

HOLDING BIG TECH ACCOUNTABLE: LEGISLATION TO PROTECT ONLINE USERS

HYBRID HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

MARCH 1, 2022

Serial No. 117-70



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

U.S. GOVERNMENT PUBLISHING OFFICE

59-693 PDF

WASHINGTON : 2025

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

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

PROFESSIONAL STAFF

TIFFANY GUARASCIO, *Staff Director*
WAVERLY GORDON, *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 Mc NERNEY, California
YVETTE D. CLARKE, New York
TONY CARDENAS, California, *Vice Chair*
DEBBIE DINGELL, Michigan
ROBIN L. KELLY, Illinois
DARREN SOTO, Florida
KATHLEEN M. RICE, New York
ANGIE CRAIG, Minnesota
LIZZIE FLETCHER, Texas
FRANK PALLONE, Jr., New Jersey (*ex officio*)

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

C O N T E N T S

	Page
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement	2
Prepared statement	4
Hon. Gus Bilirakis, a Representative in Congress from the State of Florida, opening statement	6
Prepared statement	8
Hon. Frank Pallone, a Representative in Congress from the State of New Jersey, opening statement	11
Prepared statement	13
Hon. Cathy McMorris Rodgers, a Representative in Congress from the State of Washington, opening statement	15
Prepared statement	17

WITNESSES

Laurel Lehman, Policy Analyst, Consumer Reports	21
Prepared statement	23
Answers to submitted questions ³	
Katie McInnis, Senior Public Policy Manager U.S., Duckduckgo, Inc.	43
Prepared statement	45
Answers to submitted questions ³	
Mike Duffey, Special Agent Supervisor, Florida Department of Law Enforcement	50
Prepared statement	52
Answers to submitted questions	126
Mutale Nkonde, Chief Executive Officer, AI for the People U.S.	56
Prepared statement	58
Answers to submitted questions	145

SUBMITTED MATERIAL

H.R. 6416 the Banning Surveillance Advertising Act of 2022 ¹	
H.R. 6580 the Algorithmic Accountability Act of 2022 ¹	
H.R. 6755 the Cooperation Among Police, Tech, and Users to Resist Exploitation Act ¹	
H.R. 6786 the Increasing Consumers' Education on Law Enforcement Resources ¹	
H.R. 6796 the Digital Services Oversight and Safety Act of 2022 ¹	
Letter of February 14, 2022, from Christopher Oswald, Executive Vice President, Government Relations the Association of National Advertisers, Driving Growth, to Ms. Eshoo, et al., submitted by Mr. Latta	99
Letter of March 1, 2022, from Interactive Advertising Bureau, submitted by Ms. Lesko ²	

¹ Legislation has been retained in committee files and also is available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114439>.

² The information has been retained in committee files and also is available at <https://docs.house.gov/meetings/IF/IF17/20220301/114439/HHRG-117-IF17-20220301-SD004.pdf>.

³ Ms. Lehman and Ms. McInnis, did not answer submitted questions for the record by the time of publications.

VI

	Page
Report “Enhancing the FTC’s Consumer Protection Authority to Regulate Social Media Companies” by Paul M. Barrett and Lily Warnke, NYU/STERN, submitted by Ms. Trahan	102
Letter of February 28, 2022, from Paul Lekas, Senior Vice President, Global Public Policy, Software and Information Industry Association, to Ms. Schakowsky and Mr. Bilirakis, submitted by Ms. Schakowsky	115
Letter of February 28, 2022, from Ms. Rodgers, et al., to Ms. Khan, submitted by Mr. Bilirakis	121
Letter of March 1, 2022, Neil L. Bradley, Executive Vice President, Chief Policy Officer, Head of Strategic Advocacy, U.S. Chamber of Commerce, to Ms. Schakowsky and Mr. Bilirakis, submitted by Mr. Guthrie	124

HOLDING BIG TECH ACCOUNTABLE: LEGISLATION TO PROTECT ONLINE USERS

TUESDAY, MARCH 1, 2022

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

The subcommittee met, pursuant to notice, at 10:31 a.m., in the John D. Dingell Room 2123, Rayburn House Office Building, and remotely via Cisco Webex online video conferencing, Hon. Jan Schakowsky, (chair of the subcommittee) presiding.

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

Also present: Representatives Eshoo and Walberg.

Staff present: Katherine Durkin, Policy Coordinator; Waverly Gordon, Deputy Staff Director and General Counsel; Jessica Grandberry, Staff Assistant; Tiffany Guarascio, Staff Director; Perry Hamilton, Clerk; Ed Kaczmariski, Policy Analyst; Zach Kahan, Deputy Director Outreach and Member Service; Mackenzie Kuhl, Press Assistant; Jerry Leverich, Chief Counsel, Communications and Technology; David Miller, Counsel; Kaitlyn Peel, Digital Director; Caroline Rinker, Press Assistant; Chloe Rodriguez, Clerk; Andrew Souvall, Director of Communications, Outreach, and Member Services; Michele Viterise, Counsel; Caroline Wood, Staff Assistant; C.J. Young, Deputy Communications Director; Michael Cameron, Minority Policy Analyst, Consumer Protection and Commerce, Energy, Environment; Peter Kielty, Minority General Counsel; Emily King, Minority Member Services Director; Tim Kurth, Minority Chief Counsel, Consumer Protection and Commerce; Kate O'Connor, Minority Chief Counsel, Communication and Technology; 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 hold a legislative hearing entitled, "Holding Big Tech Accountable: Legislation to Protect Online Users."

Due to COVID-19, members can now participate in today's hearing, either in person, remotely, or remotely online via conference,

and in accord with the updated guidelines issued by the attending physician.

Members, staff, and members of the press can participate in the hearing room, and are not required to wear masks.

For members participating remotely, your microphones will be set on mute for the purpose of eliminating inadvertent background noise. Members participating remotely will need to unmute your microphones each time that you wish to speak.

Please note—please notice that, once you have unmuted your microphone and anything that is—but anything that is said will be—can be heard over the loudspeakers. And so you don’t want to do that.

Since members are participating from different locations at today’s hearing, all recognition of members shall—such as—such for—as such for questions will be in the order of subcommittee seniority.

Documents for the record can be sent to Ed Kaczmariski at the email address that was provided to staff, and all documents shall be entered into the record at the end of—the conclusion of the hearing.

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

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

So today we begin the third legislative hearing of the Energy and Commerce Committee to consider legislation to rein in Big Tech.

This subcommittee has worked long and hard to respond to the challenge, the challenges presented by Big Tech. But despite our scrutiny and repeated calls for change, the tech industry has not responded. Now is the time for change and for accountability.

We know social media platforms can be used for good, and we have seen in the last week the heroic stories of Ukrainian people, and the amazing fight-back that they have shown, and courage that they have shown. But misinformation and disinformation are seemingly still amplified, and that is having dramatic costs for people around the world.

For example, Russian state-owned media is targeting Spanish speakers around the globe with disinformation to—excuse me, when it comes to the—what is going on in the invasion of Ukraine. Previously, social media abetted a genocide in Myanmar and a deadly insurrection on January 6th.

We are done with apologies and denials from Big Tech companies. We are done turning a blind eye when billionaires build economic empires by feeding Americans an ever-increasing diet of disinformation. It is time to regulate. So we will be considering five bills today.

Ms. Eshoo’s bill, the Banning Surveillance—excuse me. What does that say?

VOICE. Advertising.

Ms. SCHAKOWSKY. What?

VOICE. Advertising.

Ms. SCHAKOWSKY. OK, the Banning Surveillance Advertising Act, which I am a proud cosponsor of, to ban targeting advertising that can track individual users across the internet.

Ms. Clarke's bill, the Algorithms Accountability Act, will require technology companies using the art of—using artificial intelligence to assess the impact of their algorithms on consumers—disinformation to—discrimination, rather, to—of protected classes no—has no place in our digital world.

Mrs. Trahan's bill, the Digital Service, Oversight, and Safety Act, improves transparency for consumers and ensures that research can be—can measure the impact of social media on our society.

Mr. Bilirakis's bill, the CAPTURE Act—that is the short title—studies whether law enforcement has the resources to keep us safe online.

Mr. Mullin's bill, the Increasing Consumer Education on Law Enforcement Act, empowers consumers to protect the—them—to protect themselves.

So as we refine these proposals, I have no doubt that can help create a fairer, safer internet, one that protects consumers, and who—and whose business model isn't rooted in disinformation.

So I look forward to the hearing, and welcome all the comments of my colleagues on both sides of the aisle, so that we can work together on this.

[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 Protect Online Users"

March 1, 2022

Today, we begin the third legislative hearing in the Energy and Commerce Committee to consider legislation to reign in Big Tech.

This subcommittee has worked long and hard to respond to the challenges presented by Big Tech.

But despite our scrutiny and repeated calls for change, the tech industry has not responded.

Now is the time for change and for accountability.

We know social media platforms can be used for good. We've seen that in the heroic stories of the Ukrainian people over the last week.

But misinformation and disinformation are seemingly still amplified, and that is having dramatic costs for people around the world.

For example, Russia's state-owned media is targeting Spanish speakers around the globe with disinformation to distort the narrative around their invasion of Ukraine.

Previously, social media abetted a genocide in Myanmar and a deadly insurrection on January 6th.

We are done with apologies and denials from tech companies.

We are done turning a blind eye while billionaires build economic empires by feeding Americans an ever-increasing diet of disinformation.

It is time to regulate.

We will consider five bills including Ms. Eshoo's bill, the "Banning Surveillance Advertising Act," which I am proud to co-lead, to ban targeted advertising that can track individual users across the internet.

Ms. Clarke's bill, the "Algorithmic Accountability Act," will require tech companies using artificial intelligence to assess the impact of their algorithms on consumers.

March 1, 2022

Page 2

Discrimination of protected classes has no place in our digital world.

Ms. Trahan's bill, the "Digital Services Oversight and Safety Act," improves transparency for consumers and ensures researchers can measure the impact of social media on our society.

Mr. Bilirakis's bill, the "CAPTURE Act," studies whether law enforcement has the resources to keep us safe online.

Mr. Mullin's bill, the "Increasing Consumers' Education on Law Enforcement Act," empowers consumers to protect themselves.

As we refine these proposals, I have no doubt they can help create a fairer, safer internet.

One that protects consumers. And whose business model isn't rooted in discrimination.

I look forward to hearing how we can improve these proposals to achieve that goal.

Thank you to the witnesses for joining us today.

I now recognize the Ranking Member, Mr. Bilirakis, for five minutes.

Ms. SCHAKOWSKY. And with that, I would like to welcome the ranking member, Mr. Bilirakis, for his 5 minutes.

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

Mr. BILIRAKIS. Thank you so very much, Madam Chair.

Good morning, and welcome to today's subcommittee legislative hearing, our witnesses.

Today's hearing is the third in a series of what the majority calls "Holding Big Tech Accountable." I am—I certainly hope the fourth will be on a national privacy and data security framework.

For the December hearing, Republicans invited TikTok to testify as our witness, since they are not at the center—they are at the center of many of our shared concerns. But TikTok declined.

For this hearing, I appreciate that the majority backed our efforts to invite the company, this particular company, TikTok, this time on a bipartisan basis. But sadly, TikTok declined yet again. I know this isn't what you want, Madam Chair. I certainly don't want it, either. So again, very disappointing, and we are not going to give up.

Madam Chair, if we put our heads together, I am sure we can figure out a way to get this company, this particular company, TikTok, before our subcommittee, like so many others who have appeared as part of our country's democratic process. How very arrogant of them. But again, we are not going to give up. We need to hear from TikTok.

The legislation today covers a broad range of issues, you know, not just hear from TikTok. We need to ask questions of TikTok.

While I share many of the same concerns as my colleagues regarding Big Tech's abuse of power, I worry about proposals that miss the target and hurt other parts of our economy. Without more careful vetting, these bills will lead to a worse consumer experience, adversely impact American innovators and small businesses, and increase market dominance for large companies, specifically Google in this case.

So far this Congress, this committee has heard from academics, industry experts, and consumer advocates, which is great. I am pleased that today we finally get to hear from law enforcement's perspective. They are on the front lines—and I know you agree, Madam Chair—for protecting our kids online, which is a primary focus in our fight against Big Tech. And thank you again for holding this hearing.

I am proud to welcome Mike Duffey, a law enforcement officer based in my home State of Florida, who has dedicated more than 20 years of his career to protecting our Floridians and our Nation's children from predators and other dangerous threats online.

Law enforcement's insights are critically important, as we consider multiple avenues to rein in the abuses perpetrated by Big Tech. I believe two bills under consideration today will help.

First we have got the H.R. 6786, the Increasing Consumers Education on Law Enforcement Resources Act, introduced by my good friend, Representative Mullin. It will require FTC and attorneys general to develop a public education program to inform our constituents about law enforcement resources regarding online safety.

The second is my bill—and thank you for mentioning it, Madam Chair, and agendaing the bill—H.R. 6755, the Cooperation Among Police, Tech, and Users to Resist Exploitation Act, or the CAPTURE Act, which will require the Government Accountability Office to research and provide recommendations on how to improve coordination and consultation between social media companies and law enforcement without creating constitutional issues.

Some here may recognize the single point of contact proposal, as it currently exists in the FirstNet framework. This is a model I am looking to apply to tech platforms so Federal, State, and local law enforcement have clarity on who is reached reaching out to these companies in order to tackle harms online.

Given the connection to today's Democratic bills have on privacy and data security, I know my friend, the Chair, will appreciate me once again emphasizing the importance of passing a national privacy and data security law. Even the House Administration Committee just held a hearing on a national privacy standard. We are all well overdue—we are overdue to hold a committee hearing because we have the jurisdiction in this committee, and I know the Chair has promised that we would.

Madam Chair, I know these issues are extremely important to you, and the best way to protect our constituents online is through a national privacy and data security framework. It is time our subcommittee moves beyond these one-off bills that beat around the bush of privacy and data security concerns. Leader Rodgers—and she will—I am sure she will confirm this—and I remain fully committed to working across the aisle with anyone to enact a truly comprehensive privacy and data security law, and I urge my colleagues to join me in these efforts.

Thank you again for allowing me to participate today, and I look forward to the discussion, especially how these proposals will help protect our kids online.

[The prepared statement of Mr. Bilirakis follows:]

PREPARED STATEMENT OF HON. GUS BILIRAKIS

Opening Statement for Republican Leader Bilirakis

Subcommittee on Consumer Protection and Commerce

Legislative hearing on “Holding Big Tech Accountable: Legislation to Protect Online Users”

March 1, 2022

As Prepared For Delivery

Good morning, and welcome to today’s subcommittee legislative hearing.

Today’s hearing is the third in a series of what the majority calls “Holding Big Tech Accountable.” I certainly hope the fourth will be on a national privacy and data security framework.

For the December hearing, Republicans invited TikTok to testify as our witness, since they are at the center of so many of our shared concerns, but TikTok declined.

For this hearing, I appreciate that the Majority backed our efforts to invite this company, this time on a bipartisan basis but sadly, TikTok declined yet again.

Madam Chair, if we put our heads together, I’m sure we can figure out a way to get this company before our subcommittee like so many others who have appeared as part of OUR country’s democratic process.

The legislation today covers a broad range of issues. While I share many of the same concerns as my colleagues regarding Big Tech’s abuse of power, I worry about proposals that miss the target and hurt other parts of our economy.

Without more careful vetting, these bills will lead to a worse consumer experience, adversely impact American innovators and small businesses, and increase market dominance for large companies... specifically Google.

So far this Congress, this committee has heard from academics, industry experts, and consumer advocates. I’m pleased that today we finally get to hear law enforcement’s perspective. They are at the front lines of protecting our kids online, which is a primary focus in our fight against Big Tech.

I'm proud to welcome Mike Duffey, a law enforcement officer based in my home state of Florida, who has dedicated more than 20 years of his career to protecting our Floridians and our nation's children from predators and other dangerous threats online.

Law enforcement's insights are critically important as we consider multiple avenues to rein in the abuses perpetrated by Big Tech. I believe two bills under consideration today will help.

First, H.R. 6786, the Increasing Consumer's Education on Law Enforcement Resources Act introduced by Rep. Mullin, will require FTC and Attorneys General to develop a public education programs to inform our constituents about law enforcement resources regarding online safety.

The second is my bill H.R. 6755, the Cooperation Among Police, Tech, and Users to Resist Exploitation Act or "the CAPTURE Act," which will require the Government Accountability Office to research and provide recommendations on how to improve coordination and consultation between social media companies and law enforcement, without creating constitutional issues.

Some here may recognize the "single point of contact" proposal, as it currently exists in the FirstNet framework. This is a model I'm looking to apply to tech platforms so Federal, State, and local law enforcement have clarity on who to reach out to at these companies in order to tackle harms online.

Given the connection today's Democratic bills have on privacy and data security, I know my friend, the Chair, will appreciate me once again emphasizing the importance of passing a national privacy and data security law. Even the House Administration Committee just held a hearing on a national privacy standard. We are well overdue to hold one in the Committee of jurisdiction.

Madam Chair, I know these issues are important to you, and the best way to protect our constituents online is through a national privacy and data security framework. It is time our subcommittee moves beyond these "one-off" bills that beat around the edges of privacy and data security concerns. Leader Rodgers and I remain fully committed to working across the aisle

with anyone to enact a comprehensive privacy and data security law, and I urge my colleagues to join me in these efforts.

Thank you to everyone participating today, and I look forward to the discussion, especially how these proposals will help protect our kids online.

I yield back.

Mr. BILIRAKIS. Thank you, and I yield back.

Ms. SCHAKOWSKY. Thank you, Mr. Bilirakis. And I do look forward to very soon dealing with a comprehensive privacy bill. I think we are on our way.

And let me now welcome the chair of the full committee, Mr. Pallone, for 5 minutes.

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

Mr. PALLONE. Thank you, Chair Schakowsky. Today's hearing is the third in a series of hearings this committee has held on legislative reforms to hold social media companies accountable. The two previous legislative hearings covered reforms to section 230 of the Communications Decency Act and consumer protection-focused legislation to help build a safer internet. Today we will examine legislation to enhance transparency and further promote safety online.

These hearings come after years of repeated bipartisan calls for social media companies to change their ways. Since 2018 the committee has held 8 hearings on the subject. We have examined these issues from all sides, and now it is time for us to come together and to act. We are committed to working with our Republican colleagues on legislation to increase transparency, limit online manipulation, and improve online safety.

And we all know how important social media is to our daily lives. It allows us to connect with family and friends to organize and to stay safe. And we are seeing that firsthand right now in Ukraine, as images posted on social media are exposing the world to just how depraved and misguided Vladimir Putin's actions are.

Ukrainians armed with their smartphones are documenting the bravery of their fellow citizens standing up to the Russian military and the brutality of war. Social media is allowing Ukrainians to spread the word without any filters of the true impacts of this war. The images they are capturing on their phones are being shown worldwide, showing the world the atrocities being inflicted on the Ukrainian people.

But at the very same time, we have seen weeks of Russian disinformation campaigns used to lay the groundwork for the invasion of Ukraine. These campaigns use propaganda to build support for the Kremlin and, unfortunately, they spread like wildfire online.

And there is no question that fast-moving current events can be difficult for social media companies to respond to quickly. But that is their responsibility, and they must be held accountable. We must ensure they are transparent, and their incentives align with the good social media can do for people, and not the bad.

Today we will discuss five 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 establishes an Office of Independent Research Facilitation at the FTC. This new office would help facilitate academic research on social media platforms to help us get the data we need on how these companies are targeting users.

Another bill requires companies that use automated decision-making to conduct impact assessments on their systems, and regularly report the results to the FTC. Now, these assessments will help ensure that machine learning is being employed in a fair and nondiscriminatory manner.

We will also consider a bill to ban the practice of targeted advertising, which includes a provision prohibiting advertisers from using information that identifies a consumer as a member of a protected class for advertising purposes.

And finally, we will consider bills that will help social media companies work better with Federal, State, and local law enforcement to protect users who feel their safety has been violated online.

Now, these proposals, along with the proposals we considered in the two previous legislative hearings, are collectively major steps in addressing the real harms caused by Big Tech.

Another part of tech accountability is protecting people's privacy. I know that both the ranking member of the subcommittee and the Chair mentioned this, and have been involved with this, and we are particularly concerned about our children's privacy, as more and more apps are used by and targeted to our kids.

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 draft. Our work on that legislation continues, and I hope the Republicans will work together with us on that, as well.

The bills before us today collectively address tech accountability. The time to act is now, and these bills can help us make the internet a safer place. And I look forward to our discussion today and, obviously, hearing from our excellent panel.

[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 Protect Online Users"

March 1, 2022

Today's hearing is the third in a series of hearings this Committee has held on legislative reforms to hold social media companies accountable. The two previous legislative hearings covered reforms to Section 230 of the Communications Decency Act and consumer protection-focused legislation to help build a safer internet. Today we will examine legislation to enhance transparency and further promote safety online.

These hearings come after years of repeated, bipartisan calls for social media companies to change their ways. Since 2018, the Committee has held eight hearings on this subject. We've examined these issues from all sides and now it's time for us to come together and to act. We're committed to working with our Republican colleagues on legislation to increase transparency, limit online manipulation, and improve online safety.

We all know how important social media is to our daily lives. It allows us to connect with family and friends, to organize, and stay safe.

We're seeing that firsthand right now in Ukraine as images posted on social media are exposing the world to just how depraved and misguided Vladimir Putin's actions are. Ukrainians armed with their smartphones are documenting the bravery of their fellow citizens standing up to the Russian military, and the brutality of war. Social media is allowing Ukrainians to spread the word, without any filters, of the true impacts of this war. The images they are capturing on their phones are being shown worldwide – showing the world the atrocities being inflicted on the Ukrainian people.

But at the very same time, we have seen weeks of Russian disinformation campaigns used to lay the groundwork for the invasion of Ukraine. These campaigns use propaganda to build support for the Kremlin and, unfortunately, they spread like wildfire online.

There's no question that fast moving current events can be difficult for social media companies to respond to quickly, but that is their responsibility and they must be held accountable. We must ensure they are transparent, and their incentives align with the good social media can do for people, not the bad.

Today, we will discuss five bills that target different parts of the social media ecosystem to make platforms safer for users.

March 1, 2022
Page 2

One of the best ways to make these companies more accountable is to make them more transparent. We will discuss legislation that establishes an “Office of Independent Research Facilitation” at the Federal Trade Commission (FTC). This new office would help facilitate academic research on social media platforms, to help us get the data we need on how these companies are targeting users.

Another bill requires companies that use automated decision making to conduct impact assessments on their systems and regularly report the results to the FTC. These assessments will help us ensure that machine learning is being employed in a fair and non-discriminatory matter.

