparency is an essential tool in countering online hate and lies. The Social Media Data Act, therefore, would give independent researchers the access needed to detect dangerous trends.

Whistle blowers have leaked internal documents illuminating wrongdoing by Big Tech, providing new urgency to the reform debate. But whistleblowing is still profoundly risky for the whistleblower, which is why the incentives and protections provided by the FTC Whistleblower Act are critical.

Social media apps trick users very often into giving up their personal data, their thoughts, their fears, their likes, their dislikes, which they then sell to advertisers. Big Tech's big data is designed to exploit people, not to serve them better. The DETOUR Act puts a stop to that destructive spiral.

There are also two much-needed bills to address the growing threat of hostile foreign actors who revel in the divisions that social media creates and exacerbates in democratic societies. In approving these bills, the committee would take a huge step forwards towards better regulation, and give us hope that an internet that brings out the best in people is possible.

Thank you very much.

[The prepared statement of Mr. Ahmed follows:]

Subcommittee Chairwoman Schakowsky, Ranking Member Bilirakis, and members of the Committee.

Thank you for this opportunity to appear before you today.

The Center for Countering Digital Hate (CCDH) is a non-profit researching how bad actors spread hate and misinformation on social media with impunity using increasingly sophisticated tactics and strategies undermining democracy, rule of law, the mental health of children, and our ability to deal with life-threatening crises, such as COVID and climate change.

Why?

Keeping people agitated, angered, emotional, enthralled and addicted to their ad-and-profit-pumping platforms yields enormous profits for social media companies.

CCDH's research has documented how, instead of taking responsibility, these companies stick to a well-worn playbook when confronted with the harm caused by their platforms.

It goes like this. Initially, *deny* there's a problem. Then admit there's a problem but *deflect* responsibility. Finally, acknowledge responsibility, but *delay* any action.

Deny, deflect, delay.

We ourselves can document such a case - one involving a threat to thousands of American lives.

On March 24, CCDH released a report showing that up to 65 percent of anti-vaccine content circulating on Facebook and Twitter originates with sites and social media accounts operated by just 12 anti-vaxxers - the Disinformation Dozen.

This Committee asked Mark Zuckerberg about the report in a hearing on March 25th. He promised to look into it.

But a month later, our researchers found that the Disinformation Dozen had continued to operate with impunity on his platforms.

Six months later, after the Surgeon General and the President of the United States cited our report, Facebook executives officially responded to our research, claiming it was based on a "faulty narrative."

However, we now know from documents disclosed by Facebook whistleblower Frances Haugen that on March 24, the very same day CCDH released the Disinformation Dozen report, Facebook had produced internal research confirming that a tiny number of accounts were responsible for more than half of anti-vaccine content on the platform.

To this day Mr. Zuckerberg's company has not accepted its share of the responsibility by taking comprehensive action.

Meanwhile, hospitals throughout the country are packed with unvaccinated COVID-19 patients telling their doctors they would have taken the vaccine but for content spread by members of the Disinformation Dozen, most of whom are *still* allowed to use Facebook to disseminate vaccine lies. Some of those patients will not survive the night.

The members of this Committee have seen the same tactics - deny, deflect, and delay - from social media executives time and time again.

You have correctly determined that social media companies are woefully incapable of self-regulation and that the time to act is now.

The bills being considered today would collectively represent an enormous step forward to protecting children, families, society, and democracy.

There is no group more vulnerable online than children, yet social media companies are developing ever-more sophisticated ways to hook children at an early age to their apps. *The KIDS Act* would finally put real and much-needed protections in place for kids...

Transparency is an essential tool in fighting online hate and disinformation, but Big Tech execs simply shut all of us out.

Why?

Because right now they can.

The Social Media DATA Act would give researchers access that's needed to better detect dangerous trends.

The whistleblowers that have come forward to reveal ugly truths about Big Tech are heroes; their actions have provided new urgency to the reform debate.

There need to be easier avenues to expose wrongdoing, which is why the incentives and protections provided by the *FTC Whistleblower Act* are so critical.

Social media apps are rigged to trick users into giving up their personal data.

The more data Big Tech has on you, the more ways they can exploit you.

The DETOUR Act would finally put a stop to this destructive spiral.

There is also today the consideration of two much-needed bills to address the growing threat of hostile foreign actors who revel in the divisions that social media has inculcated in the societies they purport to serve.

Today, there are no rules, no transparency, and no accountability for Big Tech.

By approving these bills, this Committee will provide hope that an internet that brings out the best in people is possible.

Thank you and I look forward to answering your questions.

Ms. SCHAKOWSKY. Thank you very much. We have now concluded the incredible—and I am so grateful for the witness testimony, and their opening statements are finished.

And at this time we will move to member questions. Each member will have 5 minutes to question our witnesses. I will start by recognizing myself for 5 minutes.

Let me begin by saying the Federal Trade Commission is the top regulatory agency tasked with keeping Americans safe online by preventing unfair and deceptive practices. But the FTC stands out from many other regulatory agencies because whistleblowers are not protected by Federal law.

Recent events, as we have seen with Frances Haugen, have made it clear how important whistleblower protection really is, and that is why I introduced the FTC Whistleblower Act and—along with Lori Trahan, my colleague. This legislation protects whistleblowers from retaliation for coming—that is, coming forward.

And I wanted to get the opinion of some of our witnesses.

It also incentivizes—and Mr. Ahmed, you mentioned incentivization—to make sure that these harms are not present there. And I wondered if you could comment on—a little bit more on, you know, whether or not and why you believe that the FTC Whistleblower Act would actually help deter social media companies from making business decisions that could be harmful for consumers.

Mr. AHMED. Well, thank you. Yes, I mean, Frances Haugen turned on the floodlights, so to speak, within Facebook. But what she did can't easily be replicated.

For one thing, it is incredibly expensive. She had lawyers. You know, there is government affairs, there is the loss of income. And her real value, the reason it is so important, is that she really exposed deception, active deception by social media companies, something that can't easily be replicated with any other mechanism beyond whistleblowing. So, you know, the only way to cast a light on that deception is for moral people to shed light on immorality from within.

But the window of a whistleblower like Frances Haugen is limited. Think that, since she took all these documents, they have evolved into Meta, they have moved into the metaverse. Most of the anti-vax crisis has happened since then. And we need disclosure of deceit not every decade, but every time that there is active deceit on something of great public interest.

So this bill is incredibly important in bringing forward more moral characters when we need them.

Ms. SCHAKOWSKY. Thank you.

Mr. Greenblatt, in your view, would this legislation, do you think, work in favor of protecting consumers and ending some of the spreading of the harms that are done?

Mr. GREENBLATT. Yes, Madam Chairman. I think there is no question that the Whistleblower Act is necessary.

I mean, to build upon what Mr. Ahmed just said, what we know is—I mean, I have had direct conversations with Mark Zuckerberg and other Facebook executives, and they have lied to my face. They have lied to you, they have lied to their advertisers, they have lied to the public.

But let's be clear. Silicon Valley is a clicky place. It is not easy. And so we need to give these people the protections that they need, so they don't risk being in violation of their NDAs, they don't risk future opportunities for employment.

But I think, again, if we are playing the long game here, we need to realize the moral leadership and the courage displayed by people like, again, Frances Haugen—but think about it. We learned, because of her bravery, that Facebook is only tackling three to five percent of the hate speech on their platform, despite their protestations. We learned that they—their AI gets less than—wait for it—one percent of the incitements to violence on their platform. The reason why this has prevailed for so long is they are exempt from liability, and lack the incentives.

So, Madam Chairman, unless we have the means to protect the people who have access to this information, it is clear the companies will not volunteer it to us. So I think it is vital that your Act, the whistleblower—FTC Whistleblower Act is passed.

Ms. SCHAKOWSKY. Thank you. I wanted to ask Mr.—Dr. Marechal how this legislation would actually help regulators and law enforcement to better understand the economic incentive behind decisions by internet platforms and the ones that they make.

Dr. MARECHAL. I agree wholeheartedly with the points that my esteemed colleagues on the panel have made.

Again, Federal whistleblower protections make it easier for Big Tech workers who want to do the right thing to do that.

Again, Ms. Haugen benefited from the SEC whistleblower statute, which is why so many of her disclosures directly relate to matters within the SEC's jurisdiction. I would—I am confident that, if there were an equivalent for the FTC, we would have seen additional disclosures from her, additional whistleblower complaints related to matters under the FTC's jurisdiction, which includes economic decision-making and the economic factors that go into companies' decision-making.

Ms. SCHAKOWSKY. OK, thank you so much, and my time has expired, and now I welcome the questioning by my ranking member, Mr. Bilirakis, 5 minutes.

Mr. BILIRAKIS. Thank you, Madam Chair. I appreciate it very much.

And I want to thank all of you for your testimony today. Very informative.

There are reasonable proposals on and off the bills—again, off the list of bills being considered today and in the future. However, I am concerned by the unintended consequence that will arise if Congress decided to legislate—in other words, decides to legislate on privacy and data security in multiple bills, without establishing a comprehensive framework.

Ms. Rich, a question for you. Can you elaborate on any potential consequences that businesses and our constituents may face as a result of enacting several individual one-off bills on privacy, as opposed to one comprehensive bill?

I know you touched on it. If you could elaborate, I would really appreciate it very much.

Ms. RICH. Right now, it is a confusing—a highly confusing environment for both businesses and consumers. There are so many

sectoral laws that pertain to privacy, to technology, to, you know, many related issues, and no one really knows what the rules are.

So one of the chief benefits of enacting a comprehensive privacy law, which could include many of the issues we have talked about today, is to bring it all together, even if certain laws—it is not going to repeal all the sectoral laws, it is not going to roll back, you know, everything that people are dealing with now, but it could bring it together and create a comprehensive enforcement scheme.

And so that is one of the reasons getting rid of that confusion, make—bringing greater clarity to the marketplace, that it is so vital that we pass that kind of law.

Mr. BILIRAKIS. Thank you so much. Next question, it ultimately will be for Mr. Lane, but I want to—I have—I do have some comments first.

In addition to privacy and data security, one central theme to today's conversations, a Big Tech accountability platform, that particular Act is sponsored by Leader Rodgers, and we released it earlier this year.

One issue that is very near to my constituents is the growing rise of illegal activity, like the scale of deadly fentanyl products that are plaguing social media platforms. In fact, I was able to question the DEA about this issue just last week, and I am holding a roundtable in my particular district in Florida, the 12th congressional district of Florida, in the Tampa Bay Area, to discuss the fentanyl crisis with local leaders and law enforcement. We are doing that on Monday at noon.

To curb the tide of this activity, I also authored draft legislation that would direct the GAO to conduct a study on how online platforms can better work with law enforcement to address illegal content and crimes on their platforms.

So the question is for Mr. Lane.

What do you believe, Mr. Lane, is important for us to consider as part of this particular discussion?

Mr. LANE. Well, as you know, I have been working with families who have had children die from fentanyl poisoning, and it is a very sad situation that we are facing.

I do believe that, working with the FDA and others, they are taking some important steps. There is a lot of groups out there that are focusing on this. But there are two things that have to occur.

One, I know that groups have asked expressly to have an open and accessible and accurate WHOIS database, because that is how they are finding websites that are engaged in selling these drugs. And right now it is dark, and the FDA itself has asked for an open, accessible, and accurate WHOIS database. So that is a very important step in moving forward.

The other important step is that everyone talks about how these social networking sites are rabbit holes. Rabbit holes were 1996, when you had bulletin board services, and you had to find the rabbit hole. These social networking sites are more like black holes. They have a gravitational force of sucking people in to the darkness, and it is very hard for them to see the light again.

And those are the issues that we have to address: what are the algorithms? How are these black hole social networking sites that are sucking these young people in, and exposing them to drugs that

maybe they would not have ever had access to, and how do we stop that?

Mr. BILIRAKIS. All right, thank you very much. I appreciate it. And I want to discuss that even further with you, but I appreciate your response.

One last question. During the Senate Commerce Committee nomination of Gigi Sohn and Alan Davidson, both nominees discussed the harms that are occurring regarding the misuse of consumer personal information, and ultimately expressed support for passing a comprehensive privacy bill. I think this highlights how important it is for Congress to pass a national law on privacy and data security.

To the entire panel, a yes or no answer would be fine. Would you support this committee passing a comprehensive, national privacy and data security bill that sets one national standard, provides new rights to consumers, and sets clear guidelines for businesses to comply?

Again, a yes or no. Ms. Rich, please. I know what your answer is going to be.

Ms. RICH. Yes.

Mr. BILIRAKIS. Yes. Mr. Golin, please.

Mr. GOLIN. Yes.

Mr. BILIRAKIS. Thank you.

Mr. Lane, please.

Mr. LANE. Yes.

Mr. BILIRAKIS. Thank you.

Ms. Marechal—Dr. Marechal, excuse me.

Dr. MARECHAL. Yes, but it must be a strong standard, and it must——

Mr. BILIRAKIS. OK.

Dr. MARECHAL [continue]. With appropriate enforcement mechanisms.

Mr. BILIRAKIS. Thank you.

Mr. Ahmed?

Mr. AHMED. Yes.

Mr. BILIRAKIS. OK. And Mr. Greenblatt?

Mr. GREENBLATT. Yes, but I would want more information.

Mr. BILIRAKIS. Thank you. Thank you so very much.

And I yield back, Madam Chair. Thanks for the extra time.

Ms. SCHAKOWSKY. Absolutely. I would say yes also.

Mr. BILIRAKIS. Yes, I was going to ask you, but I knew your answer, as well.

Ms. SCHAKOWSKY. Yes, absolutely. And now I recognize the chairman of the full committee for 5 minutes for questions, Mr. Pallone.

TMr. PALLONE. OK. Thank you, Chairman Schakowsky.

As—I mentioned in my opening statement that we have held several hearings in the committee examining the real harms some social media companies have caused. And obviously, we are here today to discuss meaningful solutions. But I wanted to start out with Mr. Greenblatt.

The Anti-Defamation League has done important work showing the role social media companies play in amplifying racist, extreme, and divisive content. And you have also shown how those actions disproportionately affect marginalized communities. So can you

talk about the real harms you have seen social media companies cause through the use of their algorithms in that respect?

Mr. GREENBLATT. Sure. Thank you for the question, Mr. Chairman.

Yes, and I would say right off the bat, you know, the companies often use the smokescreen of freedom of speech to explain why this shouldn't be regulated. But the founding fathers wrote the Constitution for Americans, not algorithms, right? Products aren't people, and they don't deserve to be protected. But citizens do.

And we, indeed, have a situation where hate crimes are on the rise in this country. You know, the FBI reported a 13 percent increase in 2020, and the largest total since 2001. And ADL indeed has been studying online hate and harassment, and we find that one out of three users who report being harassed online relate it back to a characteristic like race, religion, gender, sexual orientation. And we have seen real examples.

I think about Taylor Dumpson, who is the young woman—she was the first African American female president of the student government at American University. I think she may have testified before you a year or two ago. And she was—after she was elected president, she was mercilessly attacked with a campaign that was conducted all online. It originated on a disgusting blog, neo-Nazi blog, and was perpetrated through Facebook and other platforms. And it ended up—started with the hate online, Mr. Chairman, and then you had nooses being placed all over campus. ADL worked very closely with Ms. Dumpson, and she is in a much better place today.

I think about a woman named Tanya Gersh, a Jewish woman from Whitefish, Montana, who had the misfortune of being from the same town that Richard Spencer, the notorious leader of the alt-right, was from. And when Ms. Gersh was identified and then doxed by the alt-right and neo-Nazis, she indeed, as well, was so mercilessly attacked, her and her family, they had to not only change all of their information, like their phone numbers, they had to move to a different home. They had to get 24/7 protection. Literally, again, death threats happened offline because of what started online.

So algorithms, we need much more transparency around them to ensure that they don't discriminate against marginalized communities. We need to realize that, as we were saying earlier, Facebook's AI, their vaunted machine learning, literally misses 95 to 97 percent of the hate speech.

You know, I used to be an executive at Starbucks, Mr. Pallone. I didn't get to say to my customers, "Well, three to five percent of our coffees don't have poison, so we think they are pretty good."

Mr. PALLONE. That——

Mr. GREENBLATT. You have to have a success rate of 100 percent, and I don't think it is too much to ask of, literally, one of the most well-capitalized and profitable companies in America to ensure that their products simply work, and don't harm their customers or the public.

Ms. SCHAKOWSKY. Thank you. I wanted to ask you another question, though, about transparency, because, in the case of holding

Big Tech accountable, increased transparency, I think, would go a long way to making it a safer place.

So how would the bills before us today bring greater transparency and, with it, greater accountability to the Big Tech platforms, if you—

Mr. GREENBLATT. Well, first and foremost, making the companies simply share their data about how the algorithms perform for the benefit of researchers and watchdogs. Think about it. These are public companies who have the privilege of getting resources from the public, right? Selling shares. But they don't disclose their information. Forget the risk to the companies, it is a risk to the general public.

The right analogy here is really Big Tobacco or Big Oil. We learned later that Big Tobacco knew the damage that their products were doing to their consumers, but suppressed the research. And we didn't have insight until it became revealed. And we learned that Big Oil knew the damage that fossil fuels were doing to the environment, but they denied it, and lied, until it was revealed. Well, now we know the damage that Big Tech is doing to our children, and to our communities. So asking them to simply be transparent, to simply make the information available.