We’ll consider a bill to ban the practice of targeted advertising, which includes a provision prohibiting advertisers from using information that identifies a consumer as a member of a protected class for advertising purposes.

Finally, we’ll consider bills that will help social media companies work better with federal, state, and local law enforcement to protect users who feel their safety has been violated online.

These proposals, along with the proposals we considered in the two previous legislative hearings, are collectively major steps in addressing the real harms caused by Big Tech.

Another part of tech accountability is protecting people’s privacy, especially our children’s privacy, as more and more apps are used by and targeted to our kids. 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 draft. Our work on that legislation continues and I hope that the Republicans will work together with us on that as well.

The bills before us today are important bills to address tech accountability. The time to act is now and these bills can help us make the internet a safer place. I look forward to our discussion today.

Mr. PALLONE. I yield back, Madam Chair, and thank you for all that you have done on these issues. You are—you really have been working on them for a long time, and it is—it has made a difference in terms of where we are today. Thank you.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. And now, wearing her Ukrainian yellow——

Mrs. RODGERS. That is right.

Ms. SCHAKOWSKY. I want to recognize Mrs. Rodgers, our ranking member, 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.

First I want to say, “Glory to Ukraine.” Several of us on this committee had the opportunity to travel to Ukraine, and were inspired at the time with their fight for self-determination and independence. And today I continue to support their fight for freedom, and I pray for their strength and security, and their freedom to prevail.

While some tech companies have taken steps to prevent the proliferation of Russian state-sponsored propaganda, I hope that we too on the subcommittee will be vigilant in addressing how others, like Twitter, maintaining an account for the Kremlin; or TikTok, reinstating Russian, state-owned media, are complicit in spreading it, as well as other disinformation campaigns from Putin. This has real-world consequences for the Ukrainians and our other European allies.

We all share the goal of holding Big Tech accountable, especially for our children. Big Tech platforms are my biggest fear as a parent. Nearly every conversation I have with parents in schools these days comes back to the concerns about Big Tech and our kids. It is echoed by pediatricians, school administrators, and teachers. Big Tech are not advocates for children. Our kids, the users, are their product, and they are being manipulated and exploited for profit. They are being exposed to cruelty, bullying, and induced to self-harm. These harms have been worsened by the move to virtual life because of government-imposed school closures and lockdowns.

We must—this committee can and must—do more to address this crisis. If we are going to address issues with Big Tech and the advertising industry, that discussion includes improving transparency and accountability for how these businesses are collecting personal information, especially from our children. My Republican colleagues and I unveiled a privacy and data security framework last year. Addressing these issues in a hearing would help us make progress.

One bipartisan bill we asked to be considered is the Walberg-Rush Child Online Privacy Protection Act update. Despite many changes being considered on the collection and use of data today, unfortunately, this one is still missing on the schedule.

Also, if we are discussing emerging technologies like artificial intelligence, we should be addressing how AI can strengthen American leadership and reflect our values of freedom, human rights,

and human dignity. These are issues that require time, education, and hearings to debate and identify common ground.

A key component for many of these issues is the authority Congress grants to the Federal Trade Commission. The bills today proposed by the Democrats enact sweeping changes for the FTC. I appreciate that the Commission wants to be more involved in improving data security. We have been clear that we are willing to negotiate on additional authority, but changes like this must be given the appropriate time for discussion and vetting.

We need to start by ensuring accountability and transparency from the FTC on its current authorities before we give them more power. The FTC should come before this committee to help us better understand how they would use additional authority, as well as provide us assurances it has its own house in order.

For this reason I sent a letter to Chair Khan yesterday on the FTC's recent enforcement announcements for the security vulnerabilities found in the open source software—specifically, Log4J. Recent testimony in the Senate suggests government systems may have used Log4J, so we must learn whether agencies under our jurisdiction have system vulnerabilities that could be exploited specifically by foreign actors like Russia or China.

Missing from today's witness panel is TikTok, who declined an invitation to testify. And it is not the first time. TikTok threatens the safety, mental health, and well-being of our kids. A recent Wall Street Journal investigation found teen girls are developing tics from content they watch on TikTok. This is alarming, and their complete carelessness with people's personal information is even more concerning.

TikTok's ties to China raise significant concerns regarding the amount of access the CCP has to information of Americans. We know TikTok's parent company, ByteDance, is an extension of this authoritarian regime, and now we see reports that TikTok is allowing Russian Government propaganda to proliferate. TikTok operates with disregard for U.S. national security concerns. Our witness today, Officer Duffey, can share more on how they challenge the reach of local law enforcement, as well.

These concerns about privacy and Big Tech are issues we have been leading on, and we look forward to working together to address.

[The prepared statement of Mrs. Rodgers follows:]

PREPARED STATEMENT OF HON. CATHY McMORRIS RODGERS

**Opening Statement for Republican Leader Cathy McMorris Rodgers
Subcommittee on Consumer Protection and Commerce
Legislative Hearing on “Holding Big Tech Accountable: Legislation to
Protect Online Users”
March 1, 2022**

As Prepared for Delivery

Thank you. I want to first say, Glory to Ukraine. I support their fight for freedom and continue to pray for their safety, security, and for freedom to prevail.

While some tech companies have taken steps to prevent the proliferation of Russian state sponsored propaganda, I hope this Subcommittee will be vigilant in addressing how others like Twitter maintaining an account for the Kremlin or TikTok reinstating Russian state-owned media are complicit in spreading it, as well as other disinformation campaigns from Putin.

This has real world consequences for Ukrainians and our other European allies. We all share the goal to hold Big Tech accountable especially for our children. Big Tech platforms are my biggest fear as a parent.

Nearly every conversation I have with parents and schools these days comes back to their concerns about Big Tech and our kids. This is echoed by pediatricians, school administrators, and teachers. [Big Tech are not advocates for children](#). Our kids — the users — are the product and they're being manipulated and exploited for profit.

They are exposed to cruelty, bullying, and induced to self-harm. These harms have been worsened by the move to a virtual life because of government imposed school closures and lockdowns. This committee can and must do more to address this crisis. If we are going to address issues with Big Tech and the advertising industry, that discussion should include improving transparency and accountability for how these businesses are collecting personal information especially from our children.

My Republican colleagues and I unveiled a privacy and data security framework last year. Addressing these issues in a hearing would help us

make progress. One bipartisan bill we asked to be considered is the [Walberg-Rush Child Online Privacy Protection Act update](#).

Despite the many changes being considered on the collection and use of data today, this is still missing from our hearings. Also, if we are discussing emerging technologies like artificial intelligence we should be addressing how AI can strengthen American leadership and reflect our values of freedom, human rights, and human dignity. These are issues that require time, education, and hearings to debate and identifying common ground.

A key component for many of these issues is the authority Congress grants to the Federal Trade Commission. The Democratic bills today would enact sweeping changes for the FTC. I appreciate the commission wants to be more involved in improving data security.

We have been clear that we are willing to negotiate on additional authority but changes like these should be given the appropriate time for discussion and vetting. We need to ensure accountability and transparency from the FTC on its current authorities before we give them more power. The FTC should come before this committee to help us better understand how they would use any additional authority as well as provide us assurances it has its own house in order.

For this reason, I sent a letter to Chair Khan yesterday on the FTC's recent enforcement announcements for the security vulnerabilities found in open-source software, specifically, Log4j. Recent testimony in the Senate suggests government systems may have used Log4j. So, we must learn whether agencies under our jurisdiction have system vulnerabilities that could be exploited, specifically, by foreign actors like Russia or China.

Notably missing from the witness panel today is TikTok, who declined our invitation to testify. This wasn't the first time. TikTok threatens the safety, mental health, and well-being of our kids. A recent Wall Street Journal investigation found teen girls are developing tics from content they watch on TikTok.

This is alarming, and their complete carelessness with people's personal information is even more concerning. TikTok's ties to China raise significant concerns regarding the amount of access the CCP has to the information of Americans. We know TikTok's parent company, ByteDance, is an

extension of this authoritarian regime, and now we see reports that TikTok is allowing Russian government propaganda to proliferate.

TikTok operates with disregard for U.S. national security concerns. Our witness today, Officer Duffey, can share more on how they challenge the reach of the local law enforcement as well. These concerns about privacy and Big Tech are issues E&C Republicans have been leading on since day one. I yield back.

Mrs. RODGERS. I yield back.

Ms. SCHAKOWSKY. The gentlelady yields back, and the Chair would like to remind members that, pursuant to committee rules, that all Members' written opening statements shall be included in the record.

And now I would like to introduce our witnesses for today's hearing. As you can see, two are here. Is that three in person?

VOICE. Yes, just—

Ms. SCHAKOWSKY. Oh, three in person and one remotely. And I want to welcome Laurel Lehman, who is Policy Analyst at Consumer Reports; Katie McInnis, who is Senior Policy—Public Policy Manager at Duck Duck Goose.

VOICE. DuckDuckGo.

[Laughter.]

Ms. SCHAKOWSKY. I am sorry. Duck, Duck Goose, that is a game. Duck Duck Go. OK, sorry about that.

OK, I want to also welcome Mike Duffey, who is Special Agent Supervisor in charge at the Florida Department of Law Enforcement.

And Mutale Nkonde, who is the Founder and Chief Executive Officer at AI—excuse me, of AI at the—what is this, public?

VOICE. AI for the People.

Ms. SCHAKOWSKY. Oh, AI for the People U.S. There we go.

So at this time the Chair will recognize each witness for 5 minutes to provide their opening statements.

But before we begin, I want to make sure that I call attention to the witnesses that are testifying in person. In front of you, you—some of you have testified before, but if not, you will notice that there are lights in front of you, and the light will initially be green. The green will turn yellow when you have 1-minute remaining. And please begin to wrap up your testimony at that point. The light will turn red when your time has expired.

For the witness who is testifying remotely, there is a timer on your screen that will count down your remaining time.

And with that, let me ask Ms. Lehman.

You are recognized now for your 5 minutes.

Ms. LEHMAN. Thank you, Chair Schakowsky.

Ms. SCHAKOWSKY. Microphone.

VOICE. We can't hear you. Is it on?

VOICE. Maybe closer—

VOICE. Pull it closer.

Ms. LEHMAN. All right. There we go?

VOICE. There we—

Ms. SCHAKOWSKY. There we go.

Ms. LEHMAN. All right.

VOICE. Fine.

Ms. LEHMAN. All right. Thank you, Chair Schakowsky.

STATEMENT OF LAUREL LEHMAN, POLICY ANALYST, CONSUMER REPORTS; KATIE MCINNIS, SENIOR PUBLIC POLICY MANAGER U.S., DUCKDUCKGO, INC.; MIKE DUFFEY, SPECIAL AGENT SUPERVISOR, FLORIDA DEPARTMENT OF LAW ENFORCEMENT; AND MUTALE NKONDE, CHIEF EXECUTIVE OFFICER, AI FOR THE PEOPLE U.S.

STATEMENT OF LAUREL LEHMAN

Ms. LEHMAN. Chairman Pallone, Ranking Member Rodgers, Chair Schakowsky, Ranking Member Bilirakis, and members of the subcommittee, thank you for inviting Consumer Reports to testify today on the crucial matter of protecting consumers online.

My name is Laurel Lehman, and my work at CR focuses specifically on platform accountability, so that is where I will spend most of my time today.

For 86 years, consumers have turned to CR for answers to questions like, “Is this product safe? Is it worth my time or money? What risks might it pose to my family?” Consumers today grapple with the same questions, but about their online experiences. It is this platform safe? Is it worth my time? Are the goods I am buying from this ad authentic? Why am I seeing this ad again?

Today’s hearing grapples with this century’s version of confronting the very same challenges that have driven CR’s fight for a fair, just, and transparent marketplace all along. The bills before the subcommittee today seek these same aims, and we are excited to work with you to refine, craft, and pass legislation that can help us usher in the online ecosystem that consumers deserve.

Consumers face a range of issues in the digital marketplace. In a nationally representative survey, CR found that, of the 94 percent of Americans who said they had ever had at least 1 social media account, 84 percent had adjusted their social media settings at some point to limit or filter content in some way; 39 percent had elected to turn off targeted ads; 59 percent said that they had read news on a social media site they initially believed to be true, but later learned was made up; and 37 percent told us that they had, at some point, wanted to change their privacy settings on a social media platform, but didn’t know how.

And their concerns are limited to social media. They expand to e-commerce and the way that AI impacts their lives, as I elaborate on in my written testimony.

Yet the digital marketplace is as varied in potential solutions as it is in its problems. Just as one no recall safety standard or warning label can unilaterally keep consumers safe offline, the variety of challenges consumers face online requires a range of evidence-based policy solutions, from comprehensive transparency to expanded use of section 5 authorities to approaches of consumer protection law to cautious, narrow changes to section 230, and certainly include a stronger, better-funded FTC.

Auto and product manufacturers are expected to conduct safety testing, and CR can test cars and appliances for performance under stress to see how manufacturer claims line up with their advertising. Digital product manufacturers, however, have no such obli-

gations to research, mitigate, or disclose risks or dangers in the ways their systems work. They are not required to publish clear community guidelines or terms of service, or report on how effective their enforcement of such guidelines may be. And they make no guarantees they are appropriately staffing and equipping the teams that—dedicated to keeping consumers safe from harassment, spam, counterfeit products, hate speech, and misinformation.

Transparency will be fundamental to all such evidence-based policy. In particular, three different kinds. I talk about pipelines, processes, and personnel.

When I talk about pipeline transparency, we are talking about what factors influence what a consumer sees online. Whether that is an algorithm, or whether that is an ad, what components go into that?

When we talk about process transparency, consumers deserve to know the rules of the road. What can they expect from their online communities, and how can they expect those rules to be enforced?

When we talk about personnel, we are talking about, when platform fail consumers, how can we make sure that platform whistleblowers are empowered to make sure the public knows? And also, how we are making sure that platforms are appropriately staffed to enforce their terms of service everywhere they operate?

CR's test track can figure out how cars handle stress because we have speedometers. Right now no one can crash test ads and algorithmic recommendations, except the platforms that profit from them.

But transparency is the floor, not the ceiling, when it comes to building a more responsible online information ecosystem. Platforms clearly require stronger incentives to take responsibility for the harms they compound and accelerate.

Across consumer products, it is well understood that companies should bear responsibility for design and process choices related to foreseeable preventable harms. Meanwhile, YouTube failed to ban vaccine misinformation until September 2021, when platforms like Pinterest had started as early as February 2019. CR investigations in 2020 show that Facebook failed—that Facebook had approved ads with COVID-19 misinformation.

Online platforms fail to take reasonable baseline steps to ensure their products are designed and managed responsibly. Consumers should be able to expect an online system where we can trust that platforms have values past those which they return to their shareholders.

At the end of the day, consumers deserve a safe, just, and transparent digital marketplace that they can trust. Congress can and must work to pass legislation that makes it possible, and CR looks forward to working with you in pursuit of that aim.

Thank you again for inviting us here today. I look forward to your questions, and to today's discussion.

[The prepared statement of Ms. Lehman follows:]



**Testimony of Laurel Lehman
Policy Analyst, Advocacy
Consumer Reports**

**Before the
United States House of Representatives Committee on Energy & Commerce
Subcommittee on Consumer Protection and Commerce**

**Hearing on
“Holding Big Tech Accountable: Legislation To Protect Online Users”**

March 1, 2022

Thank you Chair Schakowsky, Ranking Member Bilirakis, and Members of the Subcommittee, for inviting Consumer Reports (CR) to testify on the crucial matter of tech accountability and protecting consumers online. CR was founded in 1936 and at a time of rapidly proliferating new technologies. A new media landscape was riddled with unfettered advertising claims that paltry patchwork regulation did little to address. As a result, consumers were left with precious few ways to gauge the value, quality, or authenticity of goods and services.

For 86 years, consumers have turned to CR for answers to questions such as, “Is this product safe? Is it worth my time or money? What risks might it pose to me or my family? How does it perform day-by-day? How does that change over time? How will it hold up under stress?”

Consumers today grapple with the same questions, but about their online experiences. Today’s hearing, focused on ways to protect consumers online, is the digital version of the very same challenges that have driven CR’s mission all along.

CR has surveyed consumers extensively on these topics in the last year, to better understand their concerns as we work towards workable solutions. Consumers face a range of issues online: in an August 2021 nationally-representative Consumer Reports survey, 94% of Americans said they had ever had at least one social media account. Among those, 84% had ever adjusted their social media settings to limit or filter content in some way (with 39% electing to turn off targeted ads); 59% said that they had read news on social media that they initially believed to be true but later learned was made up; and 37% percent had, at some point, wanted to change their privacy settings on a social media platform but didn’t know how.¹

Consumer concerns in the digital marketplace are not limited to social media, and expand to e-commerce. While nearly two-thirds of Americans told us in CR’s November 2021 nationally-representative survey that they often or always read online reviews to help them decide what to buy, nearly eight out of ten (79%) of people who read online reviews before deciding what to buy say they have ever read a review that they thought was fake.² And, in CR’s September 2021 nationally-representative survey, consumers were overwhelmingly opposed to online retailers using personalized pricing: seven in ten Americans oppose this practice, with 49% of Americans saying they “strongly oppose it.”³

Finally, even as artificial intelligence (AI) proliferates rapidly across consumer sectors, more than three-quarters (76%) say they would be uncomfortable (very uncomfortable; 46%,

¹ August 2021 Consumer Reports nationally representative Social Media Survey of 2,263 US adults.

² November 2021 Consumer Reports nationally representative American Experiences Survey of 2,057 US adults.

³ September 2021 Consumer Reports nationally representative American Experiences Survey of 2,341 US adults. Personalized pricing was described in this way: “Online retailers are in the practice of selling the same goods and services at different prices, depending on things like your income, home address, age, credit rating, browsing history and other personal information. This can result in someone being charged more or less than the standard retail price, depending on the algorithm used.”

somewhat uncomfortable; 30%) allowing AI to screen a video by grading responses and facial movements of them answering preselected questions during the job interview process. Furthermore, 62% say they would be uncomfortable allowing banks to use AI to make credit decisions to determine if they would qualify for a personal loan, and 52% would be uncomfortable using AI in hospital systems to help make diagnoses and a treatment plan.⁴

The digital marketplace is as varied in potential solutions as it is in its issues. Just as no singular recall, regulation, safety standard, or warning label can unilaterally keep consumers safe offline, the variety of challenges consumers face online also require comprehensive engagement with a full toolbox of evidence-based legislative, regulatory, and standards-driven solutions. Current law governing the online information ecosystem both fails to provide sufficient incentive for tech platforms to take responsibility for the harms that their systems compound and accelerate, and fails in parallel to equip regulators, researchers, and the public with the tools and context necessary to understand and help mitigate these harms.

In short, consumers deserve a safe, just, transparent information and e-commerce ecosystem that they can trust. Congress can—and must—work to pass legislation that makes it possible.

I. Transparency: Baseline Initiatives

CR has long advocated for transparency across the board for consumers, and the digital marketplace is no exception. When consumers are buying cars, appliances, or new electronics they ask, “What kind of performance can I expect? How does it perform over time and under stress? What safety standards does the manufacturer adhere to?” And consumers can get some answers from mandated testing, safety ratings and standards, and disclosures—like window stickers detailing a car’s mileage—and still other answers come from research and testing by independent parties like CR. Yet despite more and more critical components of our lives taking place online—particularly in the wake of COVID-19—consumers online have nowhere near such insight for digital products behind ever-growing screen-time: the internet has no crash-test disclosures.

That is why CR was proud to support the requirement that internet service providers (ISPs) display a “consumer broadband label” (or broadband nutrition label) detailing the price,

⁴ September 2021 Consumer Reports nationally representative American Experiences Survey of 2,341 US adults. AI was described in this way: “Artificial intelligence (AI) is a branch of computer science concerned with building smart machines capable of performing tasks such as problem-solving and decision making that would otherwise require human intelligence. Artificial intelligence is all around us and playing an active role in our daily lives. Every time we open our Facebook newsfeed, do a Google search, get a product recommendation from Amazon or book a trip online from Travelocity, AI is working in the background to learn from and adapt to data input in real time, and refine the content that is delivered.” For each of these situations, 7-8% of respondents said they were “unsure” how they would view it.

performance, and speed of internet access for consumers to help them make better decisions about broadband service. It represents a step in the right direction, but much more needs to be done in the online space.

Auto and product manufacturers are expected to conduct safety testing, and CR can test cars and appliances for performance under stress to see how manufacturer claims line up with their advertising. Digital product manufacturers, however, have no such obligations to research, mitigate, or disclose risks or dangers in the manufacturing of their information display and content moderation pipelines. They need not publish clear community guidelines or terms of service, or report on how effective their enforcement of such guidelines may be (indeed—CR published a guide on various’ platforms misinformation policies early in the COVID-19 pandemic because so much consumer confusion persisted⁵) and they make no guarantees that they are appropriately staffing and equipping the teams dedicated to keeping consumers safe from harassment, spam, hate speech, and misinformation.

In August 2021, the lead researcher for NYU Cybersecurity for Democracy, Laura Edelson, was running the program’s Ad Observatory—a crowdsourced effort where consumers shared political ads they had been shown, in an effort to understand how political ads were targeted. Only hours after informing Facebook that she and her team were studying how disinformation about the Jan. 6 attack on the U.S. Capitol had proliferated on the platform, Facebook disabled their accounts.⁶ And last summer reporting on Facebook’s internal chafing at the narratives that CrowdTangle—the data analytics tool they had acquired that offered some insight into news and misinformation spread across their platforms—had made possible before Meta disbanded the team running the tool.⁷ Google notoriously fired AI ethicist Timnit Gebru—and shortly after, her AI ethics colleague Margaret Mitchell as well—after their team sought to publish on the risks of AI systems Google was developing.⁸ Time and time again, platforms have shown that when researchers attempt to set-up test tracks to better understand the algorithmic systems driving the public’s online information ecosystem—tech giants will move to shut them down.

⁵ CR, “On Social Media, Only Some Lies Are Against the Rules” (Aug. 13, 2020) (online at: <https://www.consumerreports.org/social-media/social-media-misinformation-policies/>)

⁶ AP, “Facebook shuts out NYU academics’ research on political ads” (Aug. 4, 2021) (online at: <https://apnews.com/article/technology-business-5d3021ed9f193bf249c3af158b128d18>)

⁷ New York Times, “Inside Facebook’s Data Wars” (Jul. 14, 2021) (online at: <https://www.nytimes.com/2021/07/14/technology/facebook-data.html>)

⁸ Washington Post, “Google hired Timnit Gebru to be an outspoken critic of unethical AI. Then she was fired for it.” (Dec. 23, 2020) (online at: <https://www.washingtonpost.com/technology/2020/12/23/google-timnit-gebru-ai-ethics/>); see also: BBC, “Margaret Mitchell: Google fires AI ethics founder” (Feb. 20, 2021) (online at: <https://www.bbc.com/news/technology-56135817>)

Requests for transparency along these lines are not new,⁹ and—Meta’s recent market cap drop notwithstanding—the largest platforms do not lack the resources to make such transparency possible. Yet consumers—and those who would seek to protect them—remain left operating in the dark. These companies claim to be proud of how effectively they protect consumers, releasing reports packed with statistics that sound great on paper—yet fail to convey the whole picture.¹⁰ At the end of the day, if these companies were truly proud of how effectively they protect consumers in their product design and moderation practices—we would expect them to welcome independent researchers verifying their claims, not shut down the test track.