The last thing I will just say to keep in mind is—what is the information we are asking for? It is user data. You know, there is this—there is an expression: If the product is free, you are the product. The information that we want is information about us. That shouldn't be too much to ask.

Mr. PALLONE. Thank you. Thank you, Madam Chair.

Ms. SCHAKOWSKY. Mr. Latta, you are recognized for 5 minutes.

Mr. LATTA. Well, I think the Chair, my good friend for yielding, and thanks for the hearing today, very, very informational. And I want to thank our witnesses for all being with us today.

Ms. Rich, if I can start my questions with you, and my good friend, the ranking member of the subcommittee, was getting into some privacy questions, and that is one of the issues that, you know, that is being struggled with today because, you know, looking at the testimony that you submitted, you know, you say for consumer survey—one of the surveys shows that consumers are concerned or confused about their privacy. Then it says consumers need a clear and consistent privacy law. Businesses, they are confused. Then we look at the enforcers.

And this was kind of also interesting. It says the lack of clear privacy standards are undermined—has undermined the FTC, too. And you state that, among other things, that the law does not establish clear standards for everyone to follow before problems occur. And what are some of these—because it says it is largely reactive.

So what is out there that the FTC has been doing, even though they have been trying to do what they are supposed to be doing in enforcement, but what are some of the standards that they need to have right now, to go forward and be clearer for the public?

Ms. RICH. Well, some of the basic building blocks that we see in every privacy law aren't required by the FTC Act: basic transparency, choices, accountability. There aren't—there isn't a data security law that applies across the country.

So—and, you know, you may not want this in a law, but, you know, access, correction, deletion, all of those types of rights that you see in law after law, anti-discrimination provisions, all of that—the FTC has to examine a specific company and decide after the fact, using its authority to police unfair or deceptive practices, whether a practice was unfair or deceptive. But there aren't clear requirements. All those elements aren't clearly required in any nationwide law that applies across different situations.

And so, as I think I said in my testimony, the FTC has been able to do a lot with its authority under the FTC Act. But it would be so much better for the public, for consumers, for businesses, for everybody, for the marketplace to have rules that everyone knows what they are, and they know what the consequences are if they violate them.

Mr. LATTA. Well, thank you very much.

Mr. Lane, you know, I am very glad we are holding today's hearing today, where we can consider legislative proposals like the Big Tech discussion draft that I authored that would require companies to disclose their content enforcement decisions. This is intended to cover illegal activity and harms that are happening online, such as fraud, illegal drug sales, and human trafficking.

I think complementary to this goal is the ability to have access to accurate WHOIS data. This would go a long way in helping to solve these problems.

As you mentioned in your testimony, WHOIS information can play a vital role in combating fraud and facilitating better cybersecurity. In 2020 I sent letters to several executive branch agencies to ask them about the importance of WHOIS in conducting their investigative and prosecutorial obligations. In responses from the FDA, FTC, and DHS, they emphasized the importance of this information in identifying bad actors, and connecting criminal networks, and protecting consumers about our cyber assets (sic).

You know, would restored access to WHOIS complement my discussion draft to make the internet safer?

Mr. LANE. Yes, absolutely. First of all, I want to thank you, Mr. Latta, and your staff for taking a leading role in the WHOIS issue. Your letters have been critically important to show and highlight the real concerns and cybersecurity threats that our nation is facing because of a dark WHOIS, based on the decision from the European Union and the GDPR, and a very broad interpretation of having it go dark.

I just also wanted to add one thing, and it is not just me saying it. In 2021, a survey by the two leading cybersecurity working groups found that restricted access to WHOIS data impeded investigations of cyber attacks. Two-thirds of the two hundred and seventy-seven respondents said their ability to detect malicious domains has decreased, and seventy percent indicated they can no longer address threats in a timely manner. And more than 80 percent reported that the time it takes to address abuse has increased, which means that cyber attacks harms the victims, lasts longer.

The group basically said this: Changes to WHOIS access following ICANN's implementation of the EU GDPR continued to significantly impede cyber applications and forensic investigation, and

thus cause harm to victims of phishing, malware, and other cyber attacks.

The Federal Trade Commission, as well as ICANN, is trying to fix this problem. And it is—what you are pushing in your legislation, and your letters—and, hopefully, this Congress will enact legislation—is critical. We can no longer put the multi-stakeholder process of ICANN ahead of the American people and the safety and security—and our national security needs to be protected by this Congress. And we should not be kowtowing to a law and a regulation that is from another country.

And I just want to end on this. ICANN itself, this chairman, the CEO of ICANN, has said that they are limited in their actions because of the GDPR, not because of U.S. law, not because of the California privacy laws, but by the GDPR. So we are at risk of having our own security put at risk because of a foreign entity's legislation and regulation.

And thank you so much for everything you are doing in this space.

Mr. LATTA. Well, thank you very much.

Madam Chair, before I yield back, I would like to ask unanimous consent to ask for the—entering the documents from the DHS, the FTC, and the FDA, and a report from the ICANN, GDPR, and a WHOIS user survey into the record.

Ms. SCHAKOWSKY. Without objection.

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

Mr. LATTA. Thank you very much for your indulgence. I yield back.

Ms. SCHAKOWSKY. Now I recognize Mr. Rush for 5 minutes for his questions.

Mr. RUSH. I want to thank you, Madam Chair, for convening this important hearing.

Like my colleagues, I am also a strong advocate for a comprehensive Federal policy legislation. In fact, when I served as chair of this subcommittee, we passed a strong, bipartisan bill that, ultimately and unfortunately, died in the Senate.

While I continue to advocate for policy legislation, Madam Chair, I am also cognizant of the fact that privacy is not a panacea that would solve all of the internet-connected problems that our nation currently faces.

Today, in addition to privacy issues, we also face very real and very pressing threats from issues like misinformation, disinformation, and algorithmic biases. With that in mind, and while I look forward to working on comprehensive privacy legislation, I am pleased that we are addressing these other equally important issues, as well.

That said, Mr. Golin, in your testimony you state that —and I quote—"children in lower-income households spent nearly two hours more on screens than children from higher-income households, and Black and Hispanic children spend significantly more time on screens than their White peers."

You also described how increased exposure to screen time is linked to increases in mental health issues, such as depression. It is too often the case that when—catches pneumonia. And while I feel that—this is true when it comes to screen time, also.

To that point, what type of impact is this increased screen time having in lower-income households, and particularly for Black and Hispanic children?

Has there been any data that shows how these outcomes compare to White or children in higher-income households?

Mr. GOLIN. Thank you so much for that question. Yes, so, as you referenced, the data shows that low-income and Black and Hispanic children have more screen time and spend more time playing games online than their higher-income and their White peers. And you know, the data also shows that screen time-linked problems, like childhood obesity, there are much higher rates in—for low-income children and Black and Hispanic children.

So I think that, you know, given what we know about the severity of the problems linked to excessive screen time, and that these children from these communities are having even higher rates, it is absolutely essential that we pass policies to protect to protect them.

Like all issues, you know, this is—affects all children. But like every issue, children from marginalized communities, children from more vulnerable communities are getting the worst of it. And so that is why it is so important that we create a new set of rules, and build a better internet for children, because we need to protect the most vulnerable among us.

Mr. RUSH. Does this create problems in the public education system?

Also, do you—is there any data that supports other ramifications of this particular phenomena?

[No response.]

Mr. RUSH. Hello.

Mr. GOLIN. I am sorry, I don't think I heard the question. Was that a question for me? I am not sure if I heard it correctly.

Mr. RUSH. Yes, this is you, this is the second question.

Is there any data that says that this particular phenomena affects the public education system, students in the public education system?

Is there an effect on—the increase in screen time—on children in school?

Mr. GOLIN. Yes. Well, there is data that shows the more time that kids are spending online for entertainment, the—it is correlated with lower academic achievement.

There has also been a rush to use EdTech in our schools, and to see EdTech as a panacea for fixing educational inequality when, in fact, what the data is showing is that, the more hands-on learning that kids get, it is actually better for their academic achievement.

So I think one of the things that is really worrisome is this, you know, this idea that, if schools invest heavily in EdTech platforms, that that is going to fix educational inequality. And, in fact, I think there is a real danger that is going to worsen it, because what kids need is quality teachers. They need smaller class sizes. They need to interact with each other. And the more time that kids are spending on screens for their learning, it is taking away from those things.

Mr. RUSH. Thank you.

I yield back, Madam Chair. Thank you for your indulgence.

Ms. SCHAKOWSKY. The gentleman yields back, and now Mrs. Rodgers is recognized for 5 minutes.

Mrs. RODGERS. Thank you, Madam Chair.

Ms. Rich, thank you for your decades of service. Your experience at the FTC was under a democratic chair, yet I appreciate your dedication to bipartisan consensus when possible, which had been the Commission's tradition.

Yesterday, Mr. Bilirakis and I sent a letter to FTC Chairwoman Khan regarding the FTC's current direction. It expresses concern with the Commission's use of zombie voting to pass rules, and the recent decision to delete legitimate business activity from the FTC mission statement.

Given the number of bills before us, I think it is essential that we find a realistic enforcement balance. We need to know how the Commission would manage all these competing priorities, without hurting legitimate business activity.

This alarming mission statement change happened while the Build Back Better Act was pending in the Senate. That legislation includes an amendment to the FTC Act, which would give the Commission broad, first-offense penalty authority.

How expansive is this proposed authority?

Is there any commercial activity or sector of the economy that it wouldn't apply to?

Ms. RICH. The civil penalty provision in the Build Back Better Act, as I read it, would apply to anything covered by the FTC Act: unfair or deceptive practices under the FTC Act.

So the FTC does lack jurisdiction over certain sectors of the marketplace: banks, non-profits, certain functions of common carriers. But otherwise, as I understand the provision, if it were to pass, it would apply across wide swaths of the marketplace.

Mrs. RODGERS. Thank you. Regarding the proposed new authorities, am I correct this only deals with civil penalties, and not remedies, like judgment or restitution?

Ms. RICH. That is right. Civil penalties only.

Mrs. RODGERS. During your FTC service, was the Commission able to predict how many violations would occur each year?

Ms. RICH. No.

Mrs. RODGERS. That is in line with our experience. The FTC cannot predict who is going to break the law.

I would note we supported and enacted such civil penalty authority targeting COVID-19 scams, and the Congressional Budget Office reported back that such revenues were insignificant over the 2021 to 2030 period.

This might be a basic question, but if all companies are following the law, there is no violation of the FTC Act. And thus, revenue is not generated via enforcement actions. Correct?

Ms. RICH. Yes, although I have never seen a situation where all companies are——

Mrs. RODGERS [continue]. See changes in actions. I worry about the lack of regulatory certainty for small businesses. They, after all, are not experts, like you, on what protections they may have under the FTC Act.

Is it fair to say that they may not have the resources or the sophistication to manage a review by the FTC of their operations?

Ms. RICH. Yes, but I am—not to be a broken record, but I think Congress can fix this problem by passing a privacy law that does provide standards.

Mrs. RODGERS. OK, well, I appreciate you answering those questions and providing the insight. And I do thank all the witnesses for being here.

I want to note that we have incorporated first-offense penalty authority in our comprehensive privacy and data security legislation, the Comptroller Data Act, as a means of policy enforcement, and I urge this committee to take action.

I yield back. Thank you.

Ms. SCHAKOWSKY. The gentlewoman yields back, and now I recognize Congresswoman Castor for her 5 minutes of questions.

Ms. CASTOR. Well, thank you very much, Chair Schakowsky, for holding this very important hearing, and for including my Kids Internet Design and Safety Act that I am leading with Representatives Clarke, Trahan, and Wexton, and, of course, Senator Markey and Blumenthal, and including the Social Media Data Act that Rep. Trahan and I are leading, as well.

We really do come to this hearing more than—more so than other hearings, as parents and as grandparents. We know, as Mr. Greenblatt said, these Big Tech companies are complicit in the harm that is being caused by online operations and, as Mr. Ahmed pointed out, profiting from the harm. So we clearly have to take action now on 230, on children's privacy, everyone's privacy, and especially the design of these platforms.

So I want to focus in on the KIDS Act. Mr. Golin, thank you very much for your years of work on this. So your testimony is that they—these Big Tech platforms like Instagram and YouTube and others, they intentionally design the way children interact online to kind of keep them addicted. Will you go into a little more detail on that?

Mr. GOLIN. Sure. And, first of all, Representative Castor, thank you for your tireless work to see that children get the online protections that they deserve.

So the business model for all of this media is to maximize engagement, because the more time a kid is on a platform, the more money they are worth to the platform. And so they design their platforms intentionally in ways to keep kids on those platforms, and to keep them checking those platforms as often as possible.

Just a few examples of that, they use things like rewards, and nudges, and push notifications. So things like Snap streaks. So on Snapchat, kids are incentivized to communicate through Snapchat every day with a friend, and then keep a streak going, and that becomes a very powerful motivation. It gamifies the relationship, and kids really want to keep that going.

They use things like autoplay and infinite scrolls on TikTok to make it really, really, really easy to keep using a platform, and really, really hard to disconnect.

They use things like likes and the follower counts, and so there is—everybody can see who is popular, and whose posts are popular at any given moment. And this is a really powerful incentive for kids to create content. And not only just create content, but to cre-

ate provocative content, and risque content, because they know that is what is most likely to get them attention.

And then, of course, there is the algorithmic recommendations, which personalize everything to kids to show them the content that is most likely to keep them engaged and keep going on a platform, regardless of whether that content is good for them. And in fact, as we have been talking a lot about lately, very often that content is terrible for them.

Ms. CASTOR. And, you know, I have been out when I am out and about, and I see very young children now on tablets and iPhones. I mean, we are talking toddlers. And what does the latest research tell us about how young children are when they are first interacting with online platforms?

Mr. GOLIN. Well, I mean, I think one of the things that is really disturbing is we all know that the age for social media, when you are supposed to go on social media, is 13. Forty percent of nine to twelve-year-olds report using TikTok every day. And the numbers are just about identical for Instagram and Snapchat.

Ms. CASTOR. And do they have the ability to kind of self-regulate at that age?

Mr. GOLIN. No, absolutely not. Executive functioning is still developing. It is very—you know, I mean, these are platforms that adults get lost in. These are platforms that, you know, we are all struggling with, as adults. And to think that developing children, who are still developing their executive function, and whose habits are being formed are using these platforms——

Ms. CASTOR. So how will the KIDS Act then help parents, and help address these harms that these online platforms are peddling and profiting off of?

Mr. GOLIN. So I think the KIDS Act does a number of really important things.

So, first of all, it prohibits those design choices that are there to maximize engagement, things like—to children—things like autoplay, things like rewards, things like quantified popularity.

It prohibits algorithmic—platforms from using algorithms to amplify harmful content to children, something that we have all been talking about a lot lately.

It also bans influencer marketing to children, which is one of the most manipulative forms of advertising there is.

So it really would do a huge amount to start creating that online environment that kids——

Ms. CASTOR. And then we have to pair it with privacy protections, right? And I have worked with you on the Kids Online Privacy Act. Do you agree that we need—those need to work together, and be passed together?

Mr. GOLIN. If we could pass both of those bills, we would really go so far towards creating the internet kids deserve.

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

Ms. SCHAKOWSKY. The gentle lady yields back.

Mr. Dunn, you are recognized for 5 minutes.

Mr. DUNN. Thank you very much, Madam Chair. I appreciate the opportunity to discuss these important issues.

You know, the Chinese Communist Party is probably the single greatest threat to the free world since the Cold War, and they seek

to sabotage freedom, democracy everywhere it exists. And malign influence permeates all of their corporations, including those that operate in the United States. They have CCP members in key board positions, and many of those organizations, they have direct control over decision-making.

Despite that, American tech companies still continue to operate within China, and we allow them—or companies with those ties—to operate quite freely here, in the United States, as well. Just this year, Microsoft was the victim of a Chinese state-sponsored cyber attack. Yet, if you look at the number of job postings for Microsoft in China, you get the feeling they are expanding rapidly in China.

So I think it is the concern of this committee what these U.S. tech companies are doing within China, and what those Chinese companies are doing here. For purposes of this hearing, I want to focus on what the CCP-affiliated companies might be doing here, in the United States.

The CCP doesn't respect the rights of their own citizens. Why should they respect ours?

Congress has a responsibility to ensure that American consumers are protected from these evolving threats. And I think this can be accomplished, and a number of you have said that today, as we—if we can get a comprehensive data security bill through that protects our citizens, without sacrificing innovation and competitiveness in our nation's technological fronts.

Mr. Lane, I, like many of my constituents, am very concerned about the amount of personal information that is currently collected without any basic level of protection. A specific example is BGI—that is the Chinese genomics giant—and the activities that they instituted during the COVID pandemic. They sold millions of tests kits to U.S. labs, and offered their own sequencing services to the government and individual states.

The lack of privacy standards attached to that does pose a national security risk, and I would like to know what concerns you most when it comes to protecting Americans' consumer data from foreign adversaries. What keeps you awake at night?

Mr. LANE. Thank you for the question, Congressman. What keeps me awake at night is that most people don't realize that the driver in this artificial intelligence race and machine learning is human interaction and data. And those who collect it the most will win in that fight.

And I do have strong concerns that we don't know how data is being collected and used. There is some great legislation. The Duncan bill and the Kinzinger bill are great examples of how we can try to know that.

But we also have to be concerned, because the head of government affairs for TikTok, over in the Senate, basically he talked about how the data is stored in Singapore. Well, my pictures are stored I don't know where, somewhere in the cloud. But I can manipulate them, I can access them, I can even print them. So we need to make sure that we know, not just where the data is stored, but how they are getting access to it.

And one of the things that has always bothered me about one of the TikTok statements is that they will never hand over U.S. American citizen information to China. And maybe they believe

that. But if someone gets a knock on their door, and a family member who is still living in China—from the Chinese Communist Party, and says, "We would like your relative to hand over the data," I don't—I know what I would do. Just as a person, if it was my family being threatened, would I hand that data over? Probably. And so those assurances cannot be taken seriously with that.

Mr. DUNN. So physical location of the data, which is real, even in the cloud, right, is something that is important. And of course, the jurisdiction over that data is important.

Ms. Rich, in the remaining seconds we have, I would like you to address what help you would like from Congress to give to the FTC to improve the security of our data.

Ms. RICH. Specific data security requirements, which do not apply across the market right now, there is no general data security law that applies to the U.S. marketplace. That would include process requirements, such as doing a risk assessment, accountability among officers in the company, oversight of service providers, contracts with service providers. There is many elements.

Mr. DUNN. A reliable audit on these companies, perhaps, as well.

Ms. RICH. Yes.

Mr. DUNN. Thank you very much for your time. All of you have been excellent witnesses.

Madam Chair, I yield back.

Ms. SCHAKOWSKY. Thank you, Mr. Dunn. Now I recognize Congresswoman Trahan for 5 minutes.

Mrs. TRAHAN. Thank you. Chairwoman Schakowsky and Ranking Member Bilirakis, thank you for convening this important hearing, and thank you to the witnesses. Many of you have offered invaluable expertise to my team and me when we introduced the Social Media Data Act in May, and now, as we draft text to create a new bureau at the FTC focused on platform transparency and safety.

Mr. Golin, Fairplay, formerly the Campaign for Commercial-Free Childhood, has been studying the impact of advertising on child—on children for decades. Can you explain why surveillance advertising, the method used by Instagram and YouTube, is particularly harmful for our teens?

Mr. GOLIN. Sure. There is a couple of reasons it is so harmful.

And first of all, thank you so much for all of your work to protect children online.

There is—so it is harmful because it allows companies to target teens' vulnerabilities. In fact, Facebook, a couple of years ago, they bragged to their advertisers that they were able to target a teen at the exact moment that they were feeling bad about themselves, and including when they feel bad about their bodies. So this leads to things like, you know, girls who express interest in dieting getting targeted with ads for flat tummy tees and dangerous exercise routines.

So again, being able to target those things that people are very vulnerable to, and try and encourage consumption of products that will make those things worse.

The other thing is that there is a complete asymmetry of information. It is just completely unfair. The only thing that teens may know about surveillance advertising is that there is some creepy ad that keeps following them around, and they do use the word

"creepy" to describe the advertising. But the advertisers know everything about that child. They know every website they have ever visited, every video they have ever liked, every comment they have ever made online, how much money their parents make, where they live, all the places they go. So it is just—it is completely unfair. The advertiser knows everything about the child, and the child knows very little about how the advertising works.

And then the last thing I will just say is, of course, it leads to a tremendous amount of data collection, and that data can be misused in all sorts of ways.

Mrs. TRAHAN. Well, certainly. I thank you for that. I mean, as Congresswoman Castor pointed out, many of us are mothers. I am the mother of two young girls. I am very concerned that they could be watching an online video of their favorite athlete, only to be targeted with a dangerous weight loss supplement. And we certainly need more transparency into how these ads are targeted.

Dr. Marechal, can you speak to why it is important for researchers to be able to study all digital advertisements, as opposed to just a subset, like political ads?

Dr. MARECHAL. First, it is very difficult to draw a clear line around what ads are political or not. For example, when an oil company runs ads advertising its commitment to green energy, is that political?

How about when Facebook runs ads claiming to support updated internet regulation, while lobbying against it behind closed doors?

What about these diet ads that we were just talking about, is that political?

Moreover, even if we agree where to draw the line, can we trust platforms to enforce it accurately? I think it is clear that the answer there is no.

But more importantly, ads can be dangerous or discriminatory, even if they are not political. The diet ads here is a great example, again.

But more importantly—but many people would say that a housing ad is not political. But if it is targeted in such a way that Black users can't see it, that is discriminatory and harmful. And that is exactly what——

Mrs. TRAHAN. That is——

Dr. MARECHAL [continue]. What targeted advertising enables.

[Audio malfunction.]

Mrs. TRAHAN [continue]. You can speak to why researchers need to have details regarding, not just the aggregated description of its audience that is targeted, but also a description of the aggregate users who saw or engaged with an ad.

Dr. MARECHAL. Right. So the targeting parameters only tell you who the advertiser was trying to reach. They don't tell you who saw the ads. Many times those two groups are the same. But if they are not, there is one of two things that is likely happening: either the platform is defrauding the advertiser by charging for a service that they didn't deliver, or it is optimizing the targeting beyond what the advertiser asked for, often in ways that are discriminatory. Either way, this is something that we should know, so that we can put an end to it.

Mrs. TRAHAN. Thank you for that. I do want to emphasize I think political ad transparency is important. I know the lines are blurred more and more.

And on the resource page of my website, I have started a digital ad library, where I am posting all of my political ads. I have included all the data outlined in the Social Media Data Act. I am happy to chat with my fellow members, if they would like to join me in that.

But I think, just in my close—and I do have a few more questions I will submit for the record.

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

Mrs. TRAHAN. But Frances Haugen told us just last week that researchers have begged and begged and begged for very basic data, data that they will never get unless Congress acts. And the Social Media Data Act begins to address this issue. And I look forward to continuing to work with all of you on the transparency issues that will pave the way for us to legislate.

Thank you.

Ms. SCHAKOWSKY. Thank you. The gentlewoman yields back, and I recognize Mr. Pence for his 5 minutes of questions.

Mr. PENCE. Thank you, Chairwoman Schakowsky and Ranking Member Bilirakis, for holding this hearing. And thank you to the witnesses for appearing here today.

This hearing is imperative to exploring the parts of Big Tech that could be negatively impacting the social fabric of our country, and harm the—harming the well-being of Hoosiers and all Americans.

I am increasingly concerned with the growth-at-any-cost mindset of Silicon Valley, which has been around for a long time, as we heard last week. Social media platforms monetize inflammatory content using opaque algorithms and tactics intended to manipulate the tendency of its users. This information allows Big Tech platforms to sell highly-valued advertising space with precisely placed ads at the most optimal times.

If profit is the ultimate goal, and there is nothing wrong with making money, one way to get there is to gin up users by promoting content that elicits the strongest responses. This creates a feedback loop of more clicks that lead to more data, which leads to smarter algorithms that can collect even more data. These efforts seem to work in conjunction with the expansive shield of Section 230 to evade accountability.

For Big Tobacco, warning labels plastered on the side of a pack of cigarettes served as a long-time immunity defense. For Big Tech it is Section 230. And much like Big Tobacco, tech companies use these same tactics on our youth to bring in lifelong customers—if some of you remember Joe Camel.

Unfortunately, for my constituents, there is a little insight—there is little insight into algorithms Big Tech employs to take advantage of their sweeping access in our everyday lives, nor do Hoosiers have adequate control over the amount of information collected, or how it is used to tailor personal and curated content.

You know, we had truth in lending. We had to take care of that many years ago.

Building off the Communications and Technology Subcommittee hearing last week, which many of my colleagues here attended, it

is clear this committee needs to get serious with our efforts to rein in Big Tech.

Mr. Greenblatt, I think you would agree that there are positive aspects of social media. Whether it is checking in with family or friends, or for small businesses to expand their reach, there are healthy uses of social media. But it seems to me these tech companies realized early on that they sit on top of a gold mine of user information with virtually no guardrails to protect consumers. And, as you detailed in your testimony, incendiary and controversial content is good for business.

Throughout this hearing, we have acknowledged the harmful aspects of overexposure to hateful content. This is—this has become a—very much a bipartisan issue. We—in my opinion, we ought to consider proposals that stop a platform's ability to generate revenue off content that has been adjudicated to have harmed the well-being of its users.

If platforms—Mr. Greenblatt, if platforms were eliminated—or limited in their ability to use algorithms to curate content for users, what would happen to social media companies, would they still be profitable enough to stay in business?

Mr. GREENBLATT. Well, first of all, I would just say, Representative Pence, I agree with the analogy that you drew to Big Tobacco. I mean, speech may be different than cigarettes, but addictive products that the companies fail to manage, about which they obfuscate and lie to elected officials and to watchdogs, there is clearly a problem that requires government intervention. I wish it were different. Unfortunately, it is not the case.

And I also agree that, like tobacco, you know, social media can be used in moderation for fun. And Facebook and other services have connected people across cultures, across countries. There is a lot of value to that. But the way they have been exploited by extremists, the way they have been used to abuse against children and manipulate them in ways that have been described is indefensible.

Now, the reality is these companies, indeed, are so big, and are so profitable, I actually believe they could fix this problem today, if they wanted to. Sure, it might hurt their margins a little bit as they made some capital investments. But if they have the resources—think about Facebook. It is 16 years old, and yet it has 3 billion users across the Planet Earth. It has the most sophisticated advertising——

Mr. PENCE. So, in the interest of time, you think that they could be profitable, they wouldn't necessarily go out of business?

Mr. GREENBLATT. Absolutely.

Mr. PENCE. Thank you.

Mr. GREENBLATT. Yes.

Mr. PENCE. Madam Chair, I yield back.

Ms. SCHAKOWSKY. I thank the gentleman, and now Mr.—no, Mr. McNerney, sorry.

Mr. McNerney, you are recognized for 5 minutes.

Mr. MCNERNEY. I thank the Chair for correcting that observation, and I thank the witnesses. Your testimony is very stark and important.

Mr. Golin, I just first want to say I appreciate your observation that Big Tech is counting on partisan division to prevent meaningful reform. And so we have to take that upon ourselves to make sure that that isn't the case.

Dr. Marechal, AI and machine learning are significantly more efficient for targeting specific consumers and for moderating content. Also, amplify and shape content in a way that creates entirely new harms, which we are hearing about this morning. So how does the use of AI and machine learning accelerate the spread of harmful content online, when employed to prioritize engagements of profits?

Dr. MARECHAL. Thank you for that question.

I want to be really clear that we are talking about two different types of algorithms here.

On one hand, we have the algorithms that boost content, including recommendation algorithms, the algorithms that tell you what groups to join, what people to add as friends, what accounts to—and order the content on your timeline. That is based primarily on correlation, and on predictions based on engagement. What are you most likely to click on, watch, comment on, like, et cetera.

On the other hand, we have algorithms that are meant to perform content moderation. That is to say, to identify the types of content that is illegal, that is against the platform's own rules, because it is harmful to—judged to be harmful to users and to society.

AI is not good at this latter part. This is one of the big lies that the tech industry has been selling us, that we are just around the corner from a big achievement in AI that will suddenly make it possible for them to have these huge and profitable platforms, where their goal is to have as much of human economic activity and human life filter through these platforms, so that they can make money off of it. They want us to believe that they are just around the corner from being able to identify and moderate away all the direct sales, all the incitement to violence, all the hate speech, all the content that we are rightly concerned about today. Again, that is not true. Only human judgment can do that.

Mr. MCNERNEY. Well, thank you for that clarification. So could increased transparency, artificial intelligence, and machine learning by internet platforms help to improve online safety?

Dr. MARECHAL. Absolutely. On the content moderation front, we need to know much more about the state of the art, as it is today, and what technology can and cannot do.

We have learned from Ms. Haugen's revelations, as well as from other whistleblowers previously, that Facebook in particular basically does not moderate content in languages other than English. I am exaggerating slightly here, but if you look at—again, at Ms. Haugen's testimonies before Congress and in other places, it is really clear that that—as things are for us in the U.S., and for other English speakers around the world, it is orders of magnitude worse than that elsewhere.

When it comes to content recommendation, you know, recommendation systems, likewise, we really need to understand what recommendations we are getting, what other people are getting, right? I have a sense of what is being recommended to me; I have

no idea what is being recommended to you, or to other people in society.

And again, policymaking in this area requires evidence. The first step towards getting evidence is greater transparency.

Mr. MCNERNEY. Well, thank you. Some clarification there.

I also want to thank you for your recommendation that we not allow CEOs to be both board members and majority shareholders. Hopefully, we can work with the committees of jurisdiction to get that done to do something there.

You also recommended that we should create conditions to help us produce evidence-based policy. Would you expand on that a little bit?

Dr. MARECHAL. Yes, absolutely. So that is what I was referring to when I was speaking to the need for transparency, and for researcher access to platform data.

So much of what we believe about—or think we know about platforms is based on our own individual experience, on anecdotes, on investigative journalism, on kind of one-off research studies, but it is not comprehensive, right? We have little snapshots of a huge problem, but that does not—that is not enough to fully understand the nature and extent of the problems, because only the platforms have access to that information.

So I believe that, in order to legislate effectively, we need a much more detailed understanding of the facts on the ground.

Mr. MCNERNEY. I yield back.

Ms. SCHAKOWSKY. The gentleman yields back.

Mr. Armstrong, you are recognized for 5 minutes.

Mr. ARMSTRONG. Thank you, Madam Chair. I appreciate everybody being here today.

And I think how we get here—I have sat through a lot of hearings in this committee and in my former committee, and I think we come down to this simple truth, that, as the larger the platform gets, more data is collected, more sophisticated algorithms are developed, which further entrenches their place in the marketplace, and stifles competition, and continues to incentivize the collection and use of that data to maximize profit. And seven—several of you have basically said this, and you are not unique.

The problem is with the business model, one that is designed to attract attention, collect and analyze what keeps that attention in place: ads. Whether the content is somehow detrimental to that individual, minor or adult or society in general, isn't a concern.

Now, several tech companies have recently announced that they will eliminate targeted advertising on certain topics, and we all know contextual advertising still occurs in other media. But after doing this for nearly three years now, I think my question is basically this: Should we restrict targeted advertising? Should we just restrict it?

Should we ban targeted advertising to children? I understand there would be significant consequences. But if the cost, societal costs are as high as some of the witnesses here and witnesses, indeed, that we have heard talk about today, it becomes a simple cost-benefit analysis.

The business model is not a bug, it is a feature. And it continues to do that.

And listen, Republicans talk about increasing competition in the marketplace, and how we do that, and often times—and these aren't unique, right? We have had members on both sides of the aisle agree on certain issues. We have had members disagree on issues. But eventually, when we are talking about capitalism, we are talking about profit, we are talking some of the largest, most powerful companies in the history of the world, should we start talking about taking away the financial incentive for platforms——

[Audio malfunction.]

Mr. ARMSTRONG [continue]. Of at least one empirical study from 2019 that concludes that, after accounting for other factors like user device information or geolocation data, publishers' revenue only increases by about four percent when a user's cookie is available. That increase corresponds to an average increment of just $.00008 per advertisement.

And as we continue to do this, and we move around, and we talk about how we do all of these things, I think the question has to become how do we disincentivize these companies from financially profiting off of conduct that is particularly harmful to adults and children? And I think we do this—and I have listened, I have learned more about—I have learned just enough about all of this to be dangerous, I think. And we continue to move our way through this.

But I think it is about we, as a legislative body, and as people who interact in this industry, I think it is about time we start having the real conversations about that. And I have got a minute and 50 seconds.

Yes, Mr. Lane. Question mark, question mark.

Mr. LANE. The industry is actually moving away from targeted advertising. If you—the last interactive advertising bureau meetings because of the GDPR and other related rules are slightly—you know, are moving away.

The question isn't targeted advertising that is the problem, especially if you talk with Jonathan Greenblatt. It is what are they watching. And if the algorithms—you know, I worked for Fox, right? So it was—you know, the goal was to, you know, spend a lot of money to—for the Super Bowl, because you got a lot of people watching it. The ads weren't relevant. And so people are going to pay for the ads. They pay a lot of money for Super Bowl ads that are not targeted because of the crowd, the viewership.

So the question is how are the algorithms, as I mentioned before, this black hole where they are trying to create people to be stuck in this system, the—you know, the edge of the net, the edge players, and how do we deal with that issue? I don't think getting rid of targeted advertising is going to help as much for the issues around what Jonathan is talking about as the issue of the manipulation of people, and bringing them down this black hole.

Mr. GREENBLATT. I would reinforce what Rick said. It is the surveillance advertising that is a problem. So I don't have a problem with advertising to our children. It happens on Saturday morning cartoons, you know, since the dawn of television. It happens in other media. The challenge is that we don't know what information they are collecting, they refuse to be transparent about it, and it is one—to use the term—one big black hole.

So I think what we need is these—companies to submit to a degree of transparency, which would elucidate how their marketing works and, again, prevent children and others from being manipulated.