What’s more, transparency propositions are thoroughly bipartisan. The reintroduced bipartisan Platform Accountability and Consumer Transparency (PACT) Act, which would modify Section 230, details an incredible amount of content moderation process transparency, and the bipartisan Platform Accountability and Transparency Act (PATA) is designed to offer researchers and the public access to platform data.¹¹ House Energy and Commerce Ranking Member McMorris Rodgers’ Big Tech Accountability Platform Memo last year sought to, “Require disclosures regarding how Big Tech develops its content policies and require regular disclosures about content policy enforcement, including the types of content taken down and why, and clearly understood appeals processes,” and Democratic proposals have ranged from those before the Subcommittee today, to last year’s Algorithmic Justice and Online Platform Transparency Act.¹²

Furthermore, different stakeholders in the online information ecosystem are best served by different kinds of transparency. While troves of granular details can overwhelm everyday consumers — and can sometimes place the onus for a platform’s responsibility on consumers unlikely to make use of such knowledge—at scale, granular data can help researchers and agencies with vested public consumer interests understand the extent of broader societal consequences of shifts in online platform information ecosystems. For ordinary users, access to ad libraries may prove useful references to better understand trends in the brands they buy from.

However, across urgently needed increased dimensions of transparency—though most especially when it comes to independent researcher access to platform data—balancing the public interest with legitimate consumer privacy concerns must be paramount. In this vein, CR urges researcher access provisions that start with a baseline standard for de-identification—at

⁹ The Atlantic, “Rage Against the Algorithms” (Oct. 3, 2013) (online at: <https://www.theatlantic.com/technology/archive/2013/10/rage-against-the-algorithms/280255/>)

¹⁰ Wired, “Facebook Uses Deceptive Math to Hide Its Hate Speech Problem” (Oct. 15, 2021) (online at: <https://www.wired.com/story/facebook-deceptive-math-when-it-comes-to-hate-speech/>)

¹¹ The Platform Accountability and Consumer Transparency (PACT) Act, S. 797, 117th Cong., (2021); The Platform Accountability and Transparency Act (PATA), S. XX, 117th Cong., (2021)

¹² Republican Leader McMorris Rodgers to Energy and Commerce Committee Republican Members, “Memo Re: Big Tech Accountability Platform” (Jan. 26, 2021) (online at: <https://repUBLICANS-energycommerce.house.gov/wp-content/uploads/2021/01/Big-Tech-Accountability-Platform-Memo.pdf>); Algorithmic Justice and Online Platform Transparency Act, H.R. 3611, 117th Cong., (2021)

least for all private content, and likely too for some public content—as defined by three prongs in the FTC’s 2012 Privacy report: achieving a reasonable level of justified confidence that the data cannot reasonably be used to infer information about a particular consumer or device; a commitment not to attempt to re-identify, and contractual obligations preventing any shared entities (if any) from attempting to reidentify.¹³

Finally, in order to future-proof transparency mechanisms in the digital ecosystem, legislation driving these efforts must build in the level of flexibility and nuance required to encompass the most relevant expectations across a variety of platform purposes, sizes, and structures, and be adaptable to changing technologies. Regulators should be explicitly given rulemaking authority, which would offer more nimble, adaptable, and industry-specific rules going forward in perpetuity than would fixed statutory requirements alone.

Keeping such distinctions in mind, we urge Congress to consider a variety of initiatives that might improve platform transparency, and offer three pillars to consider in doing so: pipelines, processes, and personnel.

Pipelines

Online platforms are made up of information pipelines: the pieces of virtual infrastructure that direct both how content is ultimately delivered to users (e.g. ads and algorithmic recommendations) and how content is siphoned out of the ecosystem (e.g. automated removal or downranking of content with particular qualities). Pipeline transparency should offer context around factors affecting the inputs entering the information ecosystem (display pipelines) and factors affecting what is taken out of the information ecosystem (moderation pipelines).

Display Pipelines

Transparency into display pipelines should uncover what kinds of factors affect and influence what users see — both ads and algorithmically sorted and recommended content. Display pipeline transparency should provide insight into how dollars, engagement, targeting, and display rankings affect and influence what consumers see, and affect various groups of consumers—especially minors, vulnerable populations, or marginalized communities—differently. The NYU Ad Observatory, which used to, “identify trends in how ads are targeted to specific audiences and what messages are being used, who is funding each ad and how much they are spending to disseminate them” before Meta cut them off, is an excellent example of an

¹³ FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012) (online at: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-cra-rapid-change-recommendations/120326privacyreport.pdf>, pg. 21)

independent attempt at display pipeline transparency.¹⁴ The information gathered helped inform consumers, advertisers, and policymakers — which, contrary to Meta’s privacy claims, was likely a portion of why they were shut down.

Components of comprehensive display pipeline transparency might include publicly accessible ad libraries alongside reach and engagement numbers, datasheets for data sets¹⁵, risk and impact assessments for display algorithms, transparency reporting with commonly defined metrics, and—in line with deidentification baselines laid out above, alongside other aggregation—substantial access to datasets for both independent researchers and for the FTC.

Moderation pipelines

Transparency for moderation pipelines should offer insight into how content is flagged for moderation in the first place— whether by reports from users or other entities, or by machine-learning driven automation. Such transparency should aim to answer questions such as: What datasets are those machine learning models built upon? Are they representative? Are they accurate? How often are they updated? Which content is flagged, how is it reviewed, and how is content prioritized for review? Does such review disproportionately affect different groups of consumers, or different types of content?

Potential mechanisms of transparency for moderation pipelines include risk assessments and datasheets for the algorithms used to proactively flag content for removal, transparency reporting with commonly defined metrics, and—in line with deidentification baselines laid out above, alongside other aggregation—substantial access to datasets for both independent researchers and for the FTC.

Processes

Process transparency should encompass transparency across a platform’s policies and the realities of how those policies are enforced. Consumers use online platforms more than ever before for education, commerce, work, social connection, and deserve to have the specific rules of the road plainly stated and consistently enforced. They should also have a clear understanding of what to expect throughout the policy enforcement process, and where to turn for review if they believe the platforms have erred in their enforcement. Consumers also deserve clear specificity from these policies in order to understand what values they can expect the platforms they use to uphold, as overly vague platform policies lend themselves to inconsistent and unpredictable enforcement.

¹⁴ The George Washington University’s Institute for Data, Democracy & Politics, “Update: NYU Ad Observatory” (Aug. 11, 2021) (online at: <https://iddp.gwu.edu/nyu-ad-observatory>)

¹⁵ CACM, Gebru et. al, “Datasheets for Datasets” (Dec. 2021) (arXiv:1803.09010) (online at: <https://arxiv.org/abs/1803.09010>)

Such clarity could be a key step forward in improving consumer experiences—and holding platforms more publicly accountable for their enforcement—as the largest platforms have repeatedly shown failures both to enforce their guidelines against the powerful—politicians, influencers, and advertisers—and to over-enforce them against marginalized communities. In many cases the largest platforms have over-moderated or removed content where activists talk *about* the hate and harassment they receive, or that use dialects and vernacular of marginalized communities, even as those same platforms dither and delay enforcing platform policies when the uploading users are advertisers, influencers, politicians, or otherwise already in positions of power.¹⁶ Meanwhile, researchers and regulators need more to understand the far-reaching effects that such enforcement—and failures thereof or inconsistencies therein—can have on the online information and e-commerce ecosystem.

Publishing acceptable terms of use, community guideline, and enforcement policies; informing consumers of content removals and successful appeals, and regular, thorough transparency reports encompassing content moderation practices and metrics, granting researcher access to evaluate platform processes, and perhaps exploring timeliness requirements, with respect to reported content—might all prove steps toward a fairer online ecosystem for consumers to engage with.

Personnel

And finally, ideally, CR urges policymakers to consider two kinds of personnel transparency that would lead to improved online information ecosystems for consumers. First, transparency that would highlight whether a platform is appropriately staffed and resourced to enforce its own terms of service across the markets where it operates. This would particularly help to mitigate crises like platforms' disproportionate failures to moderate with the appropriate linguistic and cultural context in non-English-speaking markets. Domestically, failures bear consequences like the disproportionate spread of Spanish-language misinformation in the US, particularly around COVID-19 and vaccine information¹⁷—made even more concerning

¹⁶ USA Today, "Facebook apologizes to black activist who was censored for calling out racism" (Aug. 3, 2017) (online at: <https://www.usatoday.com/story/tech/2017/08/03/facebook-jeoma-oluo-hate-speech/537682001/>; see also: The Verge, "Facebook says it 'mistakenly' suspended hundreds of activists' accounts" (Sep. 24, 2020) (online at: <https://www.theverge.com/2020/9/24/21454554/facebook-activists-suspended-accounts-coastal-gaslink-pipeline>); see also: Washington Post, "YouTube's arbitrary standards: Stars keep making money even after breaking the rules" (Aug. 9, 2019) (online at: <https://www.washingtonpost.com/technology/2019/08/09/youtubes-arbitrary-standards-stars-keep-making-money-even-after-breaking-rules/>); see also: Sexuality and Culture, "Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online" (Nov. 6, 2020) (online at: <https://link.springer.com/article/10.1007/s12119-020-09790-w>); see also: Association for Computational Linguistics, In Proceedings of the Third Workshop on Abusive Language Online, pgs. 25–35. Davidson et. al, "Racial Bias in Hate Speech and Abusive Language Detection Datasets." (Aug. 1, 2019) (online at: <https://aclanthology.org/W19-3504.pdf>)

¹⁷ Washington Post, "Misinformation online is bad in English. But it's far worse in Spanish" (Oct. 28, 2021) (online at: <https://www.washingtonpost.com/outlook/2021/10/28/misinformation-spanish-facebook-social-media/>); see also:

considering that, according to a nationally-representative CR survey, 54% of Hispanic Americans reported that they regularly get news from social media — significantly higher than any other demographic surveyed.¹⁸ Meanwhile, as just one example, Facebook’s own oversight board recommended that it engage an independent entity to audit whether its content moderation and automation across Arabic and Hebrew are applied without bias.¹⁹ Any transparency reporting and risk assessments should include detailed breakdowns of content moderation and product design staff, ensuring appropriate sensitivity to nuance across linguistic and cultural differences where platforms operate.

Second, whistleblower protections for employees and contractors would prove invaluable—as we have already seen from the likes of pathbreaking whistleblowers like Ifeoma Ozoma, Sophie Zhang, and Frances Haugen.²⁰ Because no matter how many transparency reports and APIs are developed, without employee context for intention and trade-offs from design, enforcement, and implementation that — crucial components of the picture will remain missing. Congress should enshrine and codify strong whistleblower protections as a part of any transparency or accountability package.

H.R. 6796, the "Digital Services Oversight and Safety Act of 2022" (DSOSA)

The DSOSA lays out an ambitious plan for a new bureau at the FTC centered on the oversight and safety of digital services and platforms. Such central and devoted resources would be key for protecting consumers online, as a depth of expertise is required to effectively combat the harms stemming from the range of technologies, platforms, business models, that make up the information ecosystem. The bill would provide a level of both staffing and funds to the bureau befitting the broad scope of digital systems.

As we lay out in our platform accountability discussion above, DSOSA makes comprehensive platform transparency a key tenet of this new bureau. It also differentiates appropriate levels of transparency for different audiences—across different audiences—for the public, for independent researchers, and for the FTC. Such differentiation empowers consumers’ understanding, without putting the onus on consumer behavior alone to fix the platforms’ systemic failures. Crucially, DSOSA also recognizes that this transparency is ultimately in service of driving better understanding, prevention, and mitigation of the compounded harms that

Axios, “The Spanish-language misinformation crisis” (Feb. 8, 2022) (online at: <https://www.axios.com/social-media-misinformation-latinos-2c3574d4-d437-402c-8606-94c2f6332abf.html>); see also Time, “Facebook Says It’s Removing More Hate Speech Than Ever Before. But There’s a Catch” (Nov. 26, 2019) (online at: <https://time.com/5739688/facebook-hate-speech-languages/>)

¹⁸ August 2021 Consumer Reports nationally representative Social Media Survey of 2,263 US adults.

¹⁹ Facebook Oversight Board, Case decision 2021-009-FB-UA (2021) (online at: <https://www.oversightboard.com/decision/FB-P93JPX02>)

²⁰ AP, “How one Facebook worker unfriended the giant social network” (Oct. 10, 2021) (online at: <https://apnews.com/article/facebook-science-technology-business-congress-frances-haugen-80e92043b7211590b6be84dcc7a05b4a>)

platforms drive at scale. Rather than jumping feet first into new liability standards, it requires the largest platforms to consider, account for, and have audited their assessment of risks of societal harms throughout their systems.

While we do *not* think transparency must necessarily lead to adjustments to liability standards, DSOSA's transparency offerings could go a long way toward informing conversations around the appropriate level of liability platforms should bear, and it does not pretend to be a singular replacement for other varieties of tech policy reform (be it platform responsibility, privacy, antitrust, or otherwise), but would inform and improve all other reforms in tandem.

The bill covers substantial ground across all three transparency dimensions discussed above—ranging from process-based appeals and community standards expectations, to pipeline-based ad libraries and researcher data access, to enshrining related whistleblower protections for personnel. Again, while the bill does not pretend to be a silver bullet and focuses primarily on transparency, it would also introduce some concrete changes for consumers. As we highlight in our discussion of process transparency, it would require comprehensive appeals processes. Alongside, it would require largest covered platforms to offer an option that does not rely on any of the user's personal information to display information (with a reasonable exception for information critical to the products' functionality). And without adjusting platforms' liability immunities, it requires the largest platforms to do audited risk assessments & mitigation reports across a breadth of risks to consumers, which could incentivize greater responsibility. And, where it fails to incentivize such responsibility, the bill would still empower further research to dive into the compounding harms in the interim. Finally, we appreciate that given the bill's breadth, the scale of services covered, and the nuance required throughout the sector, how much of the bill is rooted in rulemaking, which we believe allows for the appropriate level of nuance and flexibility required of platform standards.

We also look forward to continuing to discuss elements of the bill's implementation with Representative Trahan's office, other congressional staff, and colleague organizations. While we are grateful for DSOSA's privacy protections, we do look forward to working together to strengthen such protections even further in future iterations — definitions of "deidentify" that align more closely with the three pillars laid out in the FTC's 2012 Privacy Report: achieving a reasonable level of justified confidence that the data cannot reasonably be used to infer information about a particular consumer or device; a commitment not to attempt to re-identify, and contractual obligations preventing any shared entities (if any) from attempting to reidentify.²¹ We would also be encouraged to see a broader scope of appeals in some instances. While the bill would empower users to appeal content removals or account termination, recognizing the shift

²¹ FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012) (online at: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>, pg. 21)

beyond the take-down/leave-up binary, we might be inclined to see the scope of mandated appeals expand to some of the more moderate moderation²² possibilities. These might include intermediate actions such as demonetization, feature suspensions, and downranking—not least because otherwise, one could envision a world where platforms pivot to downranking content and feature-limiting users nearly out of existence instead of terminating service outright, leading to even greater opacity.

II. Platform Accountability: Negligent Design & Consumer Protection Approaches

Online platforms need to take more responsibility for the design and maintenance of their digital products and services, and they should be obligated to consider values beyond shareholder value — be it consumer safety, civic well-being, or free expression. Platforms have repeatedly demonstrated themselves unwilling to take responsibility for the harms they accelerate.

In 2020, Facebook users reported a Kenosha Militia event asking attendees to bring weapons 455 times and the platform failed to act.²³ The same year, a CR investigation found Facebook’s ad approvals system approved a number of ads with misleading and outrageous COVID-19 misinformation.²⁴ YouTube failed to ban vaccine misinformation until September 2021—despite precedent in other tech platforms having done so as early as the first quarter of 2019—more than a year before the COVID-19 pandemic even began.²⁵

Investigative reports and agency investigations have repeatedly surfaced unsafe, untested, counterfeit, and even recalled products across Amazon, Facebook Marketplace, craigslist, and a variety of e-commerce platforms. Most gallingly, these often concern products with crucial safety implications, ranging from faulty carbon monoxide detectors to baby products and bike helmets that fail to meet safety standards.²⁶ Meanwhile, adding insult to injury, consumers bear

²² (no pun intended)

²³ BuzzFeed News, “A Kenosha Militia Facebook Event Asking Attendees To Bring Weapons Was Reported 455 Times. Moderators Said It Didn’t Violate Any Rules.” (Aug. 28, 2020) (online at:

<https://www.buzzfeednews.com/article/ryanmac/kenosha-militia-facebook-reported-455-times-moderators>)

²⁴ CR, “Facebook Approved Ads with Coronavirus Misinformation” (Apr. 7, 2020) (online at:

<https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation-a1864110559/>)

²⁵ NPR, “YouTube Is Banning All Content That Spreads Vaccine Misinformation” (Sep. 29, 2021) (online at: <https://www.npr.org/2021/09/29/1041493544/youtube-vaccine-misinformation-ban>); *see also* Washington Post, “Pinterest is blocking search results about vaccines to protect users from misinformation” (Feb 21, 2019) (online at: <https://www.washingtonpost.com/business/2019/02/21/pinterest-is-blocking-all-vaccine-related-searches-all-or-not-hing-approach-policing-health-misinformation/>)

²⁶ Wall Street Journal, “Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products” (Aug. 29, 2019), (online at: <https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990>); *see also* CR, “Bike Helmets That Don’t Meet Safety Standards Are Widely Available, Consumer Reports Finds” (July 1, 2019)

the consequences for e-commerce's well-documented fake reviews problem.²⁷ For years, a variety of platforms failed—and continue to fail—to take seriously the spread of misinformation, hate speech, and harassment of marginalized communities, contributing to the growth of offline extremism, violence.²⁸

These failures offer signposts to policymakers, indicating where legal incentives driving accountability may be worth either reinforcing or adjusting. And where online platforms clearly fail to take reasonable baseline steps to ensure their products are designed and managed responsibly, where they repeatedly choose engagement, profitability, or minimized operational costs, over harms to livelihoods, public health, and consumer well-being, there should be opportunity for recourse. Platforms should not be able to launch new products and features affecting billions of consumers without having built out the ability to reasonably enforce their own community guidelines or terms of service. Further, consumers should be able to expect that platforms have considered—and taken reasonable steps to mitigate—clearly foreseeable harms that such launches could compound or accelerate.

Section 230

While recognizing that Section 230 is not within the scope of the Consumer Protection Subcommittee, it would be irresponsible to discuss American platform accountability without some discussion. Section 230 has both protected and made possible key components of the internet's original promise *and* allowed online platforms more leeway to ignore the compounded scale of harms to consumers and society that their products and policies enable.²⁹

Reforming Section 230 should be approached cautiously, and many bills that have been proposed thus far would do far more harm than good. Some proposals to modify Section 230 would seek to *disincentivize* platform moderation altogether—when it's clear that platforms need to be doing more, not less, to foster a healthier online information ecosystem and keep consumers safe. Nevertheless, we are encouraged by various component parts of the PACT Act, the Protecting Americans from Dangerous Algorithms Act, and the Justice Against Malicious

(online at:
<https://www.consumerreports.org/bike-helmets/bike-helmets-that-dont-meet-federal-safety-standards-are-widely-available/>)

²⁷ TechCrunch, "Amazon deflects responsibility on fake reviews but admits 200M were blocked last year" (Jun. 16, 2021)

<https://techcrunch.com/2021/06/16/amazon-deflects-responsibility-on-fake-reviews-but-admits-200m-were-blocked-last-year/>, *see also* CR, "Hijacked Reviews on Amazon Can Trick Shoppers" (Aug. 26, 2019)

<https://www.consumerreports.org/customer-reviews-ratings/hijacked-reviews-on-amazon-can-trick-shoppers/>

²⁸ 2021 IEEE Symposium on Security and Privacy (SP), K. Thomas *et al.*, (2021) "SoK: Hate, Harassment, and the Changing Landscape of Online Abuse," pgs. 247-267, doi: 10.1109/SP40001.2021.00028.

²⁹ As we discuss at length here:

<https://medium.com/cr-digital-lab/crs-section-230-2020-legislative-round-up-4683c309fcb3>.

Algorithms Act (JAMAA), and hope to see such conversations continue in keeping with the principles that follow.³⁰

As a general rule, and especially in the wake of FOSTA-SESTA,³¹ eliminating Section 230 (c)(1) immunities—immunities for hosting and disseminating third-party content—by way of subject matter exemptions alone) would be irresponsible. Subject matter exemptions alone are wont to drive brunt, over-broad platform responses without addressing existing failures in platform moderation systems. However, there may be room to explore narrow subject matter exceptions when they are in combination with additional narrowing factors, such as a platform’s mechanism of delivering the content. Such proposals would be along the lines introduced by the Protecting Americans from Dangerous Algorithms Act, which opened narrow civil liability for certain existing civil rights claims when platforms amplified the content in question.

Modifications that would seek to disincentivize moderation, either by removing Section 230 immunity for many subsets of content moderation, or by conditioning (c)(1) immunity on “neutral” enforcement, would run counter to consumer interests, as consumers require platforms to take more—not less—responsibility for the harms they accelerate. As discussed in the Transparency section above, process improvements and accountability mechanisms—like those found in the PACT Act, and throughout the DSOSA—would strongly benefit consumers.

JAMAA would modify Section 230 to open platforms to liability where the provider “knew or should have known” it was making a “personalized recommendation” of information, did so recklessly, and the recommendation materially contributed to injury. We are most concerned that the bill’s knowledge standard would functionally the bill’s knowledge standard would functionally strip Section 230 protections for any algorithmically sorted content, strongly deterring platforms from using algorithms in contexts where they may be useful. However, the JAMAA’s approach furthers a useful line of conversation around Section 230, as we would be encouraged to find room to pursue further cases along the lines of negligent design (more on this below), or otherwise develop reasonable expectations on platform design. without opening the potential for so much liability that extreme over-moderation or over-monitoring of content would result.

Harmful Design

³⁰Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong., (2021); Justice Against Malicious Algorithms Act, H.R. 5596, 117th Cong., (2021)

³¹ Passed in 2018, this legislation combined Senate’s Allow States and Victims to Fight Online Trafficking Act of 2017 (FOSTA), which combined a House bill of the same name with provisions from a Senate bill, the Stop Enabling Sex Traffickers Act (SESTA), which modified Section 230 with an exception to 230(e) to fight sex trafficking. It was a contentious measure whose full impacts are still unclear, but that has so far had clear effects on the speech of marginalized communities online. See: Fordham Law Review, “FOSTA: A Hostile Law with a Human Cost” (2019) (online at: <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5598&context=flr>); see also Out, “The Dangerous Trend of LGBTQ+ Censorship on the Internet” (Dec. 6, 2018) (online at: <https://www.out.com/out-exclusives/2018/12/06/dangerous-trend-lgbtq-censorship-internet>.)

Across a variety of consumer products, it is well understood that fundamentally, manufacturers and companies should bear responsibility for their design and process choices that lead to foreseeable, preventable harms to consumers using the product in its intended manner. While the way that digital products intersect with consumer data and speech complicate the premise, room remains to expand the conversation to the digital sphere.³²

Lemmon v. Snap, Inc. is an ongoing civil lawsuit against Snap Inc, brought by the parents of two teenagers who died tragically in a car accident after reaching 123 miles per hour. The parents' suit alleges that Snapchat—having designed and offered both a “speed filter” and intermittent, unpredictable engagement-based rewards of “trophies, streaks, and social recognitions” that in combination could incentivize young drivers to drive at dangerously high speeds—was negligently designed. The Ninth Circuit found that Snap was “sued for the predictable consequences of designing Snapchat in such a way that it allegedly encouraged dangerous behavior.” And it further found that Snap could not avail itself of Section 230 (c)(1) immunity because the suit did not rely on “information provided by another information content provider,” but on Snap’s, “duty to design a reasonably safe product [which] was fully independent of [its] role in monitoring or publishing third-party content.”³³

While the district court has yet to determine whether Snap is liable, that such liability is not precluded by Section 230 immunity seems to be the right result, and one legislators may wish to carefully expand. CR would be encouraged to see perhaps even a slightly broader legal avenue to pursue recourse when consumers are subject to digital products that, as-designed, or as-maintained could lead to clearly foreseeable harms—whether by way of nuanced tweaks to Section 230 or other means of imposing baseline consumer protection expectations for platforms to undertake basic best practices and reasonable steps to anticipate, prevent, and mitigate the harms their systems can accelerate, rather than apologizing for them³⁴.

FTC Act Section 5

Regulators also may be already able to take action against platforms that fail to take reasonable measures to protect users from the harmful acts of others on their platforms. Section 5 of the FTC Act broadly prohibits companies from committing “unfair or deceptive acts or practices” in the marketplace. Certainly if a company commits to taking certain acts to remediate bad activity, the FTC could find that failure to follow through on those commitments constitutes a deceptive practice. Moreover, in some situations, failure to enforce clear platform rules against

³²Lawfare, “Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must be Fixed” (Aug. 14, 2019) (online at: <https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed>)

³³ *Lemmon v. Snap, Inc.*, No. 20-55295 (9th Cir. 2021)

³⁴ Wired, “Why Zuckerberg’s 14-Year Apology Tour Hasn’t Fixed Facebook” (Apr. 6, 2018) (online at: <https://www.wired.com/story/why-zuckerberg-15-year-apology-tour-hasnt-fixed-facebook/>)

bad actors could be considered deceptive, as the existence of rules in the first place may be reasonably interpreted as an implicit promise to reasonably enforce them.

The other half of the FTC's general purpose consumer protection law is "unfairness." To constitute an unfair business practice, it might (1) cause consumers significant injury, (2) not be reasonably avoidable by consumers, and (3) is not offset by countervailing benefits to consumers or competition.³⁵ Historically, the FTC has brought many cases against companies for failing to reasonably police the behaviors of others. For example, since 2002, the FTC has brought over 80 cases against companies for failure to institute reasonable security measures to protect consumers' personal information.³⁵ Even though the threat in those cases was from hackers and other malefactors, the FTC found that companies' failure to take cost-effective means to prevent those bad actors from accessing consumers' data constituted an unfair practice: it exposed consumers to the risk of significant injury, the poor security was not reasonably avoidable by consumers, and the failure to institute safeguards was not outweighed by other consideration. Similarly, the FTC could find that platforms' failure to protect consumers from bad actors by other users of the platform could also constitute an unfair business practice.

III. Algorithmic Accountability

As algorithms and artificial intelligence become more embedded into everyday decisionmaking, the potential for discrimination, misuse, and other harm is real and alarming. Algorithms can contribute to disparate impacts in areas like housing, credit, employment and also can contribute to exacerbated power dynamics between consumers and technology companies.

Engineers often use historical data when training algorithms to make decisions. For example, a company designing an algorithm attempting to predict where crime occurs most often in a city might use historical data about where crime has occurred most often in the past — however, this type of data could be skewed towards communities that tend to be over-policed,³⁶ algorithms like these can reinforce racial biases and exacerbate societal inequalities. Furthermore, many algorithms tend to be quite opaque — even to the engineers that design them.³⁷

While discrimination is already prohibited in many sectors where algorithms are used, it can be difficult whether to tell whether algorithmic discrimination is occurring at all due to the

³⁵ FTC, "Federal Trade Commission 2020 Privacy and Data Security Update" (2020) (online at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf)

³⁶ EFF, "Technology Can't Predict Crime, It Can Only Weaponize Proximity to Policing" (Sep. 3, 2020) <https://www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-only-weaponize-proximity-policing>

³⁷ MIT Technology Review, "The Dark Secret at the Heart of AI" (Apr. 11, 2017) (online at: <https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/>)

"black box" nature of many algorithms and the lack of transparency regulations. Consumers and citizens deserve explanations on how algorithms come to their decisions, particularly when used for sensitive applications; otherwise, progress made by antidiscrimination law will be heavily rolled back. People should also be able to contest inaccurate or false outcomes of an algorithm in a straightforward process.

Consumer Reports believes that we need increased regulation regarding algorithms which include increased transparency measures (on what kinds of data an algorithm uses and how the algorithm comes to a decision) to both the public and regulators, improved testing and auditing standards for algorithms used in areas with significant legal effects, and clearer restrictions on how and when certain algorithms can and should be used. We also need regulation that better outlines the rights of consumers and citizens when using the algorithms or when an algorithm makes a decision about an individual — including more individual agency of the use of algorithms, being given clear explanations about how a particular algorithmic decision works or how an algorithm arrived to its outcome, and being able to contest decisions.

H. R. 6580, The Algorithmic Accountability Act, is an important piece of legislation that can lay the foundation for these issues. While the bill doesn't necessarily require third-party auditing or other independent oversight over a company's testing process (something we think should happen with algorithms used in sensitive areas) or restrict when algorithms can be used, it does require companies to be more thoughtful about their design and testing processes. The various requirements that are discussed regarding a company's algorithmic impact assessment will force companies to consider things like stakeholder engagement, consumer rights in regards to opting-out or contesting algorithmic decision making, and potential negative impacts of the technology.

While stricter regulations are still needed to create better oversight and restrictions for algorithms used in various sectors, this bill is an important first step that can provide regulators and the public some transparency into how companies design and evaluate their algorithms. CR has put out a petition³⁸ urging Congress to pass the Algorithmic Accountability Act, and over 20,000 people have signed on so far. We urge Congress to pass this much needed piece of regulation which will lay the groundwork of making AI more safe and equitable for all.

IV. Surveillance Advertising

CR has long been a supporter of strong comprehensive privacy legislation. Last February, Consumer Reports released its Model State Privacy Act that strictly prohibits most secondary

³⁸CR, "Cost of Love: Tinder charged higher price to older daters" (2022) (online at: https://action.consumerreports.org/20220209_finance)

data processing,³⁹ including for cross-context targeted ads.⁴⁰ In January of this year, we released a white paper along with the Electronic Privacy Information Center calling on the FTC to use its dormant rulemaking authority under Section 5 of the FTC Act to enact strong privacy rules that would likewise mandate strict data minimization and prohibit most secondary uses.⁴¹ We see FTC rulemaking only as a fallback to Congressional action: Consumer Reports has previously testified before this subcommittee on the need for Congress to pass long-overdue legislation to clamp down on unwanted surveillance and unwanted ad targeting.⁴²

We support the goals of the Banning Surveillance Advertising Act. Consumers overwhelmingly object to being tracked across different websites, apps, smart devices, and even in the physical world by hundreds of different companies just to show them relevant ads.⁴³ We appreciate that the bill is framed as a straight prohibition on surveillance advertising instead of conditioning it on opt-out or opt-in consent. In practice, opt-out rights under the California Consumer Privacy Act (CCPA) have proven to be burdensome and unworkable—it is not practical to expect consumers to navigate and manage hundreds or thousands of individual opt-outs for every site, app, or store they visit.⁴⁴ On the other hand, mandating opt-in for tracking creates burdens as well—in response to GDPR and the ePrivacy Directive, many sites forced users through tedious consent screens every time they visited a site, often using confusing language and “dark patterns”⁴⁵ to get a user to ostensibly provide “consent” to having their data shared with hundreds of companies. A simple prohibition on a universally despised practice is a better approach.

³⁹ By “secondary processing,” we mean data collection, sharing, and use not strictly necessary to provide a service which a consumer has requested. If you buy a product online, your credit card number and home address may be collected and shared with a payment processor or a delivery service. However, these uses are “primary uses” are they’re necessary to complete the transaction, and consumers generally understand what’s going on. “Secondary processing,” on the other hand, involves use and sharing for unrelated purposes, including sharing with data brokers and for targeted ads.

⁴⁰ CR Advocacy, “Model State Privacy Act” (Feb 2021) (online at: https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.)

⁴¹ Consumer Reports and the Electronic Privacy Information Center, “How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking” (Jan. 26, 2022), (online at: https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf)

⁴² Testimony of Justin Brookman, Director, Privacy and Technology Policy, Consumers Union, Before the United States House of Representatives Committee on Energy & Commerce Subcommittee on Digital Commerce and Consumer Protection, Hearing on “Understanding the Digital Advertising Ecosystem,” June 4, 2018, <https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-Wstate-BrookmanJ-20180614.pdf>

⁴³ E.g., Benson Strategy Group, Future of Tech Commission: Tech Attitudes Survey (July 20, 2021 - July 29, 2021), https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/pdfs/bsg_future_of_technology_topline_c1-1.pdf.

⁴⁴ CR Advocacy, “California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?” (Oct. 1, 2020), (online at: https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf)

⁴⁵ The term “dark patterns” refers generally to manipulative user interfaces designed to trick users into providing consent for potentially unwanted services or data processing. For more information see generally <https://www.darkpatterns.org/>.

However, focusing just on targeted ads is in our opinion too narrow an approach — there are tons of other ways that personal data can be collected and sold that intrudes on our personal spaces⁴⁶ and subjects us to adversarial uses.⁴⁷ We would prefer a more expansive bill that addresses surveillance beyond ad targeting. That said, stopping targeted ads alone is itself a worthy mission and would accomplish a lot of good for consumers beleaguered by constant tracking.⁴⁸

Finally, we have some concerns about some of the loopholes and definitions in the bill that could ultimately undermine its effectiveness. For example, Section 2(a)(3) of the bill exempts ads based on information shared by advertisers themselves (or third parties on their behalf) to advertising facilitators. This provision would exclude much if not most surveillance advertising. Consider the canonical example of surveillance advertising: you browse a pair of shoes for sale, and then those shoes follow you all over the internet, showing up in ads on other sites, in other browsers, or even other devices. Here, because the data was shared by the shoe site to its partners in the ad tech ecosystem, it falls outside the protections of the act.

Similarly, the term “advertisement” is counterintuitively defined as:

information provided by an advertiser to an advertising facilitator
that the advertising facilitator, in exchange for monetary
consideration or another thing of value, disseminates to an
individual, connected device, or group of individuals or connected
devices.

In practice, much of the information used for surveillance advertising is arguably not provided for consideration — instead, typically an advertiser gives *both* the data and money to an advertising facilitator in order to show an ad. It’s the ad space that is sold, the data is just used to make the ad more targeted. In fact, advertisers adopted such an interpretation of the term “sale” under the CCPA that led to many ad tech firms simply declaring that their activities fell outside the scope of the law.⁴⁹ Unfortunately, experience has shown that privacy laws must be drafted extremely precisely, as companies have adopted bad faith interpretations of laws like the CCPA and GDPR, grasping onto dubious readings to preserve the status quo and avoid fundamentally

⁴⁶ American Civil Liberties Union, Face Recognition Technology, online at: <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology>.

⁴⁷ FTC, “Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA” (Jun. 12, 2012) (online at: <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>)

⁴⁸ Accountable Tech, “Re: Petition for Rulemaking to Prohibit Surveillance Advertising,” (online at: <https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf>)

⁴⁹ Mediapost, “Some Advertisers See Loophole in California Privacy Law” (Oct. 22, 2019) (online at: <https://www.mediapost.com/publications/article/342338/some-advertisers-see-loopholes-in-california-privacy-law.html>)

changing their behaviors. While regulators in both California⁵⁰ and the EU⁵¹ have begun to take action to rein in the most absurd interpretations, many companies have been able to effectively skirt legislators' intentions by hiding in unintended loopholes.

V. Other Relevant FTC Powers and Authorities

Finally, for new laws to have any real impact on giant technology companies, regulators must be funded and empowered to take action. Today, the Federal Trade Commission has only 1100 employees to pursue both its consumer protection and competition missions.⁵² This number has been roughly flat over the past twelve years, and actually represents a decrease from 1746 FTEs in 1979. Put another way, since that time, the economy has grown nearly three times while the FTC's capacity has decreased 37 percent. It is not reasonable to expect the FTC to be able to hold the biggest tech companies accountable on its current shoestring budget. Consumer Reports has consistently called for Congress to substantially increase the FTC's budget to give it the resources to bring on technologists and other staff to give the agency a fighting chance to achieve the goals for which Congress created it.⁵³ We are glad that [xxx bills provide for funding] they are a good start, but even more is needed.

And there must be consequences for companies that break the law. Today, when a company violates consumer protection law, the FTC largely has no ability to obtain any monetary relief at all from the company. After the Supreme Court's decision last year in *AMG Capital Management v. Federal Trade Commission*, the FTC does not even have the legal authority to get refunds for consumers who have been ripped off by fraudsters.⁵⁴ It is outrageous that scam artists are today legally entitled to keep their ill-gotten gains even after they are caught. Congress has the ability to enact a simple fix to the law to give the FTC the ability to obtain injunctive relief from wrongdoers, but so far it has failed to take action. Last year, Consumer Reports testified before this Subcommittee in support of the Consumer Protection and Recovery

⁵⁰ Digiday, "California Attorney General says popular, digital ad opt-outs from trade groups don't comply with CCPA" (Aug. 3, 2021) (online at: <https://digiday.com/media/california-attorney-general-says-popular-digital-ad-opt-outs-from-trade-groups-dont-comply-with-ccpa/>)

⁵¹ IAPP, "Belgian DPA fines IAB Europe 250K euros over consent framework GDPR violations" (Feb. 5, 2022) (online at: <https://iapp.org/news/a/belgian-dpa-fines-iab-europe-250k-euros-over-consent-framework-gdpr-violations/>)

⁵² FTC, "FTC Appropriation and Full-Time Equivalent (FTE) History" (online at: <https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriations>)

⁵³ CR Advocacy, "Letter from Consumer Reports to Chairs Delauro and Quigley and Ranking Members Granger and Womack" (May 25, 2021) (online at: <https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR-letter-on-FTC-appropriations-052521.pdf>.)

⁵⁴ *AMG Capital Management LLC v. Federal Trade Commission*, __ U.S. __ (2021).

Act to restore the FTC's equitable authority; we strongly urge Congress to pass this simple fix to give the FTC what should be the least controversial tool it needs in order to protect consumers.⁵⁵

Of course, even that authority will not be enough to deter wrongdoers — the FTC must be able to obtain statutory penalties as well. If the only consequence of getting caught is to refund what you stole, bad actors will take what they please, knowing that no regulator (even if fully funded) has the ability to catch everybody. Today, state attorneys general have the ability to exact civil penalties from companies that break the law; the FTC must be empowered to do the same. Otherwise, giant technology companies will feel comfortable pushing the boundaries of (or potentially just ignoring) laws intended to rein in their worst behaviors.⁵⁶

⁵⁵ Testimony of Anna Laitin, Director, Financial Fairness and Legislative Strategy, Consumer Reports, Before the United States House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce, Hearing on “The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers,” April 27, 2021, (online at:

https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Laitin_CPC_2021.04.27.pdf)

⁵⁶ The FTC has been able to obtain civil penalties in a handful of cases against big companies, but only because those companies were caught violating settlement agreements they had previously reached with the FTC over earlier law violations. *E.g.*, Federal Trade Commission, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, July 24, 2019,

<https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>. The FTC also has the ability to obtain civil penalties under certain sectoral privacy statutes such as the Children's Online Privacy Protection Act (COPPA). *E.g.*, Federal Trade Commission, *Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law*, September 4, 2019, <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>. However, the considerable majority of the FTC's consumer protection cases are brought enforcing the general prohibition against “unfair or deceptive acts or practices”; in those cases, the FTC is not empowered to obtain penalties from wrongdoers.

Ms. SCHAKOWSKY. Well, thank you. And now Ms. McInnis from DuckDuckGo is recognized for 5 minutes.

STATEMENT OF KATIE MCINNIS

Ms. MCINNIS. Thank you, Chair. Chair Schakowsky, Ranking Member Bilirakis, Chairman Pallone, Ranking Member McMorris Rodgers, and members of the subcommittee, thank you for holding this important hearing and inviting me to testify. I am here to discuss DuckDuckGo's privacy-protected business model, and why we need bills like the Banning Surveillance Advertising Act to protect individuals online and to reform the general market.

DuckDuckGo is a privacy technology company. We believe that privacy is a human right, and that being private online should be simple and accessible to all. With one download of the DuckDuckGo privacy browser for mobile or the DuckDuckGo privacy essentials browser extension for desktop, we offer seamless protection from surveillance ads by blocking trackers. This includes our email protection service, our tracker blocker technology, and our private search engine, which is the fourth largest in the United States, and serves over three billion searches a month, globally. Our company was founded in 2008 in Valley Forge, Pennsylvania. And year after year, we have seen record growth, proving users' interests in being private online.

DuckDuckGo is robustly profitable, and has been since 2014, thanks to our contextual ad model. Contextual advertisements are based on the content being shown on the screen, and not—and do not need to know anything about you. So if you go to DuckDuckGo and perform a search—let's say you search for mobile phones, we are going to serve you with ads for phones. It is as simple as that.

Behavioral advertising, by contrast, is based on personal profiles from data collected both on and offline about you. Have you ever searched for something online, and then saw an ad for that exact same thing pop up on another website, or an app? Or maybe you thought that your phone is listening to you, based on the creepy ads that you are seeing online? That is surveillance advertising. And rather than finding these ads useful, a majority of Americans say that this is a misappropriate use of their data. And it is no surprise this is a massive violation of their user privacy and data collection expectations.

And it is not just that. Data collection also results in additional harm, like discrimination, identity theft, fraud, scams, and filter bubbles. This same personal information that allows a company to target you with an ad also enables them to discriminate against you and others in the presentation of critical opportunities. And these harms are not just theoretical.

For instance, the Department of Housing and Urban Development brought a case against Facebook, charging them with housing discrimination by allowing advertisers to restrict who saw ads based on race, religion, and national origin. This is a harm that was made possible, thanks to data collection for surveillance ads.

Online surveillance also enabled advertisers to use Google's ad tracking—ad targeting algorithm to present more men than women with ads for higher-paying jobs. The practice of data collection,

therefore, is not just about a user's privacy or data collection expectations, but about the presentation of critical access to opportunities and employment.

Consumers should have an easy and effective way to avoid this surveillance. And as our history makes clear, internet companies can be successful and profitable with a contextual ad model. Studies have additionally shown that publishers receive very little significant increase in revenue by using behavioral ads. And in fact, many online advertising companies started with a contextual ad model, including Google. Until recently even, most of the ads you are seeing online were contextual ads. However, due to Google's acquisition of DoubleClick and Facebook's ad—Facebook's control of the ad duopoly with Google, there has been a focus on behavioral advertising, and innovation in contextual advertising has been severely suppressed.

If data collection for targeted ads were banned, access to personal data would no longer determine whether companies would succeed or fail in the advertising market, meaning that more companies would be able to compete against Google and Facebook's ad duopoly.

As surveillance ads result in measurable harm for users and little to no increase in revenue for publishers, we must ask, "What is all this surveillance for, if it is not just lining the pockets of Facebook and Google?"

As a House Antitrust Subcommittee report and reports from governments around the world demonstrate, access to personal data enables Big Tech to protect and entrench their dominant status online, generally, and in the ad market, in particular. A shift back to contextual advertising, therefore, would significantly reduce Google and Facebook's inherent advantages in advertising and beyond.

Our mission at DuckDuckGo is to raise the standard of trust online. We therefore support bills like the Banning Surveillance Advertising Act that would do exactly that. Consumers should be protected from the harm surveillance advertising and data collection cause, like discrimination, identity theft, scams, and fraud.

We believe that getting privacy online should be as simple as closing the blinds. Therefore, we urge Congress to pass bills that allow individuals to easily protect themselves and would also have the benefit of strengthening the online market.

I am pleased to answer your questions today, and make myself available to members in the future for in-depth discussions about this bill. Thank you.

[The prepared statement of Ms. McInnis follows:]



Duck Duck Go, Inc.
20 Paoli Pike • Paoli, PA 19301, United States
+1 267.690.7758 • duckduckgo.com

Katie McInnis

Senior Public Policy Manager, US
Washington, DC
kmcinnis@duckduckgo.com

Written Testimony of Katie McInnis

Senior Public Policy Manager US for Duck Duck Go, Inc.

Before the U.S. House Committee on Energy and Commerce, Consumer Protection and Commerce
Subcommittee

Hearing on Holding Big Tech Accountable: Legislation to Protect Online Users

March 1, 2022

Chair Schakowsky, Ranking Member Bilirakis, and Members of the Subcommittee, thank you for holding this important hearing and inviting me to testify. I'm here to discuss DuckDuckGo's privacy-protective business model and why we need bills like the Banning Surveillance Advertising Act of 2022 to protect individuals online and reform the digital marketplace.