Mr. LANE. And if I was going to have one area, in talking with the groups I work with on child safety, it is to have the parental control set to on, instead of off. That would go a long way of protecting the kids, because most parents don't know how to turn on these parental controls. And having them set to on for children and younger users, both at the device level, as well as at the social networking level, would be very helpful.

Mr. GOLIN. Can I just agree with you, Representative Armstrong, that I think getting rid of data-driven advertising to children is one of the most important things that we could do to protecting them?

Mr. ARMSTRONG. Well, and I am 26 seconds over——

Ms. RICH. And——

Mr. ARMSTRONG [continue]. But I would say the one thing—the one point to that is if you—whatever the new financial incentive is, we will have to deal with that one secondly. But the reason I bring it up is the financial incentive to be there.

And with that, I yield back.

Ms. SCHAKOWSKY. The gentleman yields back.

And Congresswoman Clarke, you are recognized for 5 minutes.

Ms. CLARKE. Thank you, Chairwoman Schakowsky and Ranking Member Bilirakis, for holding this very important hearing. And thank you to our witnesses for your insightful testimony today.

Technology will always be a double-edged sword. While it is often a source of good and progress in the world, we must also take care to limit the harms and abuses that inevitably occur.

As I mentioned during our hearing last week in the Communication Technology Subcommittee, the widespread use of algorithms by social media platforms to determine the content that users view has far too often resulted in discriminatory practices and the promotion of harmful misinformation.

Recent whistleblower reports make it quite clear these platforms knowingly amplify the most dangerous, divisive content. Indeed, it is central to their business model. This is a major concern of mine when it comes to safeguarding our democracy and stopping the spread of online misinformation aimed at marginalized groups.

After the 2016 election, a Senate Intelligence Committee report found that Black Americans in urban areas were disproportionately targeted on social media with false reports and conspiracy theories meant to propagate distrust in our democratic institutions. The report specifically notes that Russian operatives "took advantage of the Facebook recommendation algorithm, an assessment Facebook officials have corroborated."

Mr. Ahmed, how would legislation like Congresswoman Matsui's Algorithmic Justice and Online Platform Transparency Act help prevent the targeted flow of disinformation aimed at marginalized communities like we saw during the 2016 elections, and are now seeing again with the COVID-19 vaccine?

Mr. AHMED. Thank you for the question. I think there are two ways in which it would help, and—to abate civil rights concerns.

The first is that it would help us to deal with the kinds of algorithms that feed racist, discriminatory material to people that weren't already following it. So one of our reports on algorithms showed how people following wellness influencers were fed anti-vax content. People that then followed anti-vax content were fed anti-Semitic content, because it knew that you could broaden, as well as deepen, people's extremisms.

The second thing it would do is—there is this issue where—misinformation is a very old thing. It has been around for a long time. But social media is like retrofitting a sort of homing package onto that misinformation, in that it turns, you know, a dumb weapon into a smart weapon, which can hone into the communities that it is most effective on. And we have seen that—the incredible ability of the—of content being produced by bad actors, such as anti-vaxxers.

So Robert F. Kennedy, Jr. and his misinformation about vaccines, which is then—the algorithm drives it to the audiences that are most vulnerable to it. And that, of course, has led to—it has led to death. I mean, 49 out of the last 50 deaths in DC were—of COVID—were of African American people. And that is a direct reflection of the misinformation that has been pumped into those—into our communities.

Ms. CLARKE. Thank you, Mr. Ahmed. The lack of accountability and transparency into how companies are using algorithmic systems is an issue I have been sounding the alarm on for years, and it is important we recognize that the use of discriminatory algorithms isn't limited to social media platforms. Increasingly, algorithms are being used by large companies to determine everything from who is eligible for health care coverage to whether or not a homebuyer receives a mortgage.

While this may have certain benefits, the reality is that our current safeguards are insufficient to protect Americans from the harmful biases and design flaws inherent in new algorithms—excuse me, in many algorithms. And this is why I will soon be introducing an updated version of my Algorithmic Accountability Act, along with Senators Wyden and Cory Booker, which requires that large companies audit their algorithms for bias and discrimination, and to report their findings to the FTC for review.

Ms. Marechal, from a general perspective, why is it so important that we address the instances of algorithmic bias that affect critical decisions in people's lives?

Dr. MARECHAL. Thank you for that question, Representative Clarke.

I think you described the stakes very well and clearly, yourself. Algorithms make decisions based on data. That data is often faulty. That data, even when it is accurate, reflects information that should not be taken into account when making certain decisions, right—make decisions——

[Audio malfunction.]

Dr. MARECHAL [continue]. To make them with things like race, or gender, or age, or other key markers of identity in mind, in order to be fair.

Algorithms can only make decisions based on data. And so, it is—and right now this is something that is perfectly legal in many cases, and——

Ms. CLARKE. Ms. Marechal, I am so sorry, I am over time. I didn't realize it. I thank you for your response.

I yield back, Madam Chair. Please, pardon me.

Ms. SCHAKOWSKY. Yes, thank you.

Congressman Bucshon, you are next. You are recognized for 5 minutes.

Mr. BUCSHON. Thank you, Madam Chair. In recent years there has been proposals for the creation of internet platforms and services aimed at children—some of this I know we have covered, I apologize for missing part of the hearing—which, I am thankful, have largely been put on indefinite hold, since I am quite certain they would become havens for predators, fraudsters, and cyber bullies. Our society has been seeing the terrible impacts of cyberbullying on our children, with far too many being injured, or even losing their lives as a result of malicious actors online.

Mr. Lane, I applaud you for your work as a child safety advocate imposing these type of bad actors.

One proposal that I have put forward would require the publication and annual updating of content moderation practices relating to cyberbullying for internet platforms. This transparency would be a powerful tool for parents and other users to know what kinds of content and actions will not be tolerated on a platform, and they could be used—and they could use this information to allow and restrict their child's access.

Do you—would you agree that providing clear and consistent rules in this space would reduce the incidence of cyberbullying?

Mr. LANE. Yes, I do. When News Corp bought Myspace—and people maybe remember Myspace, it was the largest social networking site at the time—this was one of the areas that we focused on, because of the concern that our CEO and others had when we purchased it, the harm that could be occurring through cyberbullying. And it was the first time that we looked. And we did instill a lot of practices to try to stop it, and monitor, and report, to try to hinder the access of folks who are cyberbullying one another.

So I do think having clear processes in place would be very helpful, but I also think—getting back to the point I was making earlier about having the parental control functions on in these—in this world, what kids can talk to which kids, and making sure that their kids—is critically important.

Mr. BUCSHON. I mean, it is—I have got four kids. I mean, it is a tough nut to crack. I mean, sometimes you don't even know that your kids are on certain sites. They have dual sites. They have the one where they show their parents, and they have the one that they are actually communicating on.

And, as a parent, I do think parent engagement is extremely important in this situation, because we, as parents, said, "We have access to all of your phone information and your computer information, and the first time that you don't give it to us, you lose your phone, you lose your access to the computer."

Mr. LANE. Yes, this has been an area where—has been very active in this space because of the harms, as kids go down a really

bad rabbit hole in this area, and it can be so detrimental to their health, their safety, and their education, and it is something that really needs to be addressed.

Mr. BUCSHON. Yes, and we can have everything in place, in that if the parents aren't—or guardians are not daily, really—I mean, I have got four kids—daily engaged in what their kids are doing, we can do all we want here, and we may not still be able to stop it, but it is important to do it.

Do you think the current patchwork of laws, regulations, and policies regulating the space to date have actually helped to allow cyberbullying, in many cases?

Mr. LANE. I don't know. I mean, the hard part with cyberbullying that we faced even at Myspace was, you know, the free speech—you know, First Amendment. What is cyberbullying, what is bullying? That is always difficult to address.

So the patchwork of different state laws, I mean, it is always hard when it is that way, and there is no natural law.

Mr. BUCSHON. Yes.

Mr. LANE. I don't know—and we tried to figure this out ourselves—how you draft a law that completely can stop cyberbullying.

Mr. BUCSHON. Do you—I am just curious. Did you have childhood and teenage consultants on this, when you—you know, I know it sounds crazy, but all of us that have kids understand that what we think, as parents, might be one thing. The kids actually have quite a bit of insight.

And I—you know, I talk to my kids, and I am like, OK, like, I don't quite get this. But it would be interesting to know if that—you think that would be helpful, where, actually, companies, and maybe even Congress, hear from teenagers, hear from kids about what is happening out there.

Mr. LANE. Yes, it is funny. We didn't have any teens that were with us. But Parry Aftab, who is one of the leaders and child safety advocates in the early days of the net, had this group called Teen Angels, and she would talk to them, and we would talk to her and get ideas.

The other thing that we did is we had a direct line to the National Center for Missing and Exploited Children to see what could we do to fix it, to make it better. And we basically took every recommendation that they made, some may say to the detriment that now it is all about Facebook, and no one knows about Myspace.

But we thought it was the right thing to do, and we took steps. We would not implement certain functionality because we couldn't figure out how we could protect children that made sense. Himanshu Nigam, who is our chief safety officer, we would talk almost every day on what we could do to make Myspace safer. And it is tough, but you can do it.

Mr. BUCSHON. Yes, and it not only needs to make sense to us, it needs to be—make sense to the people who are potentially being cyberbullied.

So I would suggest that we seriously consider that in the future, when we are talking about this subject. We might have a few people who—young people, who are actually in the arena, so to speak—give us some advice. I mean, I think that is not a bad idea.

I yield back.

Ms. SCHAKOWSKY. The gentleman yields back.

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

Mr. CÁRDENAS. Thank you very much, Madam Chairwoman, and also Ranking Member Bilirakis, for holding this critical hearing. And I want to thank all the witnesses for all your expertise and opinions today to help educate us, so that we, hopefully, can make good policy to guide what is going on underneath our noses every single day.

Every day Americans are forced to accept extremely complex, opaque, and one-sided terms of service to enjoy popular platforms that often market themselves as free.

What I am holding up here is 27 pages of an agreement that—anybody who uses Snapchat has agreed to these 27 pages. There are roughly 106 million active Americans on Snapchat. How many of those users do you think have the time or formal legal education to understand and agree to a contract such as this, written by a team of lawyers, by the way? The average American doesn't have a team of lawyers, nor could they afford it.

I predict that right around none is the number of Americans who have actually read every single one of these pages. And this goes for many, many, many of the platforms. Some of the platforms have reduced their agreements to two pages, probably much finer print and a lot more legalese. And once again, still, at the end of the day, same typical terms.

Snapchat prides itself on protecting user privacy, and those who use the platform believe their snaps exist temporarily before being automatically deleted. But when you read the terms of service, you realize that this is not the case. In fact, Snapchat employees can access your private user data, including photos and/or videos. To go even further, hidden in Snapchat's terms of service, you grant Snapchat and its affiliates an unrestricted, worldwide, royalty-free, irrevocable, and perpetual right and license to use the name, likeness, and voice of anyone featured in your public content for commercial and non-commercial purposes. That is one of the clauses that is buried in these 27 pages.

Folks, I said one of any—I said of anyone featured in your content. That is what that just meant. Anybody featured in your content. So if I put out content, and my colleague, Ms. Kelly, is next to me, all of a sudden I have wrapped her into it, and she hasn't agreed to anything. But it applies to what I have done, and I may have injured or aggrieved somebody that I care about. That means people who do not even sign up are subject to the—this agreement.

And again, even if that person disagrees, do they have a team of lawyers to go ahead and fight for their rights?

Those who read the terms would notice that platforms often include an arbitration clause, stripping the ability of users to take these companies to court. Instead, they force users to resolve issues in house, on the company's home turf, with their team of lawyers against you.

For supposedly free services, these platforms seem to take a lot of our users for granted, and a lot from us.

Mr. Greenblatt, can platforms use the terms of service to include a provision that harms users and put them outside the reach of the law?

Mr. GREENBLATT. Thank you for the question. I will preface my response by noting that I am not a lawyer, or a consumer protection lawyer, at that.

That being said, it seems to me that the point you have raised is incredibly valid. Pages and pages and pages of 8-point legalese, and expecting my, you know, 15-year-old or 12-year-old to understand that is laughable, at best, and it is malicious, at worst.

I mean, the reality is this is why we need transparency. We need transparency in how these algorithms work. We need transparency in the data they are collecting. And, Mr. Congressman, we need a kind of not truth in advertising, but a truth in terms. I mean, what you just laid out is indefensible when it is directed at a minor.

Mr. CARBAJAL. And not just the minor, the average American just cannot?

Mr. GREENBLATT. Absolutely.

Mr. CARBAJAL. It is just not an even playing field, not at all.

Yes, Mr. Lane, briefly.

Mr. LANE. Yes, very briefly. This is why we need Section 230 reform, because if there is a violation of the terms of service, we need to have the civil litigation to be able to find out if there is a violation, so we can get teams of lawyers to engage in this process. And without the Section 230 reform that we are talking about, and the duty of care, we are waiting for a whistleblower, which we hope comes, but may never.

Mr. CARBAJAL. Well——

Dr. MARECHAL. Can I jump in here? I realize it is awkward, because I am remote, but Section 230 has absolutely nothing to do with this. This is about privacy.

Mr. CARBAJAL. OK, thank you. I would like to ask a quick yes-or-no ?

Dr. MARECHAL. Any—can I just say any value that we care about shouldn't be subject to notice and choice in a—deep in a terms of service.

Mr. CARBAJAL. Thank you. Thank you very much. And this issue is, obviously, important, not only to the average American, especially for those of you are deeply involved in this every single day, as I can see by your answers.

Very quickly——

Ms. SCHAKOWSKY. The gentleman's time has expired. You are going to have to put that in—am I right? Yes, you are going to have to put that in writing.

Mr. CARBAJAL. I was hoping you would afford me the same generosity I have seen my colleagues do.

I love you, just kidding.

Ms. SCHAKOWSKY. OK, but——

Mr. CARBAJAL. I am going to yield back.

Ms. SCHAKOWSKY. Ask the question and then get an answer.

Mr. CARBAJAL. I yield back, I yield back.

Ms. SCHAKOWSKY. OK.

Mr. CARBAJAL. I just saw everybody go a little extra, I thought——

Ms. SCHAKOWSKY. I would, but I——

Mr. CARBAJAL. I thought I would use my position, as well. Thank you.

Ms. SCHAKOWSKY. OK. And now, Congresswoman Dingell, you are recognized for 5 minutes.

Mrs. DINGELL. Thank you, Madam Chair. Thanks for holding this hearing, and to all of you who are testifying here today.

In our March hearing, with many of the major tech CEOs, I raised the fact that violative, provocative, and divisive content often receives more engagement on social media platforms, which many of you have raised in your testimony. Several audits, investigations, and reports continue to substantiate the claims that companies are aware of this fact. And I believe it is our duty to ensure that they are not prioritizing profits and engagement over the safety and the health of their users. I would like to move some questions focused on these protections, first on prioritizing engagement.

To the panel, if you would just answer this with a simple yes or no, are these companies actively making the choice to prioritize profits and engagement over combating disinformation, violent content, and negative health outcomes for individuals and children, yes or no?

Dr. Marechal?

Dr. MARECHAL. Yes.

Mrs. DINGELL. Mr. Greenblatt?

Mr. GREENBLATT. Yes.

Mrs. DINGELL. Mr. Ahmed?

Mr. AHMED. Yes.

Mrs. DINGELL. OK. Mr. Golin ? Golin, sorry.

Mr. GOLIN. Yes.

Mrs. DINGELL. Mr. Lane?

Mr. LANE. Yes.

Ms. RICH. Yes.

Mrs. DINGELL. Ms. Rich—OK, so we got that. So my next question is for Dr. Marechal.

Is there significant evidence that the changes we are proposing today to these platform algorithms will have an outsized impact on user engagement on the platform?

What is the cost benefit for consumers and companies in incentivizing or requiring these changes?

Dr. MARECHAL. That is a great question, Congresswoman. I think the single most impactful thing that we could do to change the current incentives, which, as you say, push companies to prioritize engagement above all else, is to ban surveillance advertising. This could—this would most effectively be done through comprehensive privacy reform.

Mrs. DINGELL. Thank you for that. I firmly believe that independent researchers and the FTC should have access to data from these companies to ensure that features and user data are not being exploited in ways that push individuals and children towards disinformation, violence, extremism, negative health outcomes. And that is why I am supporting one of—the Social Media Data Act, introduced by my colleague, Rep. Trahan, to ensure that researchers have access to information on targeted online digital advertisements, to study their potential harms to consumers, and create a working group to establish guidance on handling this data.

In March I asked Mark Zuckerberg if he was opposed to a law to enable regulators to access social media algorithms—can't even

talk today. In his response he said that giving more transparency into these systems was important, but we sure haven't seen any progress on Facebook since—on that issue so far.

So Dr. Marechal, why have companies so far resisted increased transparency on sharing advertising data with independent regulators and researchers, despite repeated commitments to do so, and repeated revelations that they are aware of the impact?

Dr. MARECHAL. In short, because, as bad as they are at moderating and governing user content on their platforms, they are even worse at moderating advertising. Facebook and other platforms are replete with ads that are illegal in the country in which they are served, that violate the platform's own stated rules. And they don't want to be—get caught doing that.

And they know that when, in the case of Facebook, it is—99 percent of their revenue comes from targeted advertising, for Google it is in the—90 percent, or something like that, it is very high for other platforms, as well—that once you start tugging at that string, that the whole house of cards is likely to come down.