DuckDuckGo is a privacy technology company.¹ We believe that privacy is a human right and that being private online should be simple and accessible to all. With one download of the DuckDuckGo Privacy Browser for mobile or the DuckDuckGo Privacy Essentials browser extension for desktop, we offer seamless protection from invasive tracking. This includes our email protection service, our tracker blocker technology on the web as well as for apps on the Android operating system, and our private search engine that is the fourth largest in the United States and serves over three billion searches a month globally.

In short, DuckDuckGo helps you avoid surveillance ads (also known as behavioral ads) and data collection by seamlessly reducing your digital footprint through the blocking of hidden third-party trackers. And because we do not collect information about your search or browsing history, every time you search on DuckDuckGo it is like you are searching for the first time. Unlike most of our competitors, we do not engage in personal profiling to decide what you see online or serve you with personalized results or ads in response to your search queries.

Our company was founded in 2008 in Valley Forge, Pennsylvania. We now have employees in 24 states

¹ About, DUCKDUCKGO, <https://duckduckgo.com/about> (last visited Feb. 28, 2022).



and the District of Columbia. Year after year, we have seen record growth in our downloads, search queries, and our search engine market share, proving users' interest in being more private online. This growth enables us to commit to and expand our social impact and sustainability programs. For example, every year we donate a portion of our revenue to support non-profits around the world that work to protect digital rights and freedoms online.²

DuckDuckGo has been robustly profitable since 2014 thanks to the contextual advertisements shown to users on our search engine. Contextual advertisements are based on the content being shown on the screen and do not need to know anything about you: If you search for “mobile phones” you will get advertisements for phones. It’s that simple.

Contextual advertising contrasts with behavioral advertising, which is based on personal profiles from data collected both on and offline about the person viewing the ad. Have you ever searched for something online only to see an advertisement for that very thing show up again in ads on apps or other websites? Do you ever feel like your phone is listening to you based on the ads you see online? That is surveillance advertising. It is the invasive ads that follow you around. Rather than finding these ads useful, multiple studies have shown that the majority of people in the U.S. think this this kind of advertising is an inappropriate use of their personal data.³

The covert collection of personal information for surveillance advertisements allows companies to granularly target individuals, violating user privacy and expectations on data collection. But what many users are not aware of is that this data collection also results in additional harm like discrimination, identity theft, fraud, and filter bubbles. The same personal information that enables a business to target potential customers with creepy ads also enables companies to discriminate against users in the presentation of critical opportunities, like education, employment, housing, and financial services.

And these harms are not just theoretical. The Department of Housing and Urban Development charged Facebook with engaging in housing discrimination by allowing advertisers to restrict who sees ads based on race, religion, and national origin, a harm made possible thanks to data collection for surveillance ads.⁴ Online surveillance also enabled advertisers to use Google’s ad targeting algorithm to present more men than women with ads for higher-paying jobs.⁵ The practice of data collection therefore does not just

² *Advancing Privacy Worldwide*, DUCKDUCKGO, <https://duckduckgo.com/donations> (last visited Feb. 28, 2022).

³ *Perception of targeted advertising according to adults in the United States as of May 2019*, STATISTA, <https://www.statista.com/statistics/993399/adult-opinion-targeted-ads-us/> (last visited Feb. 28, 2022); *57% of US consumers would forego marketing personalization to protect their data*, MARKETINGDIVE (Nov. 17, 2020), <https://www.marketingdive.com/news/57-of-us-consumers-would-forego-marketing-personalization-to-protect-their/589189/>.

⁴ Katie Benner, Glenn Thrush, & Mike Issac, Facebook Engages in Housing Discrimination with Its Ad Practices, U.S. Says, N.Y. TIMES (Mar. 28, 2019), <https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html>.

⁵ Amit Datta, Michael Carl Tschantz, & Anupam Datta, *Automated Experiments on Ad Privacy Settings*, PROCEEDINGS ON PRIVACY ENHANCING TECH. (2015), <https://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf>.



affect a user's right to privacy, but also their ability to access critical opportunities and services.

Consumers should have an easy and effective way to avoid being surveilled online. That's why DuckDuckGo supports bills that would protect consumers from online and offline collection of their personal information.⁶ The Banning Surveillance Advertising Act would effectively protect users from companies collecting their personal data for the purpose of serving them with targeted advertisements. DuckDuckGo has also supported state measures that protect consumers. For example, we have been a lead supporter in the creation of the browser-based Global Privacy Control setting under the California Consumer Privacy Act.⁷

As our history makes clear, Internet companies can be successful and profitable with a contextual advertising business model and without surveilling individuals online. In addition, studies from researchers like Alessandro Acquisti have found that behavioral advertising does not result in a significant increase in revenue for publishers.⁸ Although dominant tech companies may make significant revenue through surveillance advertising now, there is no reason why contextual advertising couldn't be as relevant as behavioral advertising, by drawing on the context of the website, video, or audio being consumed.

In fact, many online advertising companies started with a contextual ad model. Even DuckDuckGo's primary search competitor, Google, used contextual advertising in the beginning. However, Google's purchase of DoubleClick in 2007 pushed the company to pivot to surveillance advertising and helped the company to establish its current dominance in digital ads.⁹ This switch gave Google a strategic advantage in the online advertising market, along with Facebook, because of their ability to collect massive amounts of personal data from users.

Despite growing privacy concerns among Americans,¹⁰ Google has not turned away from their surveillance business model. Google's response to consumers' desire for privacy, a so-called "Privacy Sandbox,"¹¹ will only serve to maintain Google's dominance without changing the fact that Google will

⁶ The Do-Not-Track Act of 2019, DuckDuckGo, <https://spreadprivacy.com/do-not-track-act-2019/> (last visited Feb. 28, 2022).

⁷ *DuckDuckGo Founding Member in Global Privacy Control (GPC) Standards Effort*, DUCKDUCKGO (Oct. 7, 2020), <https://spreadprivacy.com/announcing-global-privacy-control/>.

⁸ Keach Hagey, *Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests*, WALL ST. J. (May 29, 2019), <https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195>.

⁹ Steve Lohr, *This Deal Helped Turn Google into an Ad Powerhouse. Is That a Problem?*, N.Y. TIMES (Sept. 21, 2020), <https://www.nytimes.com/2020/09/21/technology/google-doubleclick-antitrust-ads.html>.

¹⁰ Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CTR. (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

¹¹ The Privacy Sandbox, Chrome Developers, <https://developer.chrome.com/docs/privacy-sandbox/> (last visited Feb. 28, 2022).



continue to, by default, surveil consumers' online activity and share information about them with advertisers and other parties for the purpose of behavioral advertising.¹² Instead of continuing to automatically bombard users with targeted advertisements that enable discrimination and other harms, we need to re-open the market for contextual advertising.¹³

For some time now venture capital has been largely unwilling to fund competitor advertising companies due to Google's and Facebook's strategic data advantages. As a result, innovation in the contextual advertising market has been severely suppressed. However, if consumers were protected from data collection for surveillance ads, the ability of dominant tech companies like Facebook and Google to continue stifling innovation in this market would be significantly diminished. Because access to massive troves of data would no longer determine success in the digital advertising market, more companies would be able to compete against Google and Facebook's ad duopoly.¹⁴ As surveillance ads result in measurable harm and fail to provide much added revenue for publishers, what is this surveillance for anyway, outside of maintaining this duopoly?

The 2020 Investigation of Competition in Digital Markets report from the Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary found that the concentration in the ad market is due in part to high barriers to entry: "Google and Facebook both have a significant lead in the market due to their significant collection of behavioral data online, which can be used in targeted advertising."¹⁵ Furthermore, reports from the United States and governments around the world have documented how access to individuals' private data enables companies like Google to further anchor their dominance and thwart competition from companies like DuckDuckGo outside of advertising. A shift back to contextual advertising would significantly reduce their inherent advantages, both in advertising and beyond.

Our mission at DuckDuckGo is to raise the standard of trust online. We, therefore, support bills like the Banning Surveillance Advertisements Act of 2022 that would do exactly that. Consumers should be protected from the data collection required to target them with surveillance ads and the subsequent

¹² *Use the DuckDuckGo Extension to Block FLoC, Google's New Tracking Method in Chrome*, DUCKDUCKGO (Apr. 9, 2021), <https://spreadprivacy.com/block-floc-with-duckduckgo/>; Bennett Cyphers, *Google's FLoC Is a Terrible Idea*, ELECTRONIC FRONTIER FOUND. (Mar. 3, 2021), <https://www EFF.ORG/deepinks/2021/03/googles-floc-terrible-idea>.

¹³ Gabriel Weinberg, *What if We All Just Sold Non-Creepy Advertising?*, N.Y. TIMES (July 19, 2019), <https://www.nytimes.com/2019/06/19/opinion/facebook-google-privacy.html>; John Flenday, *CMA boss blasts Facebook and Google ad market 'duopoly'*, THE DRUM (Feb. 24, 2021), <https://www.thedrum.com/news/2021/02/24/cma-boss-blasts-facebook-and-google-ad-market-duopoly>.

¹⁴ *Facebook and Google 'too powerful' says watchdog boss*, BBC (Feb. 23, 2021), <https://www.bbc.com/news/business-56174671>.

¹⁵ *Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations*, SUBCOMM. ON ANTITRUST, COMMERCIAL, & ADMIN. LAW OF THE COMM ON THE JUDICIARY (Oct. 2020), https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.



harms this data collection makes possible, like discrimination, identity theft, and fraud. We believe that getting the privacy you deserve online should be as simple as closing your blinds. We, therefore, encourage Congress to pass bills that would allow individuals to easily protect themselves online and would also have the effect of strengthening competition in the online market.

I am pleased to answer your questions today and make myself available to Members in the future for in-depth discussions about this bill and others that would reform the online ecosystem for the better. Thank you.

Ms. SCHAKOWSKY. Thank you. And now it is my pleasure to invite Mr. Duffey for 5 minutes.

STATEMENT OF MIKE DUFFEY

Mr. DUFFEY. Thank you, Madam Chair Schakowsky and Ranking Member Bilirakis, and members of the subcommittee. Thank you for inviting me today. I serve as assistant special agent in charge of Florida Department of Law Enforcement's—crimes unit.

I started my law enforcement career during the AOL dial-up days. And in the 25 years since, I have seen massive changes in the way crime is committed and investigated. In that time I have learned that, whether crimes are committed in the virtual world or in the physical world, technology companies possess a large amount of essential evidence law enforcement needs to do our job. But lack the regulatory framework that enables efficient and lawful access to that evidence means that we are ineffective at reducing criminal threats, preventing victimization, or getting justice for the victims (sic).

My investigative unit at FDLE, like thousands of others across local, State, and Federal law enforcement, is in a never-ending race to improve our access to digital evidence. We need money for training and tools to access evidence we can obtain from devices that we seize. But we are also facing increased challenges with the complete inability to access digital evidence when platforms deploy end-to-end encryption. Congress can help us address both of these issues.

I want to share today with you a few examples of the challenges we are facing. Service providers are subject to little or no data retention requirements. In contrast, the banking industry is obligated to keep financial records for a certain period of time.

In one example of how this can hurt our ability to respond to a crisis, a young person was livestreaming how he was going to commit suicide, potentially in front of a live audience. We immediately contacted the service provider that we had received this information, and to try to attempt to determine where the user was located. We noted that the live stream appeared to have ended, and the content provider was unable to find the record of the streaming event. We had nothing to followup on, if it had not been for the family's own posting that they had intervened.

The lack of data retention requirements frustrates the most traumatic cases we deal with every day, which is the child sexual abuse cases. Service providers do—who do identify CSAM on their platforms are required to report it to our partners at the National Center for Missing and Exploited Children. An investigation then begins with an agency serving legal process to a company for internet protocol information in an attempt to identify where the activities were occurring. If the provider does not retain data, a user has deleted it, the child predator becomes harder to identify and stop.

The lack of standard terminology regarding the exchange of legal process between law enforcement and service providers leads to great confusion. Unless the terms we use to determine certain types of data matches within the own company's unique corporate

terms, law enforcement must engage in a lengthy back and forth, costing valuable time in an investigation.

We have seen some service providers implement online portals that are designed to facilitate the requests from law enforcement. These portals have been helpful in terms of improving timeliness and security of data that—exchanged between both parties. The response time is anywhere from 1 month to 1 day. This lag can ultimately be dangerous to the cases we investigate.

Most tech companies routinely provide law enforcement information when they really need—in an emergency. But determining the exigent is actually in the hands of tech companies. As a matter of Federal law, we in law enforcement have the most relevant facts and content to determine exigency, but yet the companies are the ones who have the final say.

In one example, an individual made comments regarding being excited about July the 9th, and wanting to do what Nikolas Cruz did. Cruz was the murderer who took 17 innocent lives and injured 17 others at Marjory Stoneman Douglas High School, Parkland, Florida, in 2018. This individual's social media post had indicated they idolized Nikolas Cruz, and appeared to have visited the location where Cruz was arrested. Upon review of this information law enforcement provided the social media provider when asking relevant information about the user, the company unilaterally made a determination that they did not think the situation was an immediate threat at this time.

Big Tech platforms create—Big Tech platforms have created—have transformed society in many ways for the better. Others less so. Users of these platforms should expect that law enforcement officers charged with protecting them have a clear path to the evidence they need to punish the guilty and exonerate the innocent. The establishment of regulatory framework includes standardized legal processes, guidelines, and address the issues that would benefit industry, law enforcement and, most importantly, the citizens we serve (sic).

Thank you again for your invitation, and I look forward to your questions.

[The prepared statement of Mr. Duffey follows:]

Statement for the Record by Mike Duffey

Assistant Special Agent in Charge

Florida Department of Law Enforcement

Before the Subcommittee on Consumer Protection and Commerce

Committee on Energy and Commerce

United States House of Representatives

“Holding Big Tech Accountable: Legislation to Protect Online Users”

March 1, 2022

Chairwoman Schakowsky, Ranking Member Bilirakis, and members of the Subcommittee, thank you for addressing this topic and for inviting me to provide my perspective. I serve as the Assistant Special Agent in Charge for the Florida Department of Law Enforcement, Cyber High-Tech Crime Unit. In my 25 years in law enforcement I have witnessed first-hand the revolutionary impact that technology has had on criminal investigations. I started my career during the AOL dial up days, and I’m sure some of you remember the sound your computer made when the modem made the connection.

Since then, law enforcement has had to learn how to properly investigate crimes committed using computers and mobile devices and the challenges that come with identifying evidence that is stored on devices, with the service providers, and in the cloud. In some ways the explosion of digital data means that we can obtain high-quality evidence that helps us solve crimes. In other ways, the rapid proliferation of platforms and data has created challenges that negatively affect our ability to detect and investigate criminal activity.

What I would like to convey to the subcommittee today is that when crimes are committed – both online and in the physical world – technology companies possess a large amount of the essential evidence law enforcement needs to do our job. But the lack of a regulatory framework that enables efficient access to that evidence means that we cannot be as effective at reducing online criminal threats or seeking justice for crime victims.

Social media has become the new “virtual playground” for today’s youth, yet there are very few rules to govern that playground. Kids are able to follow viral “challenges” where they watch their peers consume laundry pods, climb milk crates, and perform blackout challenges to just name some. When you and I were their age, we certainly did some regrettable things, but it wasn’t possible for thousands of people to watch what we did and try to imitate it within hours.

While age restrictions on most social media platforms prevent those younger than thirteen from joining, these rules are easily bypassed with the help of friends and parents. Thus, we see children of all ages

engaging online. While they can learn and play and socialize constructively on these platforms, they can also meet bad actors. We routinely see instances of “sexstortion” where underage children are threatened if they do not provide sexual images of themselves. The resulting self-production of images and video by these children yields content that can live online forever.

My investigative unit at FDLE, just like the thousands of other units like it across local, state, and federal law enforcement, is constantly improving our ability to obtain and analyze digital evidence. We need more resources to support that continuous improvement of our in-house capabilities, but we also need better cooperation – in a transparent and accountable way – from the technology platforms. We would like to see companies move from a reactive stance to a more proactive stance in which they are able to efficiently handle the large and growing volume of law enforcement legal process being served to them.

As the popularity of tech platforms continues to grow, and as new competitive options enter the market every day, those companies struggle to build out content moderation teams and maintain law enforcement outreach teams that are robust enough to handle our growing needs. To be clear, there are instances where some companies have shown a willingness to be more helpful with compliance because they understand their users are vulnerable to serious personal safety and security risks. But we have seen them hold back because they have no clear legal or regulatory framework that levels the playing field and enables them to protect their users’ safety and bring bad actors to justice while avoiding liability or reputational risk.

It is past time for policymakers – together with stakeholders from industry, law enforcement, privacy communities – to generate the rules of the virtual playground and a system for enforcing them.

Most tech companies will insist that they are routinely providing law enforcement information when it is really needed in emergency – or exigent – circumstances. But determination of “exigency” is actually in the hands of the tech companies. We in law enforcement have the most relevant facts and context to determine exigency, yet the companies are the ones who have final say. This presents issues when law enforcement agencies receive complaints of individuals making online statements about causing harm to themselves or others. In one example, an individual made comments online regarding being “excited for July 9th and wanting to do what Nikolas Cruz did.” Cruz was the murderer who took 17 innocent lives and injured 17 others at Marjory Stoneman Douglas High School in Parkland, Florida in 2018. This individual’s social media postings indicated that they idolized Cruz and appeared to have visited the location where Cruz was arrested. Upon review of the information that law enforcement provided to the social media provider when asking for relevant information about the user, the company unilaterally made a determination that that they did not think the situation was an “imminent threat at this time”.

In another example, we received a complaint of a younger male subject who was live-streaming himself discussing how he was going to commit suicide, potentially in front of a live audience. We immediately contacted the service provider after receiving the information in an attempt to determine where the user was located, while also noting that the live stream had appeared to have ended, but the live stream had ended. The content provider was unable to find a record of the streaming event. You can imagine the frustration of our investigators who were trying to prevent the unthinkable while dealing with a

provider who could not even verify that this was occurring on their platform. Thankfully in this particular instance, the subject's mother presented herself in front of the camera, on the individuals page and informed viewers that her son was safe and that she was handling the situation, with the assistance of local law enforcement.

Another ongoing challenge stemming from the lack of a standard framework governing the exchange of legal process between law enforcement and service providers is what we call the "word game" or "guess the magic word." Specifically, unless the terms we use in formal legal process documentation to obtain content from providers match their own unique corporate terms, law enforcement must engage in a lengthy back-and-forth that costs valuable time in an investigation – for example, in an online child sexual abuse investigation. A word that we think describes a specific type of data that we're looking for may be interpreted by the provider as something different, resulting in the provider telling us that they have no information that is responsive to our legal demand. The lack of uniform terminology therefore results in frustrating and dangerous delays in our investigations.

This challenge is compounded in some cases by the lack of a uniform timeframe for service provider response to law enforcement legal demands. Response time to legal process is up to the individual companies, which is in part limited by staffing at the provider, the volume of agencies requesting data, and the time it takes the provider to identify, extract, and return the specific the requesting agencies are seeking.

We are seeing some service providers implement online law enforcement portals that are designed to facilitate legal requests. These portals have been helpful in terms of improving timeliness and enhancing the security of data that is exchanged by both parties. In instances where there is not a portal companies typically establish an email address for law enforcement to email legal process. In rare instances companies have also identified a specific point of contact who can be reached should the need arise. Believe it or not, we still encounter companies that require legal demands to be faxed to them, and that send any responsive data back to us via fax.

The typical timeline for providers to respond to our legal requests is anywhere from one day to one month or longer. Regardless of whether a law enforcement agency or a judge sets a deadline for response in the legal documentation, the timeline for response is ultimately at discretion of the companies. Again, the lack of a standard legal process, language, or guidelines that govern law enforcement exchange with providers sometimes leads to dangerous delays in our investigations.

Service providers currently have no data retention requirements. In contrast, the banking industry is obligated to keep financial transaction records for a certain period of time. Money launderers and those conducting financial transactions for illegal economic activity certainly would prefer that information be deleted or removed at their discretion. Yet the tech platforms which – despite companies' efforts – are routinely used to facilitate a vast array of criminal activities are not subject to any retention requirements after a user chooses to delete content. There have been instances where law enforcement has tried to access content days or weeks after discovering that critical evidence might exist, only to find out that the content has been deleted by the provider.

Some of the most traumatic cases we deal with every day involve child sexual abuse material (CSAM). Service providers that identify illegal content such as CSAM on their platforms report this content to our vital partners at the National Center for Missing and Exploited Children (NCMEC), which is required by federal law. Providers retain that content until such time when law enforcement begins an investigation into these leads. Typically, the investigation begins with an agency serving legal process to a company for internet protocol information in an effort to identify a location where the activity was occurring. In most cases, this information is obtained with a subpoena because all the elements of probable cause have not been established. Further complicating these situations is that illegal content is often posted to individuals' accounts without the provider or individual (hacked account) detecting it. In these instances, if law enforcement were to execute a search warrant at the residence of the account owner without knowing all the other relevant information such as login data, we could be executing a search warrant at the wrong location, due to someone else having posted the content after compromising the individual's account.

Each of these scenarios – which all levels of law enforcement encounter frequently – illustrate challenges that get in the way of our ability to protect the public and seek justice. The platforms that Big Tech has created have transformed society in many ways, some for the better, others less so. Users of these platforms should expect that the law enforcement officers charged with protecting them have a clear path to the evidence that they need to punish the guilty and exonerate the innocent. The establishment of a regulatory framework, including standardize legal process or guidelines that address these issues would benefit industry, law enforcement, and most importantly the citizens that we serve.

Thank you again for your invitation, and I look forward to your questions.

Ms. SCHAKOWSKY. Thank you.

And now, Mr. Nkonde, I welcome you for 5 minutes for your testimony.

STATEMENT OF MUTALE NKONDE

Ms. NKONDE. Good morning, Chair Schakowsky, Ranking Member Bilirakis—

Ms. SCHAKOWSKY. Oh, Ms. I am sorry.

Ms. NKONDE. No problem. And Ranking Member McMorris Rodgers, my name is Mutale Nkonde, and I am the founder and executive director of AI for the People, a national non-profit that uses strategic communications to really insert conversations around the impact that technology is having on society into public life.

I am here today in support of the Algorithmic Accountability Act that I have been working on, really, for the last 5 years, as an advocate, and something that I am happy that this committee is finally looking for.

As a storyteller, the best way for me to really express the impact that machine learning protocols have on public life is through an illustration. So this committee is very aware of the dangers of social media and algorithmic decisionmaking, so I am not going to go long, but I think that this will be illustrative in terms of the need for this Act.

In February 2022, Twitter users noticed that they were being shown ads from a company called OpenSea. OpenSea is a provider of NFTs or non-fungible tokens, which are parts of currency based in blockchain that can be traded. What these users were being offered were the ability to buy what were described as Meta Slaves. These were avatars of African American people that were put up for sale in the same way that people were as sold in times of enslavement during this country.

Upon AI for the People contacting Twitter to say that this had happened, we found that the account had been taken down from the platform. But news reports found that, instead of removing that lot, what OpenSea actually did was just add Asians and other non-White Americans to their platform.

How did those slaves get onto those social media sites? Through a process called machine learning that informs our algorithmic decisionmakers and decides who and what people get to see on their social media feeds. This is an example of the way the combination of targeted advertising online, racial animus toward non-White Americans, and machine learning conflates to create unsafe online environments for Black and other—Black people and other members of protected classes.

The Algorithmic Accountability Act is important, because what that would do would be to introduce impact assessments so that an office within the FTC could look at this potential use case, and then decide. Is this in the national best interest? I would argue that it is not, because we know, from the investigation conducted by Special Counsel Robert Mueller, one of the tactics of hostile nations such as Russia is to really incite racial divides and therefore, I would argue, undermine our national security as we divide

against ourselves, instead of looking outward to protecting this great nation.

I argue that the Algorithmic Accountability Act, and even its what I would consider in many ways to be companion legislation, the Surveillance Advertising Act, provide an online environment in which people from protected classes can be safe.

AI for the People, as an organization, really does seek to highlight the numerous ways in which advanced technological systems—and as we are looking to things like the Metaverse, Web3, and NFTs, technologies that we are not really commonly speaking about, we need to keep the protection of civil rights in mind. These platforms are enriching the few, without thinking about the ways in which they comply with laws that we have already standing.

And as I finish my remarks, because of intellectual property laws—excuse the background noise. I sit—I come to you from Brooklyn, New York. Unfortunately, this is a noisy part of the country, so it won't be long.

But the one thing I will say is, because of international—intellectual property laws, researchers and advocates do not have the ability to look at the source code to understand how these decisions are being made. So the passage of the Algorithmic Accountability Act will not only safeguard those of us from protected classes, but also give us insight into how these technologies make decisions that really have incredible impacts on the lives of many Americans.

I look forward to the discussion. I thank you for the invitation, and I yield my time.

[The prepared statement of Ms. Nkonde follows:]



Good Morning Chair Pallone and Subcommittee Chair Schakowsky.

My name is Mutale Nkonde, I am the Founder and Executive Director of AI for the People, a national nonprofit that uses strategic communications to help journalists, filmmakers and television producers add a technical analysis to social justice discourse. My background is in journalism and I started my tech career in 2011, when I worked opposite Google's External Affairs Team to help them embed a non profits focused on bringing coding education to children within urban school districts into their New York office.

Since then I have moved into research and held fellowships at the Berkman Klein Center of Internet and Society at Harvard, the Digital Civil Society Lab at Stanford and the Institute of Advanced Study at Notre Dame. In 2019 I started AI for the People based on the work I have been doing for the last decade. And I am currently studying how algorithmic systems impact Black people at Columbia University. AI for the people conducts research, publishes reports and creates content based that highlights the impact algorithmic systems have on Black communities.

Our latest film [Blackness Unbound](#) discusses how the themes of Afrofuturism, (a theoretical cannon that challenges people to imagine the state of Black people in America if they were unencumbered by the legacies of enslavement) could be used to develop anti-racist engineering practices. This film was submitted to the Smithsonian Museum of Air and Space on January 27, 2022 has been accepted to the HBO Shorts Category of the Martha's Vineyard African American Film Festival and is traveling through the film festival circuit. In 2020 we developed a social media campaign targeted at African Americans in swing states being encouraged not to vote in the US Presidential election. Our efforts were supported by celebrities like Quest Love from the Philadelphia based group The Roots and encouraged African Americans to vote for representatives that would help bring the COVID pandemic to an end. Our campaign #VoteDownCOVID received more online engagement than the "no vote" campaign and started working with local journalists working in Black serving newsrooms. In 2021 The Congressional Black Caucus took note of our efforts and Representative Stacy Plaskett warned against online voter suppression in a video played during the CBC Policy weekend in September, watch the video [here](#).

Further to this, I sit on the Tik Tok content moderation board in my personal capacity and consult regularly with teams at Twitter, Google and FitBit seeking to ensure their products do not have a negative impact on Black Americans. In 2019 I was a co-author of [Advancing Racial Literacy in Tech](#), a report published by the research institute Data and Society that pointed out how the rules governing machine learning lead to AI systems making racist determinations.



Machine learning protocols rely on the use of historical data to predict what will happen in the present. The predictions made by these algorithmic actors then create a feedback loop that changes the course of society. For example, social media platforms use recommendation algorithms to predict the type of content we will retweet, share or comment on, a process referred to as engagement. The fact advertisers can use social media recommendation algorithms to reach their target audience makes them an extension of the market square. This is resulting in social platforms being used to spread divisive and racist content by bad actors who use targeted advertising to recruit people who engage in this type of content.

For example the website [Open Sea](#) came under fire in February 2022, when Twitter users noticed it was promoting the sale of Black people on its NFT site. NFT's are non fungible tokens, which are units of data stored on a blockchain, that can be sold and traded. These Black NFT's were called **Metaselves** and part of a group of 1865 NFTs offered to the site's users. The number 1865 is a reference to the 13th amendment that was passed that year to abolish slavery. And Open Seas's refusal to take this down, but instead add Asian and other non white avatars to the lot speaks to the underlying racist sentiment of people who buy these tokens. This is just one egregious example of how algorithmic actors can be used to promote division among the American people, and while a meta slave has no utility it works to divide Americans against each other on the basis of race. A tactic of Special Counsel [Robert Mueller](#) uncovered during his investigation of the Russian Internet Agency during the 2020 election. This is a form of voter suppression, facilitated by algorithmic advertising.

This use of algorithmic actors to undermine the rights of people from protected classes goes beyond social media and includes but is not limited to facial recognition that is being discussed during this hearing. I am happy to discuss facial recognition in more depth during questioning, but for the interests of time will continue in this vein. The harm algorithmic actors have on all members of the protected classes is why we need the passage of the Algorithmic Accountability Act. Not only does it create an agency of the FTC who can protect the rights of online consumers but it raises the larger question of whether we are users or consumers of algorithmically driven systems as they are used in every element of public life.



Lastly, oversight is impossible, unless a good faith public sector actor has the right to examine how machine learning systems make their determinations. Current intellectual property laws means researchers do not have the right to examine the underlying source code, instead we are forced to make note of patterns in AI decision making to determine how it impacts people from protected classes this has to stop. We would not consider releasing food or medications into the market place without first making sure they are safe for human consumption and the broad use of algorithmic systems in public life means they should face the same level of scrutiny. Machine learning systems are here to stay and so congress needs to pass legislation to ensure our AI systems work for the People and not just enrich the few.

Thank you for allowing me to be part of this hearing. I look forward to the pending discussion.

Ms. SCHAKOWSKY. Thank you, Ms. Nkonde, and we have now concluded our witnesses' opening statements. At this time we will move to member questions.

Each member will have 5 minutes to ask questions of our witnesses.

I want to thank our witnesses for being here today.

And since we have witnesses appearing virtually, I need to ask my colleagues in the hearing room to mute themselves whenever they are not directing—directly speaking during their Q&A portion, so that we can clearly hear the witnesses' remarks.

I will begin with my 5 minutes of questions.

So targeted advertising is at the heart of the online consumer model—online business model. But it fundamentally violates users' privacy in a way that would never be accepted if consumers were actually given the choice. That is why I joined Representative Eshoo in introducing the Banning Surveillance Advertising Act, and this legislation prohibits companies from targeting advertising—advertisement based on personal information.

So, Ms. McInnis, your company already bans targeting—targeted advertising. Can you tell us why you made this decision?

Ms. MCINNIS. Thank you for the question, Chair. Our founder and CEO started out DuckDuckGo by wanting to serve answers—serve users with great instant answers at the top of the search engine results page. And he was really looking for his company to have a positive impact. As he was developing this company in 2008, he saw that there was a clear need for private search engines. And so we developed privacy for the search engine, have been expanding our privacy options ever since.

And thank you for noting that DuckDuckGo helps stem surveillance ads. We are working very hard to ensure that our users are protected as they do whatever they need to do online by blocking trackers in the first instance, so that information is not collected about them.

Ms. SCHAKOWSKY. And is your business still profitable, without the use of targeted advertising?

Ms. MCINNIS. Yes, we are very profitable. Our revenue is somewhere around 100 million per year. We have over 30 million U.S. users in the United States, and they span the whole nation and the political spectrum.

Ms. SCHAKOWSKY. Thank you. When you were asking whether people get frustrated when they see that there is an ad that pops up, you know, "How did they know to target me?" And people feel uncomfortable online because of that.

In our last tech hearing we discussed the impact of whistleblowers protection at the Federal Trade Commission. I am so glad to see that provisions in Mrs. Trahan's bill to protect whistleblowers, similar to those in the FTC—in the FTC Whistleblower Act that she and I have introduced in November.

So I wanted to ask Ms. Lehman, would consumers be better protected from online harm if the FTC whistleblowers were protected by Federal law?

Ms. LEHMAN. Thank you, Chair Schakowsky. Absolutely, yes.

We are excited about a number of the transparency provisions before us today. There is context that—as many transparency re-

ports as we have, as much nuance as we can get into, as much research as we do, there is context that you could only ever get when someone can tell you why a decision was made. And so for that reason, whistleblowers are critical to providing that context for consumers.

Ms. SCHAKOWSKY. I really don't have any more questions, except to say that we are going to move along as fast as we can to protect consumers from the harms that are out there, from the information that they don't want collected, and we want to do it in these—the bills that are introduced today that we are discussing, but also to move quickly, and efficiently, and, very hopefully, in a bipartisan way to do comprehensive privacy legislation.

The time to regulate is now. The time to hold Big Tech accountable is now. We have heard over and over again the promises, the denials of wrongdoing that we have heard from Big Tech and, really, enough is enough. Consumers want to be able to safely and confidently use what they can online, and not be exploited as they have been.

So I yield back, and now will—Mr. Bilirakis for his 5 minutes of questions.

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

Mr. Duffey, I thank you again for your testimony. Again, we appreciate the valuable insight you bring to this discussion.

I don't know if he can hear me.

But Mr. Duffey, we were having a little difficulty hearing you before, in your opening remarks. So hopefully we have—you know, we have fixed that. I don't know, maybe you need to speak into the microphone. You know, your information is so valuable, so we want to catch everything.

So anyway, I have a question for you. I am gravely concerned about the crimes perpetrated on Big Tech platforms, such as the sale of deadly fentanyl on Snapchat. And I believe companies are not doing enough to help solve these crimes. I mean, enough is enough, as the chairman said. Not—again, we can't allow this to happen anymore. Kids are dying, for crying out loud.

And so in fact, in our subcommittee, the Health Subcommittee, we had—again, we had somebody testify on the fentanyl crisis in December. And Chairman Eshoo agreed with my assessment that Big Tech companies aren't doing enough to coordinate the DEA on drug sales, in particular.

OK, that is why I recently introduced the CAPTURE Act, which will help us to develop legislation to assist social media companies to better communicate with law enforcement, specifically in relation to events of imminent injury or death to individuals.

So from your experience, sir—and I appreciate you testifying and, again, you are doing a great job in our state—so from your experience, how has Big Tech failed at cooperating with law enforcement to assist in solving these dangerous crimes? And I would like for you to elaborate, sir.

Mr. DUFFEY. Thank you, Representative. Can you hear me better now?

Mr. BILIRAKIS. Yes, we can.

Mr. DUFFEY. OK—

Mr. BILIRAKIS. Madam Chair, can we hear better? Yes, I think so. Thank you. I can. Thank you.

Mr. DUFFEY. OK. So they have failed in the sense that I don't think what we see is some of the—they don't understand the trends that today's youth is communicating by on their platforms. The data retention, when we do——

[Audio malfunction.]

Mr. DUFFEY [continuing]. Investigation, is an issue, and—is what they do and what they don't keep, and for how long they keep it.

The content moderation, they build—what we have seen is a lot of these companies build a platform for one type of use, and then, as you explained, it gets used and abused for other areas.

So I think the failure is the lack of communication in—between Big Tech and law enforcement to discuss the trends, to discuss the acronyms, and the use of emojis, and the different codes by which today's youth communicate.

Mr. BILIRAKIS. Yes, sir, when you speak slower, we can hear a lot better, so let's try that.

Ms. SCHAKOWSKY. And stay real close to the mike.

Mr. BILIRAKIS. Yes, and stay close to the mike. All right, we really appreciate it.

What more can Big Tech do, in your opinion, do you believe—again, this legislation that I filed, the CAPTURE Act—can help accomplish this?

And then also, as I mentioned in my testimony, we invited TikTok to testify at today's hearing to answer how they have failed to protect our youth online. They again ignored our requests. OK, we are not going to give up, we are going to have them here, and they are going to have to answer our questions. I know the Chair agrees with me. She is the leader in this area. It is clear they are not investing the time or resources needed to adequately curb dangerous content on their platform.

Are you familiar with the dangerous viral changes that populate the site, and how schools are scrambling to stay ahead of the harms to other students and teachers alike?

If so, can you elaborate on how this has stretched the resources?

And again, the teachers, the police officers, we can't do—they can't do it all. They need our help. So it has stretched the resources for Florida police, I know. If you can elaborate on that, I would appreciate it.

Mr. DUFFEY. Thank you, Representative. I agree with you 100 percent. The resources that we in law enforcement have for identification of these viral challenges is, a lot of times, brought to our attention by parents or school resources officers who are within the school system, who are listening to the kids, watching their activity, and hearing firsthand——

[Audio malfunction.]

Mr. DUFFEY. As you mentioned, we don't have——

[Audio malfunction.]

Mr. DUFFEY. We are left to prioritize the different types of leads which we can investigate properly, and then identify the ones that we can——

[Audio malfunction.]

Mr. BILIRAKIS. Thank you. I appreciate it. I yield back, Madam Chair. Hopefully, we can get this cleared up and straightened out, because I know a lot of members here, at least on my side, want to talk to Mr. Duffey, and get valuable information from him.

So thank you, I appreciate it.

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

Mr. PALLONE. Thank you, Chair. And we are here today, as we know, to have an open, meaningful dialog about solutions to address the harm social media companies have caused, and this is more timely than ever as we see social media companies expanding their reach.

So I want to use Facebook as an example, which now goes by Meta. We have seen reports of sexual assault and harassment in the virtual reality world that Facebook is trying to create with the Metaverse. So let me start with Ms. Nkonde.

Can you expand on this issue? What are some of the real harms that we will see as social media companies expand their reach, if you will?

Ms. NKONDE. Thank you for the question, Mr. Pallone. The issue—just to read everybody in to the issue with the Metaverse as it stands, the head of research of the Metaverse recently wrote a [inaudible] article, in which she told us that when she went in, she was sexually abused by male avatars.

The issue is, in order to get this immersive experience, what the Meta are currently doing, what their team is doing are investigating how to use light sensors to make it feel like we are seeing, audio sensors to make it feel like we are hearing, and tactile sensors to make it feel like we are being touched.

Therefore, if you go into an immersive environment where you really feel that these things are happening to you, then, despite the fact that it is in a headset, you are still going to have that very real experience of abuse. And without regulation of what is called Web2, what we know of Facebook, these harms are going to be perpetrated further in the virtual environments.

Mr. PALLONE. And what about—well, let me ask about marginalized communities. How might they be impacted by these changes that we are seeing?

Ms. NKONDE. Marginalized communities are actually the most vulnerable within this.

And so the head of Metaverse research is a woman. She is a protected class. So what we were seeing in her attack by male avatars were really the logics of sexism and hatred of women being enforced in a place where you can reach your target.

Another group that we are seeing more reports of are children in the Metaverse, which is a whole explosion of issues, specifically because people under 13 are not even supposed to be on that platform. And so, when we think about regulation, we need to think about who are the most vulnerable. Could disabled avatar got away in those situations. There is a history of racial violence in this country. If we see attacks on women, it is logical that we are going to see attacks on negatively racialized groups.

And it is committees like this and the bills that are being put forward that are really going to keep us American people safe.

Mr. PALLONE. [Inaudible] instances. I mean, I think increased transparency would go a long way in making the internet a safer place, so let me ask Ms. Lehman.

How would the legislation before us today bring greater transparency, and with a greater accountability, to these Big Tech platforms, if you will?

Ms. LEHMAN. Thank you, Chair Pallone. So the transparency in the bill across the board today is a crucial prerequisite to really understanding and forming the kinds of harms we are seeing across the board, and being able to have that kind of context, being able to speak to the specific harms.

And so the bills before us today, particularly Representative Clarke and Representative Trahan's bills, are—in requiring impact assessments, for example, and requiring—it requires companies to actually take account for what kinds of harms, what kinds of risks do we need to consider, do we need to think about, rather than building first and asking questions later, once the harms have happened.

And I will yield back.

Mr. PALLONE. I only have a little time left, but let me just say we have consistently seen some social media companies withhold critical information about how their systems work from the public, which makes it difficult for consumer protection agencies like the FTC to address the issues users face online.

Could you tell me, Ms. Lehman, how would these bills help the FTC better protect consumers from unfair or deceptive practices? But you only got 20 seconds.

Ms. LEHMAN. Thank you, I will try. The short answer is it helps inform how we do it.

Eight seconds? Boy.

It offers so much more perspective to the FTC to understand the problems and, therefore, to keep consumers safe in sort of the mission.

[Inaudible] seconds, OK.

Mr. PALLONE. I made you go too fast. Thank you.

Ms. LEHMAN. Thank you.

Mr. PALLONE. Thank you, Madam Chair.

Ms. SCHAKOWSKY. The gentleman yields back. Let me just remind everyone in the room, all members, to please unmute after you have spoken. Apparently, we are getting some feedback here.

I am sorry?

VOICE. They have to mute their mic after they have spoken.

Ms. SCHAKOWSKY. Yes, to mute your mic after you have spoken.

And now I recognize the ranking member of the full committee, Mrs. Rodgers, for 5 minutes.

Mrs. RODGERS. Thank you, Madam Chair. There certainly is a lot before us in this hearing, and I appreciate the attention. The Republicans also have—we have a couple of dozen bills around transparency and accountability.

Clearly, there is action that needs to take place, and we have been working with a variety of stakeholders getting input. I know that, in committee, there is 35 bills that have received a legislative hearing in the subcommittee. Three have been marked up, and two have received the bipartisan support.

I really believe—and what I want to make the request of—is that we work together, that this is a problem that is going to require us seeking input and support from a lot of different entities, Republicans and Democrats.

But beyond that, I believe that we need to be hearing from the advertising industry, AI developers, small businesses, even the FTC, for that matter, on how this is going to work, how they are going to operate after this—what you might call an extreme makeover, FTC addition.

And I fundamentally believe that we need to be addressing a privacy law. We need a national privacy framework in order to gird up what the whole space is right now. And so we have drafted legislation, and are anxious to work with our colleagues across the aisle on a privacy standard. Certainly, there is an opportunity to find some common ground.

On some of the issues before us today, I wanted to start with Ms. McInnis. Given recent reports on Big Tech needing to do more to protect the people of Ukraine from the misinformation campaigns generated by the Kremlin and its still-active Twitter account, I have a couple of questions to give you an opportunity to reflect on DuckDuckGo's part in this debate.

Does your company still maintain a partnership with the Russian search engine Yandex?

Ms. MCINNIS. In light of Russia's assault on democracy in Ukraine, we have paused our relationship with Yandex.

Mrs. RODGERS. Thank you—

Ms. MCINNIS. Yandex was used to provide traditional links, meaning non-news links on the search engine results page, in Russia and Turkey.

Mrs. RODGERS. Thank you. Given you raise revenue via contextual advertising and affiliated programs, are you able to say whether such revenue has ever come from Russian State media sources in this partnership?

Ms. MCINNIS. I do not know. Our advertisements are provided through Bing's contextual ads program. And so Microsoft's advertising would have the best information about that.

That said, we are—yes, I think that they would be the best ones.

Mrs. RODGERS. OK, thank you. Do you—or how do you see we best address concerns that we have over Chinese-owned TikTok, and how it may be influenced by Russia via its alliance with China?

Ms. MCINNIS. Thank you, Ranking Member. Ranking Member Bilirakis and Ranking Member McMorris Rodgers, you have talked extensively about the need to protect children online.

Although we have that Children's Online Privacy Protection Act, banning the use of surveillance ads would, I think, help protect children by banning the collection of personal information, no matter their age, which I think would help solve for some of the issues that we have been seeing online, where dominant tech companies say, "We are not sure if children are on our platform, we don't actually know that they are there." And so, if we are protecting everyone, we are protecting children more.

In addition, I think having some privacy laws like the general one you mentioned, or the Banning Surveillance Advertising bill,

which would—of course, would protect privacy—would stem the ability of platforms like TikTok to collect information, regardless.

Mrs. RODGERS. OK. Well, I thank you, and I appreciate your engagement and your support on the legislation. Fundamentally, we need a privacy framework, and so we will continue to work on that.

Officer Duffey, our law enforcement officers are American heroes, and I have personally heard some very sad tales of the role Big Tech played in tragic events impacting our children, and the pressures on first responders. In your—you reference a—exigent circumstances in suicide intervention. Can you elaborate on the subjective constraints that social media platforms put on law enforcement to intervene in harm to children?

And can you give us a sense which social media companies do a better job in cooperating?

Mr. DUFFEY. Thank you, Representative. Hopefully, we have corrected some of the audio issues.

But the

[inaudible] exigent, when we serve a company with exigent circumstances, it is left at their determination. We present them with the facts as we are given. Ultimately, each individual company is the final say-so on whether they determine there is a threat to a person's life or others—

Mrs. RODGERS. And which companies are cooperating?

Mr. DUFFEY. It varies. The last one that I referenced in my statement was TikTok.

Mrs. RODGERS. OK. OK, thank you. I have run out of time. I yield back.

Ms. SCHAKOWSKY. OK. Who is next?

My colleague from the Chicago area, Congressman Bobby Rush, you are recognized for 5 minutes.

Mr. RUSH. Well, thank you, Madam Chairman, for this magnificent hearing. My question is directed to Ms. Nkonde.

Ms. Nkonde, you mentioned facial recognition in your testimony. The error-prone nature of facial recognition software, especially when it comes to identifying people of color and women, is extremely dangerous.

In 2018 an ACLU study found that Amazon's facial recognition software falsely matched 28 Members of Congress, including me, with someone else's mug shot. We are seeing the real-world impact of this when, in June 2020, New York—the New York Times reported on the case of Robert Julian-Borchak Williams of Michigan, who was arrested by Detroit police because he was misidentified by facial recognition software. Later it was revealed that this software was used “almost exclusively against Black people” and was used even though the Detroit police chief estimated that it misidentified individuals 96 percent of the time. Clearly, this is a very serious problem with very, very serious and very real implications.