This is a completely ungoverned and anti-competitive sector of the economy that needs to be regulated as soon as possible.

Mrs. DINGELL. So I have many other questions, which I will submit for the record.

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

Mrs. DINGELL. But I will give you my last one for Dr. Marechal.

How do platforms create additional barriers or, in some cases, completely block independent researchers from obtaining data?

And how would the Social Media Data Act alleviate some of these obstacles?

Dr. MARECHAL. That is a great question. So, you know, the New York—the NYU ad observatory case from this summer is really the prime example of that.

Companies, first of all, are constantly changing their code to make it harder for researchers to scrape, or to automatically connect—collect information that is published on the internet that you don't need to log in to access.

They are—they also shut down the accounts, deplatform individual researchers when they start to do research that the companies find threatening. That is what happened to ?

Ms. SCHAKOWSKY. You are going to have to wind up your answer right now.

Dr. MARECHAL. Thank you, ma'am. They also sue individual researchers, which is very, very chilling to research.

Mrs. DINGELL. Thank you, Madam Chair. I will say one thing: the consequences of these decisions are boldly apparent and, in many cases, deadly. Thank you, Madam Chair, for holding these hearings, and I hope our committee acts soon.

Ms. SCHAKOWSKY. The gentle lady yields back, and now my colleague from Illinois, Congresswoman Kelly, for 5 minutes.

Ms. KELLY. Thank you so much, Madam Chair, for holding this hearing today, building off of our productive Communications and Technology Subcommittee hearing last week. I want to thank the witnesses for testifying today, and helping us craft legislation to hold Big Tech accountable.

And to Mr. Greenblatt, I just wanted to say to you, 20 years ago, maybe more now, I got engaged with the Anti-Defamation League, and it changed my life, because I got involved in a World of Difference and—difference, so you helped me see things through a great lens that I still have with me.

One of the fastest-growing methods for acquiring customers online is through influencer marketing. Influencers are people who have a lot of followers or social influence online, and who then use that influence to endorse and sell products. Today influencer marketing is a multibillion-dollar industry in the U.S.

What I find concerning is that so many of our—of today's top influencers are children, so-called kid influencers, with massive followings on social media. It is not clear online when content is organic or sponsored advertising. Studies show this problem is significantly worse for children, because children do not yet have the cognitive abilities to make these distinctions.

Mr. Golin, can you talk about the harms that kidfluencers pose for children online, and why do you believe such advertising has become so prevalent?

Mr. GOLIN. Yes. So the reason it has become so prevalent is because it is allowed on on the internet, and it is not allowed on children's television.

So on children's television we have the Children's Television Act, which prohibits product placement. It prohibits hosts from selling directly to children. And we don't have the same rules online, which is—which makes no sense. If a child is watching a video on YouTube, they certainly deserve the same protections as if they are watching it on Nickelodeon, or Disney, or another television channel.

And the harms—you know, so children's understanding, they already understand advertising less than adults. But the way that we can get children to understand advertising better is by having it clearly separated from content. What research shows is the more that advertising is embedded, the less children understand about what is going on.

So you have, on—situations like on YouTube, unboxing videos. You have unboxing stars like Ryan's Toys Reviews, literally billions of views of these videos, where kids—where Ryan is talking about a toy he has been paid to talk about for 10, 15 minutes. Kids are watching infomercials. Studies have shown that kids who watch these videos are more likely to nag their parents for what is advertised, and more likely to throw a temper tantrum if they say no.

These—influencer marketing is also linked to higher levels of materialism. And if you look at Frances Haugen's documents, one of the things that teens themselves are saying is that influencer culture is toxic, and makes them feel bad about themselves.

Ms. KELLY. We also know that social media platforms often facilitate and certainly make a lot of money from influencer marketing. What responsibility do you think that these platforms have to protect children from this kind of marketing, and, in your mind, are they fulfilling these responsibilities?

Mr. GOLIN. They are absolutely not fulfilling these responsibilities. I mean, YouTube is making so much money off of kids watching unboxing videos. Influencer content on TikTok and Instagram

is making those platforms—but I don't think we can wait for these platforms to do the right thing. That is why I think we need legislation like the KIDS Act, that would ban these platforms from recommending influencer marketing to kids.

Ms. KELLY. So how do you think the KIDS Act would help protect children in these instances, where it is hard to distinguish between authentic and sponsored content?

Mr. GOLIN. Well, what it would do is it would prohibit the platforms from amplifying that content to children. And so that would be a mechanism where the platforms could be held responsible. And I think, if they were facing fines for doing that, that they would start cleaning up their act.

Ms. KELLY. And because I have a little bit more time, does anyone else want to make a comment about that?

No? OK, well, I will yield back. Thank you, Madam Chair.

Ms. SCHAKOWSKY. The gentleman—the gentle lady yields back, and Mr. Soto is recognized for 5 minutes.

Mr. SOTO. Thank you, Madam Chair.

Transparency, privacy, integrity of information, protecting our kids, all critical ideals that our committee is charged with helping uphold in social media. These are a challenge in English. It is pure chaos right now in Spanish and in other languages, trying to uphold these ideals. So I applaud the Chair and the ranking member, my fellow Floridian, for the bipartisan group of bills that have been put forward today that we are starting to review.

We have seen lies about the vaccines, and about January 6th, and about the 2020 election, and we have seen lies that breed hate and division in our nation. And so this committee takes this very seriously.

For Spanish language content, it is often less moderated for misinformation and violence than English content. Spanish language content posts are often allowed to remain on social media pages for longer durations than English content. A question for Mr. Greenblatt, then Mr. Ahmed.

How does having unregulated Spanish misinformation hurt minority communities and people of color?

And how should—how do social media companies and their algorithms fail to address the Spanish misinformation?

Mr. Greenblatt?

Mr. GREENBLATT. So it is a very good question, Congressman Soto.

And one of the revelations of the Facebook whistleblower was that Facebook spends upwards of 90 percent of its resources on dealing with misinformation in English, despite the fact that less than 10 percent of its users are doing so in English. So there is a vast misallocation of resources, despite the fact that they do a pretty poor job, as has been stated already.

ADL participates—proudly participates—in the Spanish Language Disinformation Coalition, and we work a great deal to look at these issues. I can tell you we have found examples. We did an analysis last year, last November, of Spanish language anti-Semitism on Facebook, and we found, with just a few keystrokes, about two dozen Spanish language accounts that were wildly in violation of Facebook's own terms of service, that they failed to take down,

that got hundreds of thousands of—coming from groups with hundreds of thousands of users getting upwards of 55,000 views. So we know this is a big problem.

Mr. SOTO. And we have seen that published in even local newspapers and on—in local television in places in our state, so we are deeply concerned about it. And then it is repeated in social media.

I want to turn to Mr. Ahmed next.

Again, how does unregulated Spanish misinformation and other foreign language misinformation hurt minority communities and communities of color?

And how do algorithms fail to address this misinformation?

Mr. AHMED. Well, this is a mixture of both algorithms, which are very good at targeting the right misinformation to the most vulnerable audiences, and bad actors, who are—who understand that, actually, the Spanish-speaking market is an easier one to sell misinformation into, because there isn't as much moderation of the content there. And it is just—it—there is a lower potential of that content being removed.

What that means, in practice, is that if you take, for example, vaccine misinformation, that the content that was being targeted to Spanish audiences by non-Spanish-speaking originators—so you found some of the key members of the Disinformation Dozen who aren't themselves Spanish speakers were having their content translated into Spanish at the same time, and pumping it out into Spanish-speaking audiences. And we saw that being taken up, we saw people debating it, and we saw people deciding not to vaccinate initially because of it.

And what did that mean? That meant that, literally, you know, Latinx communities in America were dying because they were being—A, they were more exposed to—you know, there was a higher prevalence of acute COVID; and second, that they were then being persuaded not to take the vaccine, the thing that would most protect them.

Mr. SOTO. Thank you, Mr. Ahmed. And just as a comparison, we saw vaccination rates really high in central Florida among both Puerto Rican and Mexican American communities. Puerto Rico has the highest rate in the nation, because it wasn't politicized in the media, in social media. But we saw in other areas, like in South Florida and South Texas, where misinformation campaigns were deliberate. And what did that lead to? Low rates.

I heard crazy things said about the vaccines, when the only crazy thing about it is not taking them to stop this deadly virus.

So thank you, gentlemen, for your input.

And Madam Chair, I yield back.

[Pause.]

Ms. SCHAKOWSKY. It is to Doyle? OK. The gentleman yields back, and now as—we welcome a waive-on to the committee, and that would be the chairman of—also a chairman of the subcommittee, Mr. Doyle, for his 5 minutes of questions.

Mr. DOYLE. Well, thank you very much, Madam Chairwoman, and to both you and Chairman Pallone, for continuing this series of legislative hearings to move forward with common-sense solutions to protect consumers online, and to hold online platforms accountable for their actions.

Last week, at the Communications and Technology Subcommittee, we heard from experts on the harms caused by online platforms, as well as experts on legislative solutions to address these significant problems. And as we have heard from panelists today, providing victims access to the courts is not enough to address the breadth of issues surrounding tech platforms.

I agree that transparency and other accountability measures are necessary, as well. So today's hearing and the witnesses' testimony are very important as we move forward.

Mr. Greenblatt, you also made comments to this effect. In your testimony you note that hate speech and, potentially, disinformation and other dangerous content is often protected in the First Amendment. And then you go on to say that we need to do more than just focus on Section 230 reform as required to hold platforms accountable.

Can you first talk about how some platforms are tuned for disinformation?

I would like to hear more detail on how some platforms' designs encourages disinformation, hate speech, and harmful content.

Mr. GREENBLATT. Thank you very much for the question, Congressman Doyle.

So, first of all, let's just acknowledge that hate speech is part of living in a free society. Our First Amendment protects ideas, even those that we don't like. But the challenge is hate speech is not the same. And I am sorry, speech that causes direct harm is different.

Freedom of speech is not the freedom to slander people. Freedom of expression is not the freedom to incite violence. So platforms like Facebook or Twitter, Congressman, that often will use anonymity, that don't take down posts that are directly threatening to people, that don't take down posts that express lies or misinformation are directly damaging to the public good.

Now, the reality is that there is a reason why newspapers, magazines, movies, television, radio, and all other media do not allow such content on their services, because they would be liable for litigation and for lawsuits if they did. Only the social media companies enjoy the privilege of non-accountability, and that is because of the loophole in the law, Section 230, that was referenced earlier.

Mr. DOYLE. Thank you. Research has shown that, with very little information about a user, Facebook's algorithms can simply begin showing conspiracy theory and other disinformation to that user. Is it good policy that Federal law protects Facebook from any harm that comes to the user as a result of that information?

Mr. GREENBLATT. Absolutely, it is bad policy. It is unambiguously bad public policy, and it is a loophole that extremists have exploited to great effect.

And again, we have seen where, out in the open, extremists use Facebook groups to organize actions against other individuals. This would be inexcusable, again, in any other context. People are allowed to say hateful things. The question is whether Facebook and the other services should privilege them, should amplify them, should elevate them. I say the answer is no.

Mr. DOYLE. So how do we pair the transparency and reporting requirements with other reforms, like we discussed last week, to

protect both online users, and maintain a healthy online ecosystem?

And how do we have meaningful transparency requirements that are not abused by those promoting hateful and other odious forms of speech, even if protected by the First Amendment?

Mr. GREENBLATT. Well, I think one of the things that one—could be done right away, Mr. Congressman, would be to allow researchers access to this information. You don't have to necessarily make it available to the entire public, but accredited researchers who apply could be given access. And you would need to have real criteria, so that Facebook and the other companies couldn't deny credible requests.

But you have—as public servants, you and the government, you are—have to be compliant with a FOIA request. There is no reason why we couldn't create a similar FOIA-type requirement of these companies, because the data they have is our data, it is public data, it is citizen data, and they should be sharing—more transparent, and sharing it.

Mr. DOYLE. Thank you.

Mr. Ahmed, we know, through your research, and now through Facebook's research, thanks to Frances Haugen, that a small number of users are responsible for much of the disinformation that we are seeing online. Clearly, the incentives are not aligned for these platforms to take this type of content more seriously, even when we know it leads to real-world harms.

Can you tell us how the bills before us today will help realign the incentives?

Mr. AHMED. Well, I think, comprehensively, what they do is give us more illumination as to the underlying rationale: the drivers, the business decisions, the economic rationale for allowing this content to remain on their platforms. And they really have.

I mean, look, the Disinformation Dozen, of their 98 social media accounts, 42 are still up. They still have around 52 percent of their audiences that they had before we wrote that report. So yes, some action has been taken. But for the main part, over half of it is still up there.

And why is that true? What these would collectively do is start to create some transparency and, therefore, accountability for those failures.

Mr. DOYLE. Thank you, Madam Chair——

Ms. RICH. Mr.——

Mr. DOYLE. [continue]. For holding this hearing, and I yield back.

Ms. SCHAKOWSKY. Thank you, Mr. Doyle. We are honored to have your presence today.

I want to now recognize Representative Lesko for your 5 minutes.

Mrs. LESKO. Thank you very much, Madam Chairman, and thank you to all of the panel members for testifying today. This is such an important issue.

It has been said that false information spreads so much faster on social media than accurate information, and I found that to be true. And I think a lot of it is because people, you know, whether it is media outlets or whoever it is, want us to have salacious titles and

things so that we click on it, and then—and use it. But my first question is for Jessica Rich.

Jessica, the FTC recently released the draft fiscal year 2022 through 2026 plans. I understand Chairman Khan deleted language from the FTC mission that specifically says that the FTC will accomplish their mission without unduly burdening legitimate business activity. How concerned are you that this altered mission statement could lead to increased costly regulatory burdens on businesses?

Ms. RICH. The deletion of that language sends a really bad message. And I would like to think of my former agency that it was a mistake. But one—and they should—and that they are planning to put it back in.

One thing that is important to remember is that, regardless of whether that language is in a mission statement, that concept runs throughout so much law and policy at the FTC that, regardless of mission statement or no mission statement, it is going to be very hard to ignore undue burdens on legitimate business activity. It is built into deception, it is built into unfairness, it is built into substantiation, fencing in so many doctrines.

But it was very ill-advised to take it out of the mission statement, and it sends a terrible message.

Mrs. LESKO. Thank you for that answer. And also to you, Jessica Rich, as you said, you are a former FTC director of the Bureau of Consumer Protection. What is your reaction to the—granting the FTC civil penalty authority language in the mission statement, or granting them civil penalty authority?

Ms. RICH. Under the Build Back Better Act. The FTC badly needs stronger remedies, especially with the rollback of 13(b) authority. But it would be far better for both the FTC and the public if this type of authority came with more direction from Congress regarding the situations that—where this would apply.

One thing to note that hasn't been talked about very much is that, even with this new authority, the FTC will still need to prove that any company, before paying civil penalties, has knowledge that they are violating the law. So that would be an important safeguard that would still be in there.

Mrs. LESKO. All right, thank you very much. My next question is for Mr. Rick Lane.

Areas of clear vulnerability—and you have said it in your testimony—to putting our sensitive, personal data at risk are those situations where sensitive, personal information is stored in foreign countries known to be hostile to the United States—one, namely, is China. Mr. Lane, how important is it that any reforms to Section 230 also include reforms to transparency, and content moderation practices, and them storing our personal information?

Mr. LANE. I think it is very important. We have, actually, treaties now that we have signed about how we can't require data localization, and so we can't say where people can store, based on our treaties, and that should be looked at, as well.

But in terms of what is happening with TikTok and others, I do believe that we need to take a closer look at how this data is being accessed, who is accessing it.

One of the concerns I have is, if you have ever seen the documentary "A Social Dilemma," is where they show the—you know, supposed to be Facebook or—turning the dial to try to influence our behaviors just a little bit. You know, elections are won and lost by two percentage points sometimes. And I would hate to see that there is information that is being derived that is just—someone behind the scenes is turning that dial who may be hostile to our U.S. interest.

Mrs. LESKO. Well, I agree with you, and I did watch "Social Dilemma," and I think it is very interesting, because it kind of opens your eyes on how we are being influenced behind the scenes.

Thank you, Madam Chairman, and I yield back.

Ms. SCHAKOWSKY. The gentlewoman yields back, and now I recognize Congresswoman Blunt Rochester for her 5 minutes of questions.

Ms. BLUNT ROCHESTER. Thank you, Madam Chairwoman, for the recognition, and allowing me to join this very important and timely hearing.

The internet's remarkable power and potential have been used to create, unite, and innovate. Unfortunately, it has also been misused by bad actors to misinform, divide, and distract, preying on unsuspecting Americans. This hearing today represents a bipartisan consensus that large tech companies must reform their practices to ensure the internet remains a place of innovation and potential. The common denominator underlying the horrible things that we have heard about today is the ability for tech companies to use design practices to undermine user choice for the sake of profit.

For my part, I introduced the bipartisan and bicameral DETOUR Act, because tech companies have used decades' worth of research on compulsion and manipulation, often conducted on the gambling industry, to design products that trick or strong-arm people into giving up their data or consent to potentially harmful content.

Today we often call these "dark patterns," and they exist on virtually every tech platform today, because this data collection scheme fuels the algorithms and targeted ad programs we have decried in a bipartisan way.