Ms. Nkonde, can you please speak to the role algorithms play in these kinds of situations?

Does the solution to this problem currently exist?

If so, what needs to be done to implement them?

And if not, what do we need to do, as Members of Congress, to address these problems?

Ms. NKONDE. Thank you for the question, Representative Rush. Big questions. But yes.

So the way facial recognition works is through a computer engineering protocol called computer vision. The training data are pictures of people's faces, and then the algorithm will take a face graph. So it basically measures your face in what we call facial architecture: color of the skin, broadness of the nose, circumference of the eyes, for example.

The issue within the Gender Shades report, which kind of undergirded this idea that facial recognition technology did not work in the Amazon, Microsoft, and IBM report, found that the training data was using that of White men, which meant that when those same systems were used to identify non-White people like Mr. Williams, who you mentioned, it misidentifies us.

Therefore, one of the things that Congress could do immediately is really take the Algorithmic Accountability Act to markup. Because through impact assessments, the FTC would be then able to figure out how—what is the efficacy of this technology? Is it recognizing Black and Brown people? Where is facial recognition being used?

Because many Americans believe it is just in law enforcement, but they don't realize that when we use self-checkout, for example, in pharmacies, they are using facial recognition to figure out whether you have stolen toothpaste or not, whether—

Mr. RUSH. Ms. Nkonde, can you also include how it affects us African Americans in the area of criminal justice and banking?

Ms. NKONDE. Yes. In the area of criminal justice, misidentification leads to misincarceration or arrest. And in the area of banking or finances, the IRS has just been stopped from using facial recognition in order to access our records. And if you imagine that African Americans are not being recognized, that would bar us from access to our own financial information.

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

Ms. SCHAKOWSKY. Thank you, Mr. Rush.

Mr. Upton, you are recognized for 5 minutes for questions.

Mr. UPTON. Well, thank you, Madam Chair, and I want to echo the remarks of Cathy McMorris Rodgers. I hope that we can develop a privacy standard. It is something that is bipartisan, it is long overdue. I know it is tough to do, but I think we need to proceed down that road.

For me, I am a dad, and I am also a granddad, so I sort of like that Duck Duck Goose at the beginning.

[Laughter.]

Mr. UPTON. I know where you were coming from, I think.

But all of us want to protect the most vulnerable, and that is our kids and our grandkids. We want to make sure that there is every tool in that toolbox so that we know what is going on, and their lives can be protected, because it is no longer just don't talk to strangers. There is a lot of strangers that are out there. And that is why we need to make sure that those tools are there.

And so, Mr. Duffey, I want to thank you for your service, for coming before this committee to help us understand the ins and outs of protecting our Nation's kids online. One of the concerns that I hear about most from my constituents—and there is a lot of

them—is the way that Big Tech is impacting the mental health of our kids.

So I just wonder if you can walk us through a step by step of how you interact with a tech company, and how does that change when there is a threat to a child that is viewed as urgent?

And I would just recommend that you get as close to your mike as you can, because the—despite this being the high tech community, the connection is not all that great.

Mr. DUFFEY. Thank you, Representative. I am getting as close as I can, so hopefully this audio sounds a little bit better.

Mr. UPTON. I knew it wasn't the Florida accent, I can understand that better than Louisiana.

Mr. DUFFEY. Thank you. So really, that relationship with big technology is only engaged upon an incident occurring. In the case of a missing child, or the case of child sexual abuse material, or a threat of violence, or an act of harm, we begin that engagement with technology.

Outside of that, other than some of the big technology companies, the startups and a lot of the newer companies, we have very little engagement with them. Typically, our engagement, when it begins, is through legal process as we begin to try to investigate the issue at hand.

Mr. UPTON. What is the value of the number of cases that your department looks at every year, and has it been increasing? What is—what has been the trend line?

Mr. DUFFEY. It has been increasing. Specifically as it relates to the child sexual abuse material, we hear in the State of Florida alone—law enforcement as a whole in the State of Florida has received over 18,000 leads reported to us by the National Center for Missing and Exploited Children alone in 2020. That means law enforcement has to put eyes on each one of those leads to determine the ability to investigate

[inaudible] limited resources.

Mr. UPTON. And where was that number—where were you, say, 10 years ago, or when you started? I know you have been with law enforcement for a while. But as I hear from my law enforcement folks, I mean, they just—they shake their head in terms of some of the doors that get opened, and some of the nasty stuff that really gets out there. How has that changed from when you started?

Mr. DUFFEY. Well, exactly. When I started the—it was a—a lot of what—the work we did was through the U.S. Postal Service, because the online world didn't exist. And the online world that existed was not as widely popular as it is today. So we are seeing exponential increases as companies come online and today's youth and others begin to leverage this platform to communicate, which ultimately results in children being sexually abused online, sextorted, and

[inaudible] their mental health.

Mr. UPTON. Can you tell us one particular story of where things worked out?

Mr. DUFFEY. There has been a few where we have gotten incidences of somebody saying, "I am watching a child being sexually abused" or a child was abducted and, through the use of technology, we were able to work with the provider to determine the

location where that child or individual might be. And through the use of technology, we were able to locate that individual to prevent further abuse, or recover

[inaudible].

Mr. UPTON. And are you able to interact that with Amber Alert?

Mr. DUFFEY. We very much so are.

Mr. UPTON. Well, thank you. Again, thank you for your service. I appreciate the hearing, and I yield back.

Ms. SCHAKOWSKY. I wanted to point out that there was much more clarity with the response of our online witness because you turned off your mic each time after you asked the question. And I would recommend that for everyone who is asking questions of our online witnesses.

The—and next, Ms. Castor, I recognize you for 5 minutes for questions.

Ms. CASTOR. Well, thank you, Chair Schakowsky, for holding this hearing, and thank you to all of our witnesses for appearing today, and a special shout-out to Special Agent Mike Duffey from the Florida Department of Law Enforcement.

Thank you, Special Agent Duffey, for your 25 years of service, and especially on behalf of crimes against children and online harm.

The subcommittee has now held several hearings on legislation to hold Big Tech accountable, and the bills before us today by Rep. Trahan and Rep. Eshoo, and Rep. Clarke are steps in the right direction. But I believe it is urgent that we move legislation on online privacy issues, especially when it comes to children.

Passing a core comprehensive privacy bill is central to holding Big Tech accountable. And if we can adopt safeguards on processing personal information, tech platforms will have less of an incentive to use many of their manipulative and harmful techniques that are currently deployed to increase engagement and addict their users, many of which we have discussed in past hearings.

So one of our witnesses—witness companies today, DuckDuckGo, is a good example of this principle.

And with the online harm to kids being made plain over the past few years, I work—I have been working for a number of years to develop the Kids Privacy Act to provide parents the necessary tools to protect their children, strengthen enforcement so companies are held to account for improperly collecting children's personal data, and for misuse of that data. It also closes loopholes. It has—the bill has widespread support. It has been endorsed by the leading child protection organizations, parents, pediatricians, and privacy groups.

So to my Republican friends, we really need bipartisan support on this effort. The UK is ahead of us. The EU is ahead of us. And even the U.S. Senate, they are ahead of the House when it comes to children's online privacy. They are now two bipartisan bills over there. And while we all know that the Senate is not known for action, they are ahead of us here. So if they can come up with a bipartisan bill, so can we.

So I am really speaking out more as a mother than as a Member of Congress. I have really—I have reached out to the leadership, and I am doing so again because I am not going to give up. I am—

my door is open to any Member of Congress who wants to enter into good faith negotiations over a bill that protects children's privacy, their safety, and their health online, especially in the face of everything that we know now about crimes against kids, the rising rates of mental health problems, and more.

I mean, the Facebook whistleblower was here—also made plain that the Big Tech platforms, Facebook, Instagram, they know about the harms, but they are more interested in getting kids hooked and their profits than keeping kids safe online.

So thank you for indulging me on that. But please, my door is open, and we really want to protect kids.

So my question for the witnesses today, each one of you, yes or no, is a comprehensive Federal privacy law a critical component of Big Tech accountability and protecting consumers online?

Ms. Lehman, you can start.

Ms. LEHMAN. Yes.

Ms. CASTOR. Ms. McInnis?

Ms. MCINNIS. Absolutely.

Ms. CASTOR. Special Agent Duffey?

Mr. DUFFEY. Yes.

Ms. CASTOR. And Ms. Nkonde?

Ms. NKONDE. Yes.

Ms. CASTOR. And here is another yes-or-no. Should there be special focus on protecting children's privacy, safety, and health online, yes or no?

Ms. LEHMAN. Yes.

Ms. MCINNIS. Yes.

Mr. DUFFEY. Yes.

Ms. NKONDE. Yes.

Ms. CASTOR. Well, thank you.

And Special Agent Duffey, you—Representative Upton asked you about a good news story, but tell us what you are seeing right now because of the—just the widespread collection of data on children and their interaction with online apps? What tools do parents need? What do parents tell you right now that they feel they need from policymakers here in Washington?

[Pause.]

Ms. CASTOR. Oh, Special Agent Duffey, your audio.

Mr. DUFFEY. Sorry about that. Representative, thank you.

Being a parent myself, and talking with other parents, the biggest issue we hear is that they don't understand how to implement parental controls. A lot of these companies implement the process. The explanation of how to do it is not clear.

Ms. CASTOR. Thank you very much. It is obvious that we need to rebalance the power here, and put the power in the hands of parents, and not these Big Tech platforms.

Thank you. I yield back.

Ms. SCHAKOWSKY. Thank you.

Mr. Latta, you are recognized for 5 minutes.

Mr. LATTA. Well, I thank my friend, the Chair, for today's hearing, and I also thank our witnesses for appearing before us today.

As part of the Republican Big Tech accountability platform, many of the Members in this body have proposed a number of reforms to the laws governing Big Tech. My proposal is to remove

section 230 liability protections from companies that act as bad Samaritans and knowingly promote, solicit, or facilitate illegal activity.

Broadly, I have serious concerns about some of the activities that these companies are allowing to occur on their platforms, whether it is explicitly permitting these questionable activities or simply ignoring any illegal content that they discover.

I believe the legislation before us today misses the mark. H.R. 6796 would create a new bureau at the Federal Trade Commission with new rulemaking and investigatory authorities to define the code of conduct for online platforms. However, I do not believe it is the FTC's duty or responsibility to be the moderators of content on social media platforms. Rather, they should act as the clearinghouse and inform consumers on Big Tech's content moderation practices, including their enforcement decisions and appeals decisions.

Additionally, the legislation would require the FTC to hire 500 staffers. I can only imagine this undertaking would set back the FTC many years and further slow its rulemaking drafting process and its ability to protect consumers.

Sadly, we aren't able to explore these concerns, as the majority did not invite the FTC to testify today. Fortunately, we do have the opportunity to hear from Mr. Duffey, a career law enforcer who has dedicated his career to protecting Americans from predators in the real world, and is now working to protect Americans, especially children, from predators online.

And Mr. Duffey, if I could begin my questions with you, in your testimony it sounds like there were many instances of you being reliant on the goodwill of these tech companies to fully complete your law enforcement investigations. Would you speak about your conversations with these companies, and how would you characterize their concern for what is happening on their platforms?

Mr. DUFFEY. Thank you, Representative.

With regards to your question, the conversation is, sometimes with the newer tech companies, is it a loss. And what I mean by that is they don't understand the pure volume of data which they have, which makes it a challenge for us in law enforcement to ask for the specific information that we are referring to, specifically when we talk about the—what we will call the word game.

When we begin to do our investigation, we serve each and every company with the legal process asking for specific content. If that content language that we are asking for doesn't match up with the exact language that they have, we begin this banter back and forth to try to identify the exact content we are looking for, which is—which—transparency on what they have would be greatly—you know, greatly enhance our abilities to streamline some of our process.

Mr. LATTA. Well, you know, one of the ways we can hold Big Tech accountable is increase the transparency requirements.

You were just talking about transparency. Last year I released a discussion draft to require companies to disclose their content enforcement decisions related to child pornography, child trafficking, cyber bullying, illegal sale of drugs, foreign terrorism content, counterfeit products, revenge porn, and doxing.

Do you believe that if law enforcement had more information about how companies manage or conduct enforcement against these types of activities, would it help you overall perform your job?

Mr. DUFFEY. Yes, I believe it would. It would allow us to have a full understanding. I think it would open that door, and have the conversations with these tech companies that sometimes stand to the side. Having a better understanding by law enforcement would be a win for all.

Mr. LATTA. Well, thank you very much.

And Madam Chair, before I yield back, I do have a letter to the— for the committee from ANA, which I would like to ask unanimous consent to put in the record.

VOICE. We just have to check—

Ms. SCHAKOWSKY. Without objection.

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

Mr. LATTA. Thank you, and I yield back.

Ms. SCHAKOWSKY. Congresswoman Trahan, you are next, recognized for 5 minutes.

Mrs. TRAHAN. Well, thank you, Madam Chair.

Throughout our country's history, bold reforms have been born in moments of crisis. The Great Depression forced Congress to create the Securities and Exchange Commission, tasked with overseeing and regulating the market to protect investors. And almost 80 years later, Congress passed the Dodd-Frank Act in response to the 2008 financial crisis, strengthening consumer protections against financial market abuse and creating transparency and accountability requirements for the entire financial system.

Yet today, crisis after crisis created by large technology platforms have resulted in minimal Federal response. In fact, crickets.

Under the leadership of Republican and Democratic-controlled governments alike, a handful of U.S. companies have become monopolies. They have optimized their platforms solely for ad revenue and, in turn, they have become breeding grounds for the spread of weaponized disinformation, hate speech, and content that harms our children.

These issues have been closely examined. We have held hearings with experts, we have yelled at executives, and we have sent letters all saying the same thing: Do better. Yet the end result has remained the same. Nothing changes. And companies' stock prices hit new highs.

The focus of today's hearing may be on the legislative proposals introduced by myself and my colleagues, but the question is much simpler: How long can we continue this inaction?

How long can we look at our children and say the change is necessary, but we just haven't been able to enact it yet?

Congress has gotten off the sidelines in the past for practically every other industry: cars, airplanes, and banks. We employ key organizations that keep pace with new developments, and inform regulations aimed to protect consumers. We must get off the sidelines once again. Enough listening to companies saying, "Trust us, we have a process for that." Enough internal bickering that ends any real chance of progress. And enough watching Europe go first, and the Senate.

I commend my colleagues on the committee, including our panel's leadership, who recognize that we have everything we need to act: the smoking guns, the historical precedent, and the legislative text. All we need today is the willpower.

So Ms. Lehman, the Digital Services Oversight and Safety Act creates a bureau at the FTC, staffed with experts employed to issue rules related to public-facing transparency reports, certified researchers with data access, and disclosures to the Commission, so that we can shine sunlight on how consumer data is collected and used. Could you please explain why transparency requirements like these are so important?

Ms. LEHMAN. Absolutely, thank you. Transparency requirements, particularly like those in your bill, we have a variety of them, right? So we have users and advertisers and individuals who need to understand what values the platforms that they use operate on. They—so that parents can decide is this platform—are these platforms' values coherent with what I want my kids to be on?

And some of the most exciting components of the bill really are that we have seen time and time again that there is an allergy from the platforms to transparency and to accountability, whether that is Facebook disabling crowd sourcing, or disbanding the CrowdTangle team, whether that is other—we have seen the list that—and so, having access to understand, OK, what kinds of misinformation, how does it spread, how can we fix these problems, we don't have the context for that right now. And the parts of the bill that shine that sunlight make that possible.

Mrs. TRAHAN. Well, thank you. And in your experience, how quickly do social media companies change their products and processes?

And why is it so important to have a bureau that is flexible and nimble enough to quickly publish safety guidelines or issue new rules for disclosures?

Ms. LEHMAN. Yes, I think particularly for—in this space things can change instantaneously. I think we think we have heard a little bit today about the Metaverse, and about, like, what Web3 and AR and VR look like. If we think back to five or six years ago, which is kind of a long time, in—sometimes in legislative land, right?

You—what would—how would a—how could thinking through live video—and the advent of live video was fairly revolutionary, and the fact that video is happening on phones, and how did that change, and what kinds—as we heard from Mr. Duffey earlier, what kinds of harms can come from live video? Those are the kinds of things we need to be able to pivot instantaneously on, and—that we can't wait for.

Mrs. TRAHAN. I couldn't agree more. Certainly, there is so much in the black box that we need to shine a light on so that we can keep up. Not just the Congress, the FTC. I mean, if not them, who is going to be armed with transparency in this regard?

So I—the last thing—I know I am out of time, but I would like to request unanimous consent to enter a report from the NYU Stern Center for Business and Human Rights entitled, "Enhancing the FTC's Consumer Protection Authority to Regulate Social Media Companies."

Ms. SCHAKOWSKY. Without objection——

Mrs. TRAHAN. Thank you, Madam Chair.

Ms. SCHAKOWSKY [continuing]. So ordered.

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

Ms. SCHAKOWSKY. OK. Mr. Guthrie, you are recognized for 5 minutes.

Mr. GUTHRIE. Thank you. Thank you, Madam Chair. I have a letter from the U.S. Chamber of Commerce. It has been submitted to your staff, but I would like to ask to enter into the record.

Ms. SCHAKOWSKY. Without objection, so ordered.

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

Mr. GUTHRIE. Thank you, Madam Chair. Thank you so much. And thanks to everybody for being here today. And my questions are for Mike Duffey.

And the United States has seen historic levels of opioid abuse, leading to tragic deaths over the last several years. According to the Kentucky Office of Drug Control Policy, illicit fentanyl and its analogs were detected in more than 70 percent of all cases in Kentucky in 2020. The opioid crisis has been exacerbated by deadly fentanyl being trafficked into our communities through our southern border and on the social media platforms millions of Americans, including our children, are using.

The Energy and Commerce Committee has passed several bills to address this epidemic. One bill—I know it is in a different subcommittee, a subcommittee I have the honor of being ranking member—but the HALT Fentanyl Act.

I mean, the idea that March 11th—after this expires—after the CR expires, that illicit fentanyl will be street legal in America is just wrong. I wish we could make it permanently illegal. I do expect and hope that we can work together to at least extend it, moving forward. But it is just absolutely frustrating that we can't permanently schedule illicit fentanyl that is—70 percent of Kentuckians who died of an overdose died of illicit fentanyl in 2020.

But I am also concerned that—and where it ties into this hearing—that illegal drugs are still available online through illegal pharmacies, and even these widely popular social media platforms. This type of illegal activity online is troubling and inexcusable. I am working on a draft legislation as part of the Republican Big Tech platform that will 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 states attorneys general would ensure enforcement of these policies. So my question is for Mr. Duffey.

In your testimony, you discuss the challenges that tech platforms present to law enforcement. Do you find that most platforms have a formal process or framework by which to work with law enforcement personnel?

And do you think legislation in this space will enhance law enforcement's capabilities to track this illegal activity and facilitate?

So what is the current status of these platforms, and what would you like to see Congress do, Mr.——

Ms. SCHAKOWSKY. Unmute. That will help the—if you—we can hear him better if you unmute. There we go.

Mr. DUFFEY. All right. Thank you, Representative. I do believe that any type of framework would be to our advantage, and a win for all.

Right now, as the——

[Audio malfunction.]

Mr. DUFFEY [continuing]. Out of Big Tech, and how they struggle to—they build a tool which is used by the general population that becomes popular, and then gets misused. And then addressing and having some framework and requirements as to having a group that is able to handle the volume of law enforcement compliance legal process that we serve, and mandating that they build out these groups to respond to our responses will not only help law enforcement investigative efforts.

The other side of it is if these Big Tech corporations enact encryption, then we are back to not being able to investigate an opioid case where an individual has overdosed and now we can't get into that mobile device to identify, nor do we have the tools to try to get into this device to determine who that person was communicating with to potentially stop others from getting this drug, and work a criminal investigation.

So having—first, having these companies be held accountable to creating an outreach or law enforcement response compliance group; second, allowing the law enforcement to have the tools needed to help fight encryption. And I am not indicating that—we are not asking for anything that we aren't entitled to with proper legal process. If we can't get into these locked devices, the person who overdosed, that child who overdosed on the ground there, we can't identify where the suspect may be.

Mr. GUTHRIE. Well, thank you, and I just have 20 seconds, so I will yield back.

I don't have time for another question, so I will yield back my time. Thank you, Madam Chair.

Ms. SCHAKOWSKY. The gentleman yields back, and next is Mr. McNerney for 5 minutes.

Mr. MCNERNEY. I thank the Chair, and I thank the gentleman from Kentucky for yielding early.

[Laughter.]

Mr. MCNERNEY. I thank the witnesses. Your testimony is very compelling this morning.

Ms. McInnis, please describe for a minute or so how banning surveillance ads would transform the online ecosystem.

Ms. MCINNIS. Absolutely, and thank you for the question, Representative.

Right now, Facebook and Google control an ad duopoly in online advertising sales because they have convinced the advertising market and advertisers that behavioral ads are more relevant and serve users with more targeted ads than others would. There is no reason, however, why contextual advertisements should not and could not be just as relevant as behavioral ads.

DuckDuckGo has used contextual ads for our entire existence to show users relevant offers in the moment. We think that, you know, while you are searching for sneakers, you are likely wanting

to see ads about sneakers, and not an ad for a vacation you might have taken a few months ago.

In addition, if this bill was enacted, many companies would be prevented from the collection of online data, meaning that their duopoly—Facebook and Google’s duopoly—and ads would be diminished. Companies would be able to compete against them more forcefully in the market, and we would have more innovative, contextual advertisement services for users. And therefore, the ads would be more relevant and more useful to users in the future.

Mr. MCNERNEY. Thank you. And that was just a little more than a minute.

Ms. Lehman, you argue that if companies are truly proud of how effectively they protect consumers, you would expect them to welcome independent investigators or researchers. Unfortunately, that is not happening, which is why a comprehensive approach to transparency created in the Digital Services Oversight and Safety Act, H.R. 6796, is so important. So please explain how increased transparency from this legislation would result in concrete changes.

Ms. LEHMAN. Thank you for the question. So where platforms fail to take responsibility, transparency can flag issues. It can—and it can flag the extent of the issues, and how those issues persist.

And the kinds of issues we have talked about today a little bit, we have talked about misinformation, we have talked about discriminatory advertising. We have talked about targeting ads to children, whether that—and targeting ads to minors. And there is a CR article last year about targeting gambling and alcohol ads toward minors. This is the kind of thing that, without transparency, we don’t have a good sense of the scale of the problem, and how best to combat it.