If we allow tech platforms to hamper Americans from making choices in their own self-interest, we will never see the internet reach its full potential.

Dr. Marechal, I would like to begin with you. Can you provide us an example of a dark pattern that undermines user choice on the internet today?

And what makes these tactics so ubiquitous online, and so effective in influencing user behavior?

Dr. MARECHAL. Absolutely, ma'am. Since the GDPR and CCPA, internet users have gotten used to seeing data collection consent pop-ups when they visit websites. And the point of that is to give us choice over whether or not to share—to make our—make it possible for companies to collect our data. But this is undermined by the type of deceptive design that you are talking about.

You have noticed, I am sure, that many of them make it much, much easier to allow the website to collect whatever data it wants than to refuse that permission, or to get details about what data

we want to allow or not to be collected. Even someone like me, who is onto them, I am often pressed for time, and so I click accept, rather than going through half a dozen more clicks to limit the data collection to what is needed for the website to work properly.

Ideally, sites should only be able to collect the data that they actually need to do the thing you want them to do. But, at a minimum, it should be just as easy to protect your privacy as it is to give it away.

Ms. BLUNT ROCHESTER. Great, thank you so much.

And Mr. Golin, why is it important that we consider regulation of dark patterns that target children, especially those that cause compulsive behaviors?

Mr. GOLIN. Yes. Well, we should regulate dark patterns that are aimed at children for three reasons.

The first of all is because, as you mentioned, they are extremely prevalent. Most of the apps and the games that children are on use manipulative techniques, finally owned by endless A/B testing, in order to get kids to stay on platforms longer, in order to get them to watch more ads, and in order to get them to make in-game purchases.

The second reason that we should do it is because it is unfair. You know, that—when the idea is to undermine user autonomy and to manipulate children, that is unfair. Just a couple of examples. There are preschool apps aimed at very young children, where the characters in the game start mocking children if they try to stop playing, and taunt them into playing even longer. And you know, so many of the games that children play use virtual currencies that have no fixed rate, and so they manipulate those currencies, and—so kids don't understand, when they are buying things with real money, how much money they are actually spending.

And finally, we should regulate them because they cause harm to children. There is the financial harm that I just mentioned, where kids are racking up hundreds and thousands of dollars in in-game purchases, but they are also being used to drive compulsive use, to get kids to have more screen time, which, of course, displaces things that would be—that they could be doing that would have much more benefit to them.

Ms. BLUNT ROCHESTER. Yes, and also contribute to healthy child development. I think you are correct.

And Mr. Greenblatt, you know, a lot of times we hear, when we discuss dark patterns, about things that companies shouldn't do. But can you—you, you know, mentioned the Social Pattern Library, and it considers some very important things. What are good design principles? Can you describe some of the findings and recommendations that ADL made, as part of the Social Pattern Library?

Mr. GREENBLATT. Yes, thank you for the question. A few points.

I mean, number one, nudges are very useful. And we have seen services like YouTube and Twitter implement them based on our recommendations, and actually decrease the prevalence of hate on their platforms.

Number two, doing things like turning off the automatic auto reel that you often see on services like YouTube. So the videos keep

playing over and over again, and the young people, the children, are just fed this content without actively choosing it.

Number three, another design principle is you don't have to have, let's say, controversial videos. I think you have to have controversial videos, but videos that violate the policies, if you will, there is just no reason to be promoting them. They should be taken down. But while they are being viewed, you don't have to put them in search.

There are lots of little techniques that product managers can do in order to iterate the results slightly in a way that is consistent with preserving freedom of speech, but that doesn't——

Ms. BLUNT ROCHESTER. Thank you.

Mr. GREENBLATT [continue]. Will promote the fringes.

Ms. BLUNT ROCHESTER. Yes, my time has run out, but I will follow up with a question for Mr. Ahmed.

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

Ms. BLUNT ROCHESTER. And thank you so much, Madam Chairwoman, for this very important hearing, I yield back.

Ms. SCHAKOWSKY. Thank you.

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

Mr. WALBERG. Thank you, Madam Chairwoman, and I appreciate being waived on today. This is a hearing that I think is important, with multiple hearings we are doing on Big Tech and its impact.

I know members of this committee on both sides have long supported a comprehensive national privacy and data security framework, and we have a record of working in a bipartisan manner to achieve that. For that I am grateful. While many worthy proposals are being considered today, I fear that, without a bipartisan, cohesive framework, we will continue down a path of patchwork laws that confuse consumers and place undue compliance burdens on businesses.

We may have significant differences on issues such as Section 230 reform, but privacy, particularly when it comes to children, should be a no-brainer. Or maybe that is the wrong term to use. It should be a good-brainer. That is why I have introduced, with my good friend, Congressman Rush, a bipartisan bill that would update and modernize the Children's Online Privacy Act, or COPPA. I wish that it was part of the hearing today, but it isn't. But still, it can be in the future, and I hope it is.

Mr. Lane, as you know, this is not the only legislation aimed at enhancing child privacy laws. There are Democratic proposals in both the House and Senate, which reemphasizes my point that this should be a bipartisan issue.

However, I have concerns with some of the COPPA legislation that has been introduced, including language that would grant new authorities to the FTC that may unduly burden legitimate business activity, such as good actors that have FTC-approved self-regulatory guidelines. And so, Mr. Lane, could you speak to why elimination of self-regulatory guidelines is harmful, and what might be some unintended consequences of doing just that?

Mr. LANE. Sure, happy to, and thank you for the question.

First of all, I want to say I am a big supporter of reforming COPPA. I actually think it should start at 17 and go younger, and not at 16. I think it needs to be updated. Things have changed

since Ed Markey moved the bill back in 1998. But one of the pieces of the bill that is actually important that has not—that may be left out, or included in part of the—some of the reform bills, is the self-regulatory environment of having FTC-compliant COPPA entities being certified.

And the reason that we supported that in the past, and why we liked it, was it was to help parents. It was to help parents to know that, if their kids were going on a site that was for 12 and under, that there was some mechanism, though, that was like a Good Housekeeping Seal of Approval, because we were concerned that, as Jessica knows, the lack of resources at the FTC, they can't investigate everybody.

So we thought we could help put together a mechanism that would say we have a certification program that you go through. That certification program and that company can be certified by the Federal Trade Commission, and it would help provide parents with information that the sites that they were going to have their kids on would be COPPA-compliant.

Now there have been some bad actors, and recently one of those bad actors got booted from the program. They should have. And I would support stronger enforcement of those entities like—that are doing a great job.

But I think it may do a disservice to parents that, if they have to kind of guess and hope and pray that these thousands of websites that are targeting 12 and under are COPPA-compliant, I think that maybe that would just be a mistake.

Mr. WALBERG. Thank you. My legislation, of course, as you may know, raises the age for parental consent protections for children online from under 13 to under 16 years of age. It just seems that Big Tech, in this space, has a race to the bottom going on.

Mr. LANE. Yes. And if I can just add one other piece—and Jessica was actually one of the first individuals I reached out to on this—is this FinTech child privacy protection gap. Because what has happened is that, as kids are migrating into this digital e-commerce world, and having debit cards and digital wallets, those privacy rules are Gramm-Leach-Bliley, which is an opt-out regime, and you hope that the parents would opt out. As Congressman Cárdenas had basically said, no one reads the opt out, and no one opts out.

COPPA is for websites targeted 12 and under. So the concern is that, as you have this combination of kids' financial information being collected, and then tagging that along with social networking information, you have the perfect storm of underage kids having a whole dossier on them prior to them hitting 18. That could be detrimental to their future. And that gap, I think, needs to be filled by legislation.

Mr. WALBERG. I appreciate that. I have some more questions, but I don't have time. I will get them to you.

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

Mr. WALBERG. But I appreciate you adding that, because that is insightful. Thank you.

Ms. RICH. Can I make one quick point about the COPPA safe harbors?

Mr. WALBERG. If the chairperson allows it.

Ms. RICH. Can you——

Ms. SCHAKOWSKY. I am afraid that is going to have to go into the—to respond in writing.

Ms. RICH. OK.

Ms. SCHAKOWSKY. We have to move on. And I now recognize for 5 minutes Mr. Carter.

Mr. CARTER. Thank you, Madam Chair and Leader Bilirakis, for allowing me to waive on this hearing. I appreciate it very much.

Ms. Rich, I will go to you, but I have another question here. I want to go back to the exchange that you had with Ranking Member Rodgers.

We have got a lot of supply chain issues that are going on right now, and they can go beyond just a local retailer. Say I am the owner of a car dealership in Georgia, or a wine shop in Washington State, or even a grocer in a small town in West Virginia. I am paying more now than I was before to get access to products that aren't as available as they were before. I may have to charge more than I did a month ago, just simply because of the increased cost, obviously.

I don't know the ins and outs of the FTC Act, so aren't the processes—the process changes, the new authorities that the—that have been discussed today, and other actions going to cause a lot of confusion and—for me, as a retailer, and just for—trying to responsibly run my business?

Ms. RICH. I haven't done that analysis, but I do know that right now there is a lot of confusion about when the FTC instead chooses to pursue something through deceptive or unfair practices. And so the FTC is always better off when it has direction from Congress as to what the standards are for particular concerns like content moderation, privacy, et cetera. So I think, at least in many circumstances, direction from Congress decreases confusion.

Mr. CARTER. Decreases confusion.

Ms. RICH. Decreases confusion.

Mr. CARTER. OK.

Ms. RICH. Now, what I think maybe you are asking about, though, is the issue of having multiple sectoral laws, instead of one law together, which I have been advocating for privacy, where at least companies would be able to look in one place for a lot of direction about important issues like data use.

Mr. CARTER. Right.

Ms. RICH. And I do think having one comprehensive privacy law, which could include many of these elements in it, would be better off than having multiple sector rules.

Mr. CARTER. Look, I was in business for over 32 years, and I can tell you, first of all, I didn't have time to do all this kind of research. Secondly, I mean, we are inside baseball here. But many of these people, many of these business people, they don't know how to navigate all this.

Ms. RICH. I agree that multiple sectoral laws, which is in the area I am the greatest expert in, which is privacy, has not been good for small companies, or even big companies. But it definitely is worse for small companies who really can't figure out what laws apply to them.

Mr. CARTER. Right. All right, let me move on.

Earlier this year there were several Senate Democrats that sent a letter to Chairwoman Khan at the FTC, encouraging her to begin a rulemaking process on privacy. I am hopeful my colleagues in the Senate will second-guess this approach, once they know how complicated it truly is, because it is truly complicated, and we don't need it to be complicated. We need to simplify. Be Thoreauish: simplify, simplify, simplify.

Ms. Rich, I am also concerned with the timeliness that it is going to take to complete a rulemaking process on data. Can you shed some light on how long that process might take, and what that might mean for consumers and companies looking to understand all this patchwork of state laws?

Ms. RICH. There has been a tremendous overselling of the potential of the FTC to issue a rule on its own, using its Mag-Moss authority. Under that—that is a very cumbersome process. It requires—for each mandate in a rule, the FTC has to make—prove it is unfair, deceptive, and prevalent, and then there is all sorts of procedural hurdles. Many rules that have been pursued under this process have taken years to complete.

And also, given the controversy and all the debates surrounding privacy that have happened over the course of 20 years, the public would be best served if Congress is the one to make the tough choices in this area.

Mr. CARTER. Understood. But, you know, again, years of work that it is going to take in order to get this.

Ms. RICH. And litigation that would ?

Mr. CARTER. Absolutely.

Ms. RICH [continue]. Likely ensue.

Mr. CARTER. Absolutely. And, you know, most business owners just get so frustrated, they just throw their arms up, and they just—and a lot of them quit.

I have got a lot more, but I will submit it in writing, and thank you.

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

Mr. CARTER. And I will yield back, Madam Chair.

Ms. SCHAKOWSKY. The gentleman yields back. And last, but not least, Mr. Duncan, you are recognized for 5 minutes.

Mr. DUNCAN. Sometimes they save the best for last. I am not sure that is the case here. But I want to thank you and—Madam Chair, and the ranking member, for hosting today's hearing, and including my bill, the TELL Act. This legislation would disclose whether China and other—and their state-owned entities are storing, accessing, and transferring the personal data of American citizens without being transparent about it.

TikTok, one of the most popular social media platforms for our children, is a subsidiary of Beijing-based ByteDance. While I have notable concerns about American companies doing business in China, and accommodations they make to the People's Republic of China, it is astonishing to me that there is any doubt over the level of access and control the Chinese Communist Party has over this conglomerate and similar entities.

Mr. Lane, it is great to see you again. Thanks for being here. As this committee thinks about the future of internet, and holding Big Tech accountable, are you concerned about the data being collected

by TikTok and companies with similar relationships in China, and what that might mean for national security for our country?

Mr. LANE. I am concerned about that. I think we should all be concerned about that.

Mr. DUNCAN. Thank you. What other provisions on security vulnerabilities do you think we—should be incorporated in this legislation to protect our economic and national security interests?

Mr. LANE. Well, I think the legislation starts in the right place. You know, as parents, I like to say it is a teachable moment, that people will know where their information is being housed, and where the companies are based. And hopefully, they will take their self-correction action that is necessary.

But I also worry about those websites and other apps that are not going to disclose, and how do we find those. You know, as we know, Russia and Iran and China, you know, and the surrogates, are well-known cyber warriors. And there is going to be a lot of mischief underneath the ones that we see.

And my concern is that, you know, we have this dark WHOIS issue, where we could find out. So, combining your information, are they where they say they are, and headquartered where they say they are? We could find information like that out through an open, accessible WHOIS. That is what forensics does.

But unfortunately, you know, the NTIA and its bureaucrats have, for the past five years, stonewalled Congress taking action in this space. Congressman Latta was talking about the letters he sent to Homeland Security, the FTA, and others. And you have companies like VeriSign and GoDaddy and Namecheap, you know, they will be up on the Hill, talking to you guys about how we don't need to upset the multi-stakeholder process of ICANN. That process is now going on five years. And if—and five years of darkness. And if it—if they did develop something tomorrow, it would take three more years to implement.

Congress can act on this now. Congress has the opportunity to fix a cybersecurity problem at no cost to the U.S. taxpayer. It is in our hands. And you can ask any cybersecurity expert. I have reports, I have letters from the, you know, the top people talking about this. So adding your legislation on where they are, and where the data is being stored, on top of a strong WHOIS legislation to fix this GDPR problem—it is not a U.S. problem, it is a foreign government.

And I will end on this. Imagine if this law that shut down the WHOIS, that is threatening our national security, was a Chinese law or an Iranian law. Would we still stand here, as a U.S. Congress, and say we shouldn't all set the multi-stakeholder process to address these laws? The answer would be no. And I think it is time for the U.S. Congress to step up, and try to fix this problem before more people get hurt.

Mr. DUNCAN. You are exactly right. You know, Big Tech is not just Facebook or Twitter. It includes companies like Microsoft, and Apple, and Google, each of which has a significant presence in China.

My time is going to expire. I had another question, but I just want to make this point, because I thought about this while you were speaking.

I don't know that we truly care about all this being collected from our children through platforms like TikTok and others. And I raise that awareness because, for the past two congresses, I have tried to get this committee and this Congress to find one Democrat to cosponsor a piece of legislation that would stop the importation of child-like sex dolls, dolls that are used by pedophiles.

Images, likenesses that are stolen from social media platforms, the doll created, crafted to look like the child of one of our constituents, so that someone can play out sex fantasies with a child-like sex toy, a doll. Very humanlike, very robotic, where even the voice is taken from the child's TikTok, and digitally put into that child-like sex toy, so that it can actually talk like that child to the pervert that is enjoying themselves with it.

Madam Chair, find me a Democrat that will cosponsor that, and let's get that over, and let's stop the importation of child-like sex dolls. When I talk to your colleagues, "Oh yes, we"—yes, I will show them pictures of the dolls. I will be glad to share them with you. "Oh my God, we need to do something about that," and nothing is done, and so we continue to import sex dolls into this country that look like the children of people in our communities, sound like the children of people in our communities. And it is just wrong.

With that I yield back.

Ms. SCHAKOWSKY. The gentleman yields back, and that concludes the questioning.

And I want to thank, from the bottom of my heart—this has been a wonderful panel, and I thank all of you for the work that you have done. And I know that it will lead to real action, I believe, in the Congress.

And before we adjourn, let me also just thank my ranking member.

I don't know if you wanted to make any final comment for our witnesses. OK, you are OK?

And I request unanimous consent to enter into the formal—the following document into the record: an online tracking study.

Without objection, so ordered.

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

Ms. SCHAKOWSKY. And just stay for one more second, because I want to remind members that, pursuant to committee rules, they have ten business days to submit additional questions for the record—I know there were some unfinished questions that need answers—to be answered by the witnesses who have appeared today.

And I asked the witnesses to respond as promptly as possible to any questions that may come to you.

Once again, thank you. Thank you to—the participation. There were five waive-ons to this committee, which is a lot, showing the kind of interest in this committee.

And, at this time, the subcommittee is adjourned.

[Whereupon, at 2:52 p.m., the subcommittee was adjourned.]

Office of Congressional Relations

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536

U.S. Immigration and Customs Enforcement

July 16, 2020

The Honorable Robert E. Latta
U.S. House of Representatives
Washington, DC 20515

Dear Representative Latta:

Thank you for your June 24, 2020 letter to U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI) and the National Intellectual Property Rights Coordination Center (IPR Center) regarding the European Union's General Data Protection Regulation (GDPR) and its impact on HSI's ability to obtain WHOIS information in support of its criminal investigations.

HSI uses domain name registration information, previously available via online WHOIS query, to aid in the identification of persons or entities responsible for registering domains that are used to conduct a wide variety of crimes, which include intellectual property crimes, cyber-crimes (such as theft of personally identifiable information [PII] and credit card information), crimes related to illegal importation and exportation of goods, and the promotion and distribution of child sex abuse material.

HSI used WHOIS data regularly prior to the implementation of GDPR in May 2018. Subsequent to GDPR, the inability to conduct instant electronic queries has added an extra step and slowed down the investigative process. HSI continues to request and use domain name registrant information via legal process from registrars who maintain that information. The registries and registrars review requests for information and determine if the requestor has the authority, if the order was issued by a court of competent jurisdiction, and whether the request violates any portion of the GDPR. Unfortunately, there is no centralized point of contact from whom to request the information, and with over 2,000 registrars, some outside of the United States, it is sometimes difficult to determine who to contact and how to procure a legal order they will recognize and respond to. In addition to slowing the process to get registrant information, the likelihood of getting a judicial order for the release of information can be difficult since a number of requests are made in the initial stage of an investigation or response and agents may not have enough information on the criminal activity to satisfy necessary requirements. Lastly, due to the penalties that can be imposed by GDPR for improper release of a registrant's PII, many registries and registrars are redacting registrant information regardless of whether or not the subject is a citizen within the European Union.

As a recent example of GDPR inhibiting HSI investigations, the HSI Cyber Crime Center (C3) Cyber Crimes Unit identified several websites posing as legitimate coronavirus disease 2019 (COVID-19) fundraising organizations, but are actually fraudulent. These websites claim to be sites for entities such as the World Health Organization, United Nations' foundations, and other non-governmental organizations, and appear to be legitimate. When HSI conducted WHOIS queries for these domains, most of the subscriber information was redacted as a result of GDPR. Having

increased and expedient access to domain name registration information would have allowed HSI to identify the registered owners of the domains expeditiously in order to prevent further victimization by these illegitimate fundraising websites. When HSI is required to use legal process (e.g. administrative subpoenas, non-disclosure orders, or grand jury subpoenas) to obtain registrant information, this can cause delays and potentially negatively impact an investigation.

HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain.

In an effort to address the challenge of limited WHOIS information as a result of GDPR, the HSI C3 has assigned full-time representatives to the Public Safety Working Group (PSWG) within the Internet Corporation for Assigned Names and Numbers (ICANN) organization. The PSWG is comprised of law enforcement and consumer protection agencies that work closely with various constituencies that are represented within the ICANN ecosystem. In the absence of a more viable solution, HSI C3 members on the PSWG continue to work with registries, domain registrars, and civil society groups to develop a consensus solution for access to domain name registration information within the ICANN framework and compliant with GDPR.

Thank you again for your letter and interest in this matter. Should you wish to discuss this matter further, please do not hesitate to contact me at (202) 732-4200.

Sincerely,

Sean Hackbarth
for

Raymond Kovacic
Assistant Director
Office of Congressional Relations

FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

CATHY McMORRIS RODGERS, WASHINGTON
RANKING MEMBER

ONE HUNDRED SEVENTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

December 8, 2021

The Honorable Lina Khan
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Chairwoman Khan:

We write to you regarding our significant concerns about the trajectory of the Federal Trade Commission (FTC). Historically, the Commission has operated in a bipartisan manner to carry out its responsibility to protect consumers without unduly burdening legitimate business activity. Under your leadership, it appears that is no longer the case.

There have been many partisan FTC decisions this year that followed questionable procedure. This ill-conceived practice not only leaves the FTC vulnerable to legal challenges, but it also undermines the FTC's mission to protect consumers. As the head of the FTC, an independent agency, you are responsible for ensuring that the Commission's decision-making process is legally sufficient. Using unprecedented and questionable procedures to advance the White House's partisan progressive agenda will diminish the FTC and your legacy as Chairwoman.

We also note that the FTC's record has been a failure when it follows a flawed decision-making process in pursuit of a radical agenda. In the 1970s, the Commission "embarked on a vast enterprise to transform entire industries. Over a 15-month period, the Commission issued a rule a month, usually without a clear theory of why there was a law violation, with only a tenuous connection between the perceived problem and the recommended remedy, and with, at best, a shaky empirical foundation."[1] This process of issuing solutions in search of a problem

[1] Howard Beales and Timothy J. Muris *Striking the Proper Balance: Redress Under Section 13(b) of the FTC Act* (April 26, 2016), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764456

was an effort "to become the second most powerful legislature in Washington" [2] and to target companies across America, discouraged them from growing. A better avenue for your leadership is building bipartisan consensus amongst your colleagues and Congress. Through that approach, support for important initiatives is cemented and does not become vulnerable to funding limitations and oversight of improper communications and coordination, which in the end cripples the FTC's enforcement standing in court review.

In addition, we are concerned by reports that former-FTC Commissioner, and current Director of the Consumer Financial Protection Bureau (CFPB), Rohit Chopra, continued to influence and participate in FTC business after he was no longer a member of the Commission. According to an article in Politico, Director Chopra's "zombie" vote has continued to be counted in FTC decisions after he was no longer on the Commission.[3] The article indicates that as a "former Commissioner," CFPB Director Chopra cast as many as 20 votes by email on October 8, 2021, his last day at the FTC. The article also suggests that these votes have continued well past Director Chopra's tenure at the Commission.[4]

The use of these "zombie" votes is just one example of the FTC's questionable decision-making process and invites legal challenges. It is sloppy process, and it is unnecessary. Even FTC veterans have questioned the necessity of such extreme procedures. Former Chairman William Kovacic stated, "I don't know what you gain if [FTC nominee Alvaro] Bedoya is coming in. Why push that document out the door? Why is the end of October better than the end of December or January?"[5]

The latest example of questionable judgment is your decision to delete "without unduly burdening legitimate business activity" from the FTC's draft strategy plan for fiscal years 2022 to 2026.[6] This language has been included in FTC mission statements for decades, through both Republican and Democrat administrations. Your amendment suggests the FTC is departing from its traditional focus on protecting consumers from fraud, as well as ensuring businesses have clear rules to follow, in favor of an unorthodox interpretation of its antitrust mission to reshape the American economy.

Given our concerns with the deficiency of FTC's recent decision-making process, we ask that you respond to the following questions no later than December 22, 2021 and provide a copy of all rules relating to the FTC voting process immediately upon receipt of this letter.

1. Did President Biden, or any other members of his senior staff -- such as National Economic Council (NEC) special assistant Tim Wu, who reportedly "asked the FTC to

---

[2] *Id.*
[3] Leah Nylen, *'Zombies' to the rescue: The arcane voting rule that could saves Dems' antitrust agenda,* Politico (November 08, 2021), *available at* https://www.politico.com/news/2021/11/08/voting-rule-democrats-antitrust-519767
[4] *Id.*
[5] *Id.*
[6] Federal Trade Commission, *Draft FTC Strategic Plan for FY2022*-2026 (November 12, 2021) *available at* https://www.regulations.gov/document/FTC-2021-0061-0001

see if [you] can craft a rule around data collection"[7] -- request, influence, or pressure you in any way to hold a vote on any matter before the Commission? If yes, please be specific about what those items are and the nature of the involvement by the White House.

2. Did CFPB Director Rohit Chopra, or any member of his staff, request, influence, or pressure you in any way to allow him to vote on a matter before the Commission after Director Chopra had departed the Commission? If yes, please be specific about what those items are and who were the individuals involved.

3. Was Director Chopra briefed on the matters considered by the Commission on October 25, 2021? If yes, when did that briefing occur, and who was present at that briefing?

4. Have you received any legal guidance from your staff, other Commissioners, the White House, or outside consultants regarding this "zombie" voting practice? If so, please provide copies of such guidance to the Committee.

5. Has the Commission provided briefings to Alvaro Bedoya, President Biden's FTC nominee, on any matters before the Commission?

6. Are there any staff, on their own or at your request, still communicating with CFPB Director Chopra regarding any matters before the Commission? If so, please provide the Committee with all records of those communications.

7. Has Director Chopra contacted you, directly or indirectly, regarding any matters before the Commission? If so, please provide the Committee with all records of those communications.

8. Would coordination with CFPB Director Chopra on a matter before the FTC or the CFPB raise any procedural concerns, including but not limited to conflicts of interest or ex parte communications?

9. With Director Chopra's alleged "zombie" votes, please address the details of the Politico report and the discretion you have over how to use former Commissioner Chopra's votes.

    a. Will you continue to use "zombie" votes?

    b. Do you consult with all other Commissioners before using "zombie" voting?

10. Of the alleged 20 "zombie" votes cast by CFPB Director Chopra, the only publicly available vote occurred on October 25, 2021, on a high profile 3 to 2 partisan split to

[7] Leah Nylen, *White House likely to push for privacy legislation as FTC crafts rules, Wu* says Politico (September 30, 2021) *available at* https://subscriber.politicopro.com/article/2021/09/white-house-likely-to-push-for-privacy-legislation-as-ftc-crafts-rules-wu-says-3991475

approve a policy statement requiring FTC approval before companies may engage in a merger:

a. Did you consult with CFPB Director Chopra before his vote was used to pass the policy statement? If so, who consulted with Director Chopra, and when did the consultation occur?

b. Was CFPB Director Chopra informed of the FTC business before any other Commissioners?

11. Is the use of "zombie" voting consistent with your commitment to openness and transparency at the FTC?

12. Why are you deleting "without unduly burdening legitimate business activity" from the FTC's strategic plan?

    a. Which FTC Commissioners did you consult with before proposing this amendment?

        i. Did those Commissioners agree with your decision to delete the language?

        ii. If you did not consult other Commissioner before proposing such drastic change, why not?

13. Will you direct Commission staff to examine any potential unintended burdens to legitimate business activity that may result from proposed FTC actions?

    a. How does the amended FTC mission statement relate to section 31502 of the Build Back Better Act on first offense penalty authority, which is pending before the Senate?

    b. What is the policy case for how section 31502 will further protect consumers from unfair or deceptive acts or practices versus current law?

    c. What will be the Federal budgetary impact of this proposal if no person, partnership, or corporation is determined to have violated the FTC Act's prohibition of unfair or deceptive acts or practices?

    d. What additional costs might a person, partnership, or corporation face if section 31502 becomes law?

    e. Will you initiate any action, including but not limited to an enforcement action, against a person, partnership, or corporation, pursuant to section 31502, if that action will negatively impact legitimate business activity?

We look forward to a timely response to this letter, technical assistance on the comprehensive privacy and data security discussion draft we have previously shared with your team, and your future appearances in front of the Committee on Energy and Commerce. If you or your team have any questions about our request, please contact Tim Kurth and Brannon Rains at the Committee on Energy and Commerce at (202) 225-3641. We appreciate your prompt attention to this matter.

Sincerely,

Cathy McMorris Rodgers
Republican Leader

Gus Bilirakis
Republican Leader
Subcommittee on Consumer Protection
and Commerce

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Chairman

July 30, 2020

The Honorable Robert E. Latta
United States House of Representatives
Washington, D.C. 20515

Dear Representative Latta:

Thank you for your June 24, 2020 letter requesting information about how the Federal Trade Commission ("FTC" or "Commission") uses domain name registration information, also known as WHOIS, to carry out its law enforcement mission, including its efforts to stop frauds related to COVID-19. You also highlighted your concerns that the implementation of the European Union's General Data Protection Regulation ("GDPR") has negatively affected the ability of law enforcement to identify bad actors online. I share your concerns about the impact of COVID-19 related fraud on consumers, as well as the availability of accurate domain name registration information.

Since the beginning of the pandemic, the FTC has been monitoring the marketplace for unsubstantiated health claims, robocalls, privacy and data security concerns, sham charities, online shopping fraud, phishing scams, work at home scams, credit scams, and fake mortgage and student loan relief schemes, and other deceptions related to the economic fallout from the COVID-19 pandemic.[1] In response, we have taken actions, including filing four cases in federal courts and sending hundreds of warning letters to businesses in the United States and abroad.[2] In addition, we have conducted significant public outreach and education efforts.[3]

Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud.[4] The FTC uses this information to help identify wrongdoers and their locations, halt their conduct, and preserve money to return to defrauded victims. Our agencies may no longer rely on this information because, in response to the GDPR, ICANN developed new policies that significantly limit the publicly available contact information relating to domain name registrants. For

---

[1] *See generally* Prepared Statement by the Federal Trade Commission before the S. Comm. on Commerce, Science, and Transp., Subcommittee on Manufacturing, Trade, and Consumer Protection: Consumer Protection Issues Arising from the Coronavirus Pandemic (July 21, 2020), https://www.ftc.gov/public-statements/2020/07/prepared-statement-federal-trade-commission-consumer-protection-issues.

[2] *See generally* https://www.ftc.gov/coronavirus. This page is updated regularly.

[3] *Id.*

[4] *See, e.g.,* Comment of the Staff of the FTC Bureau of Consumer Protection before the ICANN Public Comment Forum, In the Matter of Tentative Agreements among ICANN, U.S. Dep't of Commerce, and Network Solutions, Inc. (Oct. 29, 1999), https://www.ftc.gov/policy/policy-actions/advocacy-filings/1999/10/ftc-staff-comment-internet-corporation-assigned-names; Prepared Statement of the Federal Trade Commission, Hearing on Internet Governance: The Future of ICANN, Before the Subcommittee on Trade, Tourism, and Econ. Dev. of the S. Committee on Commerce, Science, and Transp., 109th Cong. (Sept 20, 2006), http://www.ftc.gov/os/testimony/P035302igovernancefutureicanncommissiontestsenate09202006.pdf.

example, before the GDPR went into effect, the FTC could quickly and easily obtain detailed information about the name, address, telephone number and email of the domain name registrant by typing a simple query. Since May 2018, however, we generally must request this information directly from the particular registrar involved. This can be a time-consuming and cumbersome process.[5]

This lack of access also limits consumers' ability to identify bad actors using WHOIS information. Prior to the GDPR, thousands of the complaints filed in our Consumer Sentinel complaint database referred to the filer's use of WHOIS data to identify businesses involved in spyware, malware, imposter scams, tech support scams, counterfeit checks, and other malicious conduct.[6]

The FTC would benefit from greater and swifter access to domain name registration data. Achieving this goal is difficult, however, given the complexity of the GDPR's effect, the required international coordination, and the many stakeholders involved. We have been working with other U.S. agencies to develop solutions through our interaction with ICANN and our international law enforcement colleagues.

One approach that could help overcome the current obstacles would be to mandate disclosure of domain name registration data associated with legal entities, as opposed to natural persons. Legal entities register a significant percentage of domain names, and the GDPR protects the information of natural persons but does not apply to information related to legal entities. ICANN's current mechanisms result in over-application of the GDPR by permitting registrars to choose whether to make the registration data of legal entities public or not. We have raised this issue within ICANN's policy development process.

I appreciate your interest in these issues. If you or your staff has additional questions or comments, please contact Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195.

Sincerely,

Joseph J. Simons

Joseph J. Simons
Chairman

---

[5] There are more than 2,500 ICANN accredited registrars, many located outside the U.S., with different procedures to obtain registrant data. It can be challenging to determine where to direct a request and what to include in such request for access to this now non-public information as many registrars fail to place such guidance in a location that is easy to find on their websites. After submitting a request, the FTC must wait for the registrar to approve or reject our requests. Moreover, when data is located in a foreign jurisdiction, the process may be more time consuming and require cooperation from our law enforcement partners.

[6] In 2017, we identified over 4,000 complaints filed over a five-year-period.

August, 13, 2020

The Honorable Robert E. Latta
U.S. House of Representatives
Washington, DC 20515

Dear Congressman Latta:

Thank you for your letter of June 24, 2020 regarding the Coronavirus outbreak (COVID-19) and inspections. We appreciate your interest in ensuring that the Food and Drug Administration (FDA or the Agency) has the necessary tools to combat fraud and ensure the safety and supply of pharmaceuticals, human and animal food, and medical supplies. As you are aware, the U.S. Government is accelerating response efforts due to COVID-19. FDA appreciates your support, and that of Congress, as we all work together toward a united goal of controlling this outbreak.

To that end, we offer the following responses to your specific questions, broken into Criminal and Civil responses, as we have two offices that utilize WHOIS:

1. If and how your office uses or has used WHOIS in the execution of its functions?

Criminal Case Investigations

Access to WHOIS information has been a critical aspect of FDA's mission to protect public health. Implementation of the E.U. General Data Protection Regulation (GDPR) has had a detrimental impact on FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients.

WHOIS data has also been widely used in FDA's criminal investigations to identify individuals and organizations selling online a variety of unapproved/uncleared/unauthorized products such as opioids, counterfeit or adulterated drugs as well as purported dietary supplements containing deleterious or undeclared ingredients. Most recently, lack of WHOIS transparency significantly hindered FDA's ability to identify sellers of fraudulent and unproven treatments for COVID-19 as well as illegitimate test kits and counterfeit or substandard personal protective equipment. These cases range from a simple website marketplace to sophisticated transnational cybercrime networks involving thousands of websites, hidden servers, dark web applications and virtually linked co-conspirators. Many of these criminal conspiracies were linked or identified via historical WHOIS analysis.

FDA's ability to effectively regulate industry relies on transparency with the manufacturers and distributors of the products regulated by FDA. WHOIS data are frequently used to determine the owner or operator of particular website in the context of our regulatory duties. FDA has used WHOIS data to trace foodborne contamination or product tampering supply chains, contact website owners about illegal or deceptive

U.S. Food & Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
www.fda.gov

marketing or labeling online, as well as to notify online sellers about a company that has recalled products and issue Warning Letters to online sellers.

Finally, WHOIS data are an essential resource in conducting cybersecurity incident response and threat related assessments/investigations. The security and protection of FDA critical assets and infrastructure is often contingent on the identification and validation of the owners and operators of these internet resources. Specifically, the potential loss of access to WHOIS data in the cybersecurity context as part of the enforcement of GDPR would negatively impact FDA's ability to effectively analyze and validate external connections (IP addresses) within the European Union (EU).

Consistent with ICANN's (Internet Corporation for Assigned Names and Numbers) Bylaws, FDA's access to WHOIS data is essential for "the legitimate needs of law enforcement" and for "promoting consumer trust."[1] FDA's legitimate interests are also consistent with the recitals to the GDPR, which permit processing of personal data for "preventing fraud;" "ensuring network and information security," and reporting possible "criminal acts or threats to public security" to authorities.[2]

Civil Case Investigations

FDA's Health Fraud Branch (FDA-HFB) routinely accesses WHOIS databases to obtain information on the domain registrants for websites selling FDA-regulated commodities. FDA-HFB has a subscription to a database that also provides historical WHOIS data, as well as other data necessary to conduct internet investigations. FDA-HFB uses and has used WHOIS data to identify the recipients of warning letters, determine responsibility of FDA-regulated operations from a given domain or website, establish connections or relationships among different domains or to gather additional data points (email addresses, phone numbers, IP addresses) as part of Agency investigations.

2. If and how your office has experienced increased difficulty (including delays) in accessing WHOIS information since the May 2018 implementation of the EU GDPR?

Criminal Case Investigations

Although a small number of domestic registrars will offer WHOIS data pursuant to a written request, FDA cannot access WHOIS information without a Grand Jury subpoena, and WHOIS data is no longer available for foreign registrars. Unlike some other federal law enforcement agencies, FDA's Office of Criminal Investigations (OCI) does not have authority to issue an administrative subpoena for basic WHOIS data or WHOIS data shielded by a privacy/proxy service. Because FDA cannot access basic WHOIS data

[1] ICANN Bylaws, Registration Directory Services Review, §4.6(e).

[2] *See GDPR* Recitals 47, 49 and 50.

without a Grand Jury subpoena, which requires coordination with the Department of Justice, many investigative leads have not been sufficiently addressed or significantly hindered.

Civil Case Investigations

More often, the data in WHOIS reports in the searches that FDA-HFB is conducting are either missing, redacted or hidden via a proxy registrant for domains. This proxy service is the point of contact for any inquiries regarding the domain. There are hundreds of ICANN accredited registrars that provide proxy registrant services and in very few instances have these registrants been cooperative in providing non-public data to FDA about the owners and operators of a domain. In some cases, these proxy services refer any inquiries to the domain registrar, which provides only the publicly-available, redacted or missing WHOIS data. FDA-HFB has found that Regulation (EU) 2016/79, or GDPR, extends to domains that may not be operating strictly within the EU. In a recent example, one registrar cited the GDPR compliance requirements as the basis to broadly restrict WHOIS data, claiming the burdensome technical difficulties necessary to differentiate among customers on the basis of their likely geographic locale.

3. If and how your office would be able to more effectively conduct investigations and/or intercede in illegal activity with greater WHOIS access?

Criminal Case Investigations:

Greater WHOIS access would significantly assist FDA with the identification of individuals and firms illegally selling FDA-regulated products online. WHOIS adds a layer of transparency to websites, online marketplaces and vendors, and enables our regulatory, cybersecurity and law enforcement personnel to link seemingly disparate websites into organized affiliated networks and track historical domain name ownership.

In the past, suspects operating ecommerce websites illegally selling FDA-regulated products had to provide point of contact (POC) information. After developing sufficient probable cause, OCI agents investigating fraudsters could use this information as part of an affidavit to obtain search warrants. These search warrants often provided agents with additional investigative leads that helped identify the suspect(s), detailed information on the criminal scheme, location of ill-gotten assets and other items of value in a criminal investigation. Agents could also conduct "reverse WHOIS" searches using POC information provided by the suspects. This data has been used to link the suspect(s) to other affiliated websites. Now that WHOIS information is no longer available, it is extremely time-consuming, and in some instances not possible, for agents to fully identify the entire scope of an illicit online network.

Civil Case Investigations:

FDA-HFB would be able to quickly and efficiently identify and respond to the unlawful sales of FDA-regulated products if complete and accurate WHOIS data were available.

As noted above, establishing connections or determining responsibility of website owners and operators where WHOIS data are redacted or missing can be resource intensive, causing delays that can complicate investigations and cases.

Thank you again for your concern and contacting us regarding this matter. If you have any questions, please let us know.

Sincerely,

Karas Gross

Karas Gross
Associate Commissioner for
Legislative Affairs

Attachment—Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Holding Big Tech Accountable: Legislation to Build a Safer Internet."
December 9, 2021

Mr. Rick Lane, CEO, Iggy Ventures, LLC

The Honorable Michael C. Burgess (R-TX)

1. Mr. Rick Lane, the Courts ruled in *Force v. Facebook* that a platform arranging and distributing third-party information – such as through the use of algorithms – does not amount to being an information content provider; therefore, algorithms as they are used by internet platforms to promote user content will receive Section 230 immunity. Should Congress evaluate law changes to increase transparency and accountability of algorithms used by internet platforms?

   Response: Yes. In order to address concerns such as misinformation, bias, hate speech, or other "awful but lawful" speech related issues, Congress should enact strong transparency requirements that apply to both algorithmic and non-algorithmic content moderation. I am concerned that singling out just algorithmic moderation could raise First Amendment issues in light of the recent federal district court decision in NetChoice v. Paxton.

   Democrats and Republicans alike have expressed frustration with the opaque and inconsistent way platforms engage in content moderation. The Supreme Court has held that the First Amendment allows the government to require that commercial enterprises provide "purely factual and uncontroversial information about the terms under which [their] services will be available," where the "disclosure requirements are reasonably related to the State's interest in preventing deception of consumers." In any CDA 230 reform legislation, Congress should adopt transparency provisions that require each platform to: 1) publicly disclose its content moderation policies; 2) create a process by which users can file a complaint with the platform arguing it did not follow its own policies; 3) create a process by which users can appeal a platform's decision to take down or leave up specific content, or to terminate or not terminate service to a user; and 4) publicly disclose information about the decisions the platform has made to take down or leave up certain content, or to terminate or not terminate service to a user.

   Platforms that violate these transparency requirements or policies contained in their terms of service would lose the section 230 shield and thus could be culpable for breach of contract or a deceptive trade practice. These transparency requirements would also better enable individuals and businesses to decide what platforms to use—potentially prompting new entrants and existing providers to compete based on content moderation practices,

thereby promoting innovation. In addition, the public disclosure requirements would allow policymakers, law enforcement, and researchers to track problematic trends—either with users' online misbehavior or the platforms' moderation practices—and develop strategies to address them.

We must return the rule of law to the Internet. Until we hold online platforms (TikTok, Reddit, Facebook, Google, etc.) and other Internet intermediaries (Cloudflare, Verisign, GoDaddy, the Internet Society (ISOC), Namecheap, and even the Internet Corporation for Assigned Names and Numbers (ICANN), etc.) equally accountable as brick-and-mortar businesses, people will be less safe online. Therefore we need to restore to platforms the ordinary duty of care that would apply but for courts' current, overbroad application of section 230. Congress should amend section 230 to require that platforms and other Internet intermediaries take reasonable steps to curb illegal conduct online as a condition of receiving the section's protections. If platforms could be held both criminally and civilly liable for irresponsibly enabling such transactions, they'd be much more likely to pay attention and curb the activity. By making simple language changes to section 230 that restore the duty of reasonable care, Congress could help combat not just Internet opioid and fentanyl sales but all current and future illegal activity online. And in a non-regulatory, pro-free market way that both conservatives and liberals should be able to support: creating meaningful incentives for platforms to find the most effective and efficient ways to prevent online harm.

Congress also needs to rectify the "Dark Whois" problem that was created by an overly broad interpretation of the European Unions General Data Protection Regulation (GDPR) by immediately passing legislation requiring domain name providers like Verisign, Godaddy, NameCheap, to once again make accurate WHOIS information available for legitimate purposes. The lack of access to WHOIS data is hindering not only cyber security and anti-terrorism efforts, but investigations into illegal online drug sales. What good is it to have "transparency and accountability" requirements for websites if you cannot find out "Whois" behind those websites. It is critical that for any legislative solution being considered by Congress to address these real concerns to work there must be an open and accurate Whois database. Without an open and accurate Whois, the Internet becomes no better than the Dark Net.

Unfortunately, after five years of the ICANN multistakeholder process that was designed to fix the Whois/GDPR problem there is no practical solution insight. That is why Congress and the Department of Commerce can no longer continue to put ICANN's multistakeholder process over the health, safety, and cyber security of the American people and must work to immediately enact legislation to fix the Whois/GDPR problem.

The Honorable Brett Guthrie (R-KY)

1. The United States has seen historic levels of opioid abuse leading to tragic deaths over the last several years. In my home state of Kentucky, drug overdoses have climbed year-over-year between 2020 and 2021. The opioid crisis has been exacerbated by deadly fentanyl being trafficked into our communities through our Southern Border and on social media platform millions of Americans are using. The Energy and Commerce Committee has passed several bills to address this epidemic. I am especially concerned that illegal drugs are still available online through illegal pharmacies and even social media platforms. This type of illegal activity online is troubling. I have draft legislation that is part of the Republican Big Tech platform that would help prevent this from happening on these sites by requiring internet platforms to implement and maintain reasonable content moderation policies and practices to address the illegal sale of drugs on their platforms. Additionally, the Federal Trade Commission and State Attorneys General would ensure enforcement of these policies.

    a. Mr. Lane, do you think legislation in this space is enough to adequately devote resources and appropriate information sharing between Big Tech and the law enforcement community to address this illegal and potentially deadly activity?

        Response: I strongly believe legislation is necessary to help curtail the opioid and fentanyl epidemic, as well as curtailing other illegal activities that are occurring on online platforms. In order to curtail these illegal activities, Congress should focus on three main issues: 1) reforming section 230; 2) creating more transparency in the way Internet platforms operate, while protecting Internet users' privacy; and 3) restoring access to WHOIS data.

    b. How can this committee strike a balance between the need to halt this illegal activity on these platforms and holding companies accountable while also promoting innovation as we consider possible solutions?

        Response: We must return the rule of law to the Internet. Until we hold online platforms (TikTok, Reddit, Facebook, Google, etc.) and other Internet intermediaries (Cloudflare, Verisign, GoDaddy, the Internet Society (ISOC), Namecheap, and even the Internet Corporation for Assigned Names and Numbers (ICANN), etc.) equally accountable as brick-and-mortar businesses, people will be less safe online. We need to restore to platforms the ordinary duty of care that would apply but for courts' current, overbroad application of section 230. Congress should amend section 230 to require that platforms and other Internet intermediaries take reasonable steps to curb illegal conduct online as a condition of receiving the section's protections. If platforms could be held both criminally and civilly liable for irresponsibly enabling such transactions, they'd be much more likely to pay attention and curb the activity. By making simple language changes to section 230 that restore the duty of reasonable care,

Congress could help combat not just Internet opioid and fentanyl sales but all current and future illegal activity online. And in a non-regulatory, pro-free market way that both conservatives and liberals should be able to support: creating meaningful incentives for platforms to find the most effective and efficient ways to prevent online harm.

Congress also needs to rectify the "Dark Whois" problem that was created by an overly broad interpretation of the European Unions General Data Protection Regulation (GDPR) by passing legislation requiring domain name providers like Verisign, Godaddy, NameCheap, to once again make accurate WHOIS information available for legitimate purposes. The lack of access to WHOIS data is hindering not only cyber security and anti-terrorism efforts, but investigations into illegal online drug sales. As the Federal Drug Administration (FDA) stated in a August 13, 2020 letter to Representative Latta,

> " Access to WHOIS information has been a critical aspect of FDA's mission to protect public health. Implementation of the E.U. General Data Protection Regulation (GDPR) has had a detrimental impact on FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients."
>
> "WHOIS data has also been widely used in FDA's criminal investigations to identify individuals and organizations selling online a variety of unapproved/uncleared/unauthorized products such as opioids, counterfeit or adulterated drugs as well as purported dietary supplements containing deleterious or undeclared ingredients. Most recently, lack of WHOIS transparency significantly hindered FDA's ability to identify sellers of fraudulent and unproven treatments for COVID-19 as well as illegitimate test kits and counterfeit or substandard personal protective equipment. These cases range from a simple website marketplace to sophisticated transnational cybercrime networks involving thousands of websites, hidden servers, dark web applications and virtually linked co-conspirators. Many of these criminal conspiracies were linked or identified via historical WHOIS analysis."

Unfortunately it is now going on five years of the ICANN multistakeholder process that was designed to fix the Whois/GDPR problem with no practical solution insight. Congress and the Department of Commerce can no longer continue to put ICANN's multistakeholder process over the health, safety, and cyber security of the American people and must work to immediately enact legislation to fix the Whois/GDPR problem.

Another step Congress could take is to enact transparency provisions that require each platform to: 1) publicly disclose its content moderation policies; 2) create a process by which users can file a complaint with the platform arguing it did not follow its own policies; 3) create a process by which users can appeal a platform's decision to take down or leave up specific content, or to terminate or not terminate service to a user; and 4) publicly disclose information about the decisions the platform has made to take down or leave up certain content, or to terminate or not terminate service to a user.

Platforms that violate these transparency requirements or policies contained in their terms of service would lose the section 230 shield and thus could be culpable for breach of contract or a deceptive trade practice. These transparency requirements would also better enable individuals and businesses to decide what platforms to use—potentially prompting new entrants and existing providers to compete based on content moderation practices, thereby promoting innovation. In addition, the public disclosure requirements would allow policymakers, law enforcement, and researchers to track problematic trends—either with users' online misbehavior or the platforms' moderation practices—and develop strategies to address them.

Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Holding Big Tech Accountable: Legislation to Build a Safer Internet."
December 9, 2021

Ms. Jessica Rich, Of Counsel, Kelley Drye & Warren LLP

The Honorable Michael C. Burgess (R-TX)

1. Ms. Jessica Rich, in your testimony you state that, currently, consumers need to read lengthy privacy and content moderation policies just to understand how companies use their data and police their user content. I have a discussion draft of a bill to require large Internet platform companies to biannually submit to the Federal Trade Commission their policies for users to appeal content moderation decisions by the platform. Do you think such a requirement to submit appeal information to the FTC would help improve transparency for users of Internet platforms?

   Response: Requiring submission of content moderation policies to the FTC, so that the FTC can in turn post them publicly, would increase public visibility into these policies. However, consumers already are overloaded with complex information, making it unlikely that they will review such policies and understand all of the details, nuances, and decisions reflected in them. For this reason, public posting would probably be more useful for researchers and policymakers than for consumers.

2. Ms. Rich, one concern with the use of social media is the way algorithms filter and recommend content to users. It is relatively easy to manipulate your own algorithm by consecutively clicking on similar content. Within minutes, your entire feed will be filled with like-kind content. This becomes a problem when an individual repeatedly accesses content that may be harmful. For example, users can quickly be recommended content regarding eating disorders, hate speech, or ways to buy illicit products, like drugs. Are the algorithms used on social media platforms too reactive to user interactions?

   Response: Certainly, the tendency for algorithms to magnify and duplicate harmful content is a serious concern. However, addressing the way algorithms respond to user interactions is beyond my technological expertise.

3. Ms. Rich, this Congress, I introduced the TROL Act (H.R. 192) to combat abusive patent demand letters from trial lawyers. We need to pass a comprehensive privacy bill that gives enforcement to the Federal Trade Commission and State Attorneys General to help prevent abusive trial lawyers who may work through private rights of

action. Can you address the consequences small businesses may face if any privacy law includes private rights of action?

Response: Whether to grant a privacy right of action ("PRA") has proved to be one of the most controversial issues in the debate about whether to pass a federal privacy law. PRA proponents cite the need to ensure recourse for injured consumers, given the limited reach and scope of federal and state enforcement actions. Opponents cite abuses by class action lawyers seeking big payouts – a concern that is especially concerning when small businesses are involved. One approach is to ensure that any federal legislation is sufficiently robust and well-funded, so that consumers are appropriately protected without a PRA. Another is to impose parameters around a PRA to prevent abuse – for example, limits on any payments to lawyers, standards of proof that must be met, and/or providing companies with the right to cure a violation before a PRA can proceed.