When we—with Representative Trahan’s bill, we suddenly have the ability to make clear where the problems are coming from, and how they can best be stemmed.

Mr. MCNERNEY. I forgot to say that I am going to switch to DuckDuckGo tonight. Thank you.

Ms. Lehman, in your written testimony it states that algorithms can be opaque, and even for the engineers that designed them. I have designed algorithms. I know what you are talking about. How can the Algorithm Accountability Act help engineers be more thoughtful about their designs and testing processes?

Ms. LEHMAN. Thank you. So with the Algorithmic Accountability Act, it allows for—it makes possible impact assessments for—and so it forces, again, the consideration that platforms and companies utilizing algorithms don’t presently need to do.

And so, because there are so many different factors that can go into our recommendations or algorithmic decisionmaking, it forces considerations, and not changes, and not—but it—that—it is kind of a form of transparency unto itself, but it—forcing that forward is a crucial component of understanding what factors go into things that can affect everything from credit to housing to what ads we are seeing online.

Mr. MCNERNEY. Well, in other words, pre-planning and pre-specifications can help make algorithms more accountable and transparent—

Ms. LEHMAN. Yes—

Mr. MCNERNEY I BELIEVE THAT.

Ms. LEHMAN. Yes.

Mr. MCNERNEY. Ms. Nkonde, in your testimony you explained how predictions made through machine learning create a feedback loop that can change the course of society. Please elaborate on that. That is an interesting comment.

Ms. NKONDE. So once a prediction has been made—for example, a wrongful arrest in the case of Robert Williams, as we talked about earlier, that person now has a false arrest record. But more importantly, their biometric data is within that system, and there is no way of taking back that bad decisionmaking. So that person's life has been changed, not just personally, but administratively. And they become part of a data set that is feeding back wrong information.

Mr. MCNERNEY. Thank you. I ran out of time, and I yield back.

Ms. SCHAKOWSKY. The gentleman yields back, and—yes, Ms.—next is Mr. Bucshon.

Mr. BUCSHON. Thank you, Madam Chair, for calling this hearing today. This is a really, really important subject.

In the last few years, multiple reports and incidents have come out showing that America's youth has been harmed by the often opaque and insufficient data privacy and content moderation practices of tech platforms and other online services. I think we can all agree that that is true. It is extremely concerning.

I have four children. My youngest now, my daughter, is getting ready to graduate high school. And during her high school years we have had to navigate this. And in our family, just like everyone else's, like so many other people from Indiana, Hoosiers, they have had to grapple with what the fair and safe terms of our online presence is with this in mind, because, if anyone has teenagers, they know they will be online, whether you know it or not. It is critical that kids like my daughter learn to safely navigate these technologies, prepare them for the 21st century life and workplace.

I was a surgeon before, and I would like to—I always like to say these issues need to be addressed, I think, with a scalpel, rather than a hacksaw, in that there are data and usage restrictions worthy of examination by this committee, absolutely. Unfortunately, I think the legislation today, which is extremely well intended, probably takes more of a hacksaw approach than I would like to see, outright banning targeted advertising and opening a private right of action to let trial lawyers sue small business and local advertisers. I doesn't, I don't think, address the issue. Rather, we should examine policies how the FTC can better do their job as the cop on the beat to protect children from privacy dangers online.

We are also reviewing a bill today that would drastically expand the government to increase the FTC by nearly one third of its existing size.

So, Mr. Duffey, in your testimony you mentioned some of the ways that predators and other bad actors try to pressure and bully kids into providing information or materials that could harm them for the rest of their lives by putting it in cyberspace, and that never goes away.

Do you believe that requiring platforms to be more transparent with their cyber bullying content moderation practices would em-

power youth users and their parents to avoid, oppose, or remove cyber-bullying content that can quickly get out of hand and turn into exploitative or even illegal content?

Mr. DUFFEY. I do, thank you, Representative. I agree with you 100 percent that some transparency with youth, law enforcement, and parents would only add to the knowledge base that—for everybody on how to better protect yourself, the content, and what you are getting, what you are contributing when you sign up for these sites.

And it would allow for us to have a wider scope to the overall issue when it comes to sextortion and cyber-bullying, along with the tactics used by these individuals.

Mr. BUCSHON. Well, thank you very much. And even—I live in Evansville, Indiana. And I can tell you, talking with local law enforcement there, this is pervasive. It is surprising. Even in rural counties I represent, bad actors every day doing this. This is just not, you know, in cities, big cities and other places. This is everywhere.

Ms. McInnis, many consumers have already shown to be interested in not having their data tracked, as evidenced by the success of DuckDuckGo browser. But there are, obviously, those who have chosen to stay on the platforms that use their data. Do you think that encouraging wider implementation of privacy-by-design principles would give consumers the confidence that their data is being responsibly used, and could encourage more transparent practices in how a company uses a consumer's data to alleviate the concerns and abuses you have laid out by some of the advertisers currently?

Ms. McINNIS. Thank you, Representative. Absolutely.

However, as the Chair and ranking member have stated, we have waited too long for companies to self-regulate, and we really should act now to incentivize them to act in the best interests of their users.

Mr. BUCSHON. Yes, I mean, so what you are saying is implementation—wider implementation of privacy-by-design principles should be driven by change in Federal law.

Ms. McINNIS. Unfortunately—

Mr. BUCSHON. Not voluntary.

Ms. McINNIS. Unfortunately, sir, I just think that companies won't be incentivized to do so before we incentivize them with law.

In addition, I think competition reform bills would level the playing field, allowing more companies like DuckDuckGo to compete on privacy.

Mr. BUCSHON. That is a good advertisement.

I yield back.

Ms. SCHAKOWSKY. The gentleman yields back.

Relevant to this subcommittee, the President is apparently going to talk about social media and children's mental health tonight, which is very important to us, yes.

And next we have my friend, Congresswoman Clarke, for 5 minutes.

Ms. CLARKE. I thank you very much, Madam Chair and Ranking Member Bilirakis, for holding this extremely important hearing today. And I would like to thank you for including my legislation, H.R. 6580, the Algorithmic Accountability Act of 2022, which I re-

cently reintroduced, along with Senators Ron Wyden and Senator Cory Booker.

My legislation takes common-sense and long-overdue measures to protect consumers from harmful bias and discrimination resulting from the widespread use of automated systems that are governed by computer algorithms, artificial intelligence, and machine learning.

Let me be clear: the problem isn't just Facebook, Instagram, and TikTok. The problem is pervasive. The very same automated technologies that are being misused and abused by social media companies are similarly being used without oversight by a wide range of industries to make critical, split-second decisions about people's health care, housing, finances, employment, and so much more. And while these technologies reach conclusions based on calculations, these calculations are the products of systems designed by humans, subjecting them to a wide range of flaws that reinforce broader societal discrimination, particularly against women and people of color.

So Ms. Nkonde and it is so good to see you once again—could you share an example or two of algorithmic systems leading to discriminatory outcomes that have a major impact on people's lives?

MS. NKONDE. Yes, of course, Congresswoman Clarke. One of the most recent examples is a pain management algorithm that is used in over 1,000 health care settings in the United States that was discriminating against Black American patients because their health care costs were higher, in aggregate, than other groups. And it wasn't because of care. I can certainly speak about that more, but I know we don't have time.

And then the second example was one that was brought forth by the Haas Business School at Berkeley that found that mortgage recommendation algorithms were discriminating against Black borrowers at the same rates as human beings

[were], because the inputs that were being used, the questions that were being asked were asked discriminatory as it were a human banker (sic).

So those are two of a myriad of examples I could offer.

MS. CLARKE. So thank you. It is clear to me that something must be done to address the current lack of accountability and transparency around how automated systems are being used. And that is why my Algorithmic Accountability Act directs companies to assess their automated decision systems for potentially dangerous flaws such as inherent bias, safety risk, and performance gaps.

MS. Nkonde, would you agree that impact assessments are a feasible and important first step in tackling this issue?

MS. NKONDE. Yes. As it has been said earlier in this hearing, we are looking at impact assessments around algorithmic thinkers in the EU, and understanding the downstream impact of these technologies will be—will enable good faith actors on the public side to be able to decide whether this is actually in line with existing law. Because the harms I am describing are otherwise outlawed underneath civil rights statute, which we should be following if we are going to be—if we are going to follow rule of law in this country.

MS. CLARKE. And Ms. Lehman, do you agree, as well?

And how would these impacts assessments benefit consumers?

Ms. LEHMAN. Thank you, Congresswoman. A little bit, as we mentioned earlier, having companies have to consider things other than their profits, having them have to consider how the systems they build have impacts on communities, on marginalized communities, on consumers across the board, inherently, even if it may provide more internal accountability and provide more external accountability as well, I mean, it forces those considerations in a way that we haven't previously seen.

Ms. CLARKE. Well, thank you. And my legislation would further direct companies to report their findings to the FTC for review, and require the FTC to establish a public repository of automated decision systems along with high-level information such as data sources and how to contest decisions.

Ms. Nkonde, how would these transparency measures be helpful to consumers and researchers alike?

Ms. NKONDE. They would protect our rights and enable us to make informed decisions around what we are actually buying, and the impact it will have on our lives as—on a whole.

Ms. CLARKE. Well, let me thank you for your testimony here today to all of our witnesses. It is time that we make a change.

And with that, Madam Chair, I yield back. I have gone over time.

Ms. SCHAKOWSKY. The gentlelady yields back, and now, Mr. Dunn, you are recognized for 5 minutes.

Mr. DUNN. Thank you very much, Madam Chair. I appreciate the opportunity to discuss Big Tech today.

You know, thanks to advancements in technology, it is easier than ever to stay connected online. When the world went into a lockdown with COVID, our relationships could nominally be continued. And of course, essential businesses remained open. So social media, with American Big Tech leading the way, certainly was a boon to us, and we should absolutely continue to uphold an economic system that allows for innovation and open competition in the U.S. technological industry, especially for small and medium-sized enterprises that are trying to break into the market.

Unfortunately, social media platforms have also provided a new space for bad actors, foreign adversaries to exploit the social media channels, to target potential victims and, of course, spread harmful propaganda. And these threats are heightened during the crisis like we are seeing now in Europe.

Some of the Twitter accounts that were sharing information about the Russian unprovoked attack in Ukraine were curiously suspended from Twitter during the beginning days of the invasion. Twitter has noted that these accounts were moved removed by mistake, not due to Russian interference. And while this may not be an example of pure Russian aggression, we know similar reports will likely increase, and TikTok is already reporting a surge in Russian propaganda.

The dangers of foreign adversaries using social media to advance their agenda is clearly a very real danger. Social media companies have a social responsibility to not allow malign State influences on their websites, and I think our national security depends on that.

So first question, Ms. McInnis, we know China uses search engines to push conspiracy theories, and we know Russia is currently

using propaganda online to spread misleading information in Ukraine. How does DuckDuckGo detect foreign manipulation campaigns such as this?

And after detection, what steps do you take?

Ms. MCINNIS. Thank you for the question, Congressman.

First and foremost, the number-one thing that DuckDuckGo does to help stem disinformation and misinformation online is not collect your personal information. Companies that collect a lot of personal information, such as Google, are able to use that to further ensure that you are engaging in the product, which leads often to the presentation of conspiracy theories or other fringe videos that are presenting non-credible information.

Second, DuckDuckGo got started as a search engine that was providing users with instant answers at its top-of-the-search-engine results page. We have continued to do that, especially with regards to information that may be targeted by people with ill intentions to provide misinformation and disinformation.

And what many may not know is that the top of the search engine results page gets, by far, the most attention from any user. So by presenting users with credible and authoritative information at the top, we are ensuring that they are going to find the right answers to their questions, and not be steered away to another site that is looking to prey on their fear and misinformation.

Mr. DUNN. Thank you for that, Ms. McInnis. Again, our adversaries also want access to individuals' data, so they can build algorithms to target, predict, and manipulate behavior in the United States.

I am especially concerned about American companies that have ties to the Communist Chinese Party, and what data they are forced to share because of that relationship with China. You know, I think consumers deserve more transparency.

How is their data used? Can you tell us a little bit more about that data? When are they forced to share?

Ms. MCINNIS. Thank you for the question, Congressman. I am not sure what data companies are forced to share, in part because DuckDuckGo does not collect any personal user data as people use our systems. So by—

Mr. DUNN. Well, thank you for not doing that. I appreciate—time is drawing short, so I am going to ask you for yes-or-no answers to these, if you will.

Do believe that the amount of individual data collected by Big Tech companies is concerning?

Ms. MCINNIS. Very.

Mr. DUNN. Good. In general, is the data collected by Big Tech companies used to influence individual behaviors?

Ms. MCINNIS. Absolutely.

Mr. DUNN. OK, good.

Mr. Duffey, we are going to give your technology another shot here. From your experience, what tools could social media sites implement to help users identify nefarious accounts?

[Pause.]

Mr. DUNN. Shouldn't have taken the risk, I guess.

Mr. DUFFEY. Thank you—

Mr. DUNN. [Inaudible.]

Mr. DUFFEY. I think the internal tools that they collect——

Mr. DUNN. Mr. Duffey, go ahead. What tools would you wish you had from Congress?

[Pause.]

Mr. DUNN. A good computer——

[Laughter.]

Mr. DUFFEY. I would wish that the technology companies——

Mr. DUNN. What?

[Pause.]

Mr. DUNN. I appreciate the Chair's——

Mr. DUFFEY. Can you hear me?

Mr. DUNN [continuing]. Forbearance. I yield back.

Ms. SCHAKOWSKY. Yes, I think we, unfortunately, lost him. Next is Mr. Cárdenas for 5 minutes.

Mr. CÁRDENAS. Yes, thank you, Madam Chair Schakowsky, and also Ranking Member Bilirakis, for having this important meeting, and talking about these very good bills.

I would also like to thank my colleague, Representative Lori Trahan, for introducing her bill, which would help shine a light on the content moderation practices of Big Tech companies.

Without adequate transparency, we don't have the information we need to understand how disinformation spreads, and how to hold these companies accountable when they fail to make strong-enough measures to combat it.

This problem is particularly bad in Spanish-speaking communities, where we have seen social media companies fail to invest the resources necessary to fight Spanish-Language disinformation. And it has come to my attention that Russia is feeding disinformation about what is going on in the Ukraine, specifically bombarding the Spanish-speaking community here in the United States and around the world. So obviously, they are trying to skew the truth, and trying to get certain communities to believe that Putin is muy bueno, or a good guy, and he is not.

Thanks to whistleblowers like Frances Haugen, a former Facebook product manager, we know the Facebook—that Facebook directed 87 percent of their investments on combating misinformation to English language content, in spite of the fact that only 9 percent of Facebook users are English speakers. What a disparity.

These disparities are unacceptable, especially when consuming misinformation can lead to real-world health, safety, and financial consequences for communities. And also, in some cases, people are actually dying based on what people are fed and the actions that they take.

Ms. Lehman, would publicly publishing how these online platforms moderate non-English language content hopefully put some pressure on companies to correct the disparities and content moderation investment between English content and content in other languages? And if so, how so?

Ms. LEHMAN. Absolutely. And I think, in large part, because those disparities, when they are said aloud, are so dramatic and so disproportionate, and so just incredibly disheartening, right?

As the statistic you just cited, if it is 87 percent, even though it is making up 9 percent—even though English speakers make up only 9 percent of that platform, all sorts—all languages deserve the

level of attention and the intensity and the appropriate content moderation, because all consumers deserve high standards of conduct moderation, and that when they are using a platform online, they can expect that their experience won't be different from someone else's simply because of the language that they are using on that platform.

Mr. CÁRDENAS. Thank you. We had Facebook in front of us, and other companies, and they admitted that they could put some more resources in there, but they choose not to.

For example, McInnis, wasn't it earlier today that somebody asked about whether or not DuckDuckGo is actually profitable, and you said yes? What number do you—did you say that your revenue is \$100 million?

Ms. MCINNIS. That is correct, Representative.

Mr. CÁRDENAS. Is that per year?

Ms. MCINNIS. It is per year.

Mr. CÁRDENAS. An annual basis? A year. Well, I would venture to guess that \$100 million is a slow day for Facebook/Meta, Google, and Amazon.

So I pray that DuckDuckGo can actually continue to succeed in this environment, because we are talking about companies that are now net worth \$1 trillion or more. And the reason why I point that out is because they choose not to use good practices. They choose not to have practices that are respective of the consumer, respectful of the people who are using their platforms.

And so I just want to commend you, Ms. McInnis, and please tell the C-suite executives at DuckDuckGo that I hope and pray that your model continues to work in this environment. And unfortunately, you are a tiny player on this playing field. Please take a second if you think that I am mischaracterizing, what I just said.

Ms. MCINNIS. No, I appreciate your words, Representative, and we are trying very hard to compete in this marketplace. But as we have mentioned, Facebook and Google hold a duopoly in advertising. And the Banning Surveillance Advertising Act would help mediate that inadequacy in the market, and allow for more companies to compete on privacy, just like DuckDuckGo.

Mr. CÁRDENAS. Thank you so much. In 2020 a product risk assessment calculated internally by Facebook found that Spanish language misinformation detection on the platform remains, "very low performance."

In spite of that, the report's recommendation was to—and I quote—"just keep trying to improve," and aim—and claimed that—and I quote—"addition of resources will not help." That—nothing could be further from the truth.

And the last thing I will say is, without public accountability, I think that these companies will continue to do the wrong thing, and we do need to have Federal legislation to rein them in for the sake of people's health and livelihood, and for the lives of the people and the children who are badly affected by these platforms.

I am sorry I went over my time, Madam Chair, I yield back.

Ms. SCHAKOWSKY. No, I thank the gentleman.

And Mrs. Lesko, you are recognized for 5 minutes.

Mrs. LESKO. Thank you, Madam Chairman. Before I begin my question, I want to correct the record.

Earlier in the hearing Representative Castor had urged the need for the House to have a bipartisan bill updating the children's on-line privacy protection rule, and I agree we need a bipartisan bill. But such a bill already exists. Representative Walberg and Representative Rush introduced H.R. 1781, the PROTECT Kids Act, earlier this year. And I understand Republicans have requested this bill to be included in the last two legislative hearings, but still to no avail.

Furthermore, the bill was reintroduced from last year, so I am happy to say to Representative Castor that the Senate is not ahead of us on this particular issue.

I also want to add that I understand that Leader McMorris Rodgers and Ranking Member Wicker have now asked the President twice on engaging on a comprehensive national privacy and data security bill—not just on children's privacy—and have not heard back yet, or there hasn't been an attempt to build a consensus with us Republicans.

So I think we do want to work in a bipartisan area, because this is very important.

Well, again, I want to say thank you to the witnesses for being here today.

Before I begin my questions, I want to express my disappointment that representatives from the advertising industry were not invited to testify at a hearing which examines legislation that will severely impact the advertising industry. It seems that they deserve a seat at the table, so we can understand the effects.

I do want to be clear, however, I have the same concerns that my colleagues have, in terms of Big Tech abusing their power and escaping responsibilities for their wrongdoing.

However, H.R. 6416 will burden the small and medium-sized enterprises that are looking to gain entry into a market that heavily relies on advertising to be successful. The niche products created by innovators looking to capitalize on the American dream will not be able to grow or even survive under this legislation.

I do not believe that was the intent of the sponsor, my friend. I know you care about protecting Americans' privacies, but let's not do it at the expense of small businesses. Yes, abusers like Google must be held accountable, but we must be sure to examine that actions taken to curb Big Tech's power will not unduly burden small businesses.

The FTC has shown no interest in protecting good actors in the market, so that duty now falls on us. But these are the very same concerns that the Interactive Advertising Bureau, an organization that should be on today's panel, explained in a letter to this committee. And I ask that this letter—it is rather a lengthy one—be submitted for the record.

And if Mr. Duffey can hear us—

Ms. SCHAKOWSKY. Without objection, so ordered.

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

Mrs. LESKO. Thank you, Madam Chair.

Mr. Duffey, thank you again for your testimony, and for your long career wearing the badge. You raised many issues that we should be examining as we hold Big Tech accountable.

Central to our goal is the Federal Trade Commission and their ability to inform Americans about resources they have when their security has been violated. As a law enforcement expert, what information would you want people to know about when their safety is violated on social media platforms?

Mr. DUFFEY. Thank you, Representative. Hopefully, the audio is coming through a little bit clearer.

To answer your question, I think today you would want to know, when your safety is violated, what exactly is the data that is—was available to that individual. Was it personal information, as it relates to your phone number? Was it date of birth information?

What—a lot of times, when we see these social media sites, there is a growing concern amongst individuals that they are being encouraged to link their profiles to other social media sites. The question then becomes—is what data carries from company to company, and how does that impact the citizens that we serve every day?

So I think, while a lot of it is we are used to credit reports being offered to people once they are—once they have been compromised, from a social media perspective, were my pictures taken? The big picture of what exactly was compromised, so that I can make a self-assessment as a citizen to what safety factors I am more concerned of.

Mrs. LESKO. Thank you.

And Madam Chair, I yield back.

Ms. SCHAKOWSKY. The gentlewoman yields back. And now, Congresswoman Debbie Dingell, it is yours for 5 minutes.

Mrs. DINGELL. Thank you, Chairman Schakowsky. Thanks for holding this important hearing, and to all the witnesses for testifying today.

In our December hearing on holding Big Tech accountable, I discussed how these platforms prioritized profits over people by keeping users engaged. These direct design choices have a profound impact on children and adolescents who are using these platforms, and we have seen an increasing connection between time spent on new media and mental health issues we are seeing in children and adolescents. In this increasingly digital age, we need to be vigilant in re-evaluating how these design choices impact children, and we need to work to prevent subsequent harms online.

I am going to—I know previous questioners—my colleagues have asked some of these questions, and I am going to try to build on them. I want to start just by getting each of you on record with the same question I asked at the subcommittee's previous tech accountability hearing.

To the panel, are social media companies conducting business online actively making the choice to prioritize profits and engagement over combating disinformation, violent content, and negative health outcomes for individuals and children?

Just a yes or no answer, Ms. Lehman.

Ms. LEHMAN. Yes.

Mrs. DINGELL. Ms. McInnis?

Ms. MCINNIS. Yes.

Mrs. DINGELL. Ms. Nkonde?

Ms. NKONDE. Yes.

Mrs. DINGELL. Mr. Duffey?

Mr. DUFFEY. Yes.

Mrs. DINGELL. Thank you. OK.

Ms. Lehman, are there ways in which the design features or algorithms of these platforms can take advantage of young people in particular, leading to worse outcomes?

Do these design choices increase the likelihood that children will be exposed to divisive, violent, hurtful, or inappropriate content?

Ms. LEHMAN. Absolutely. So right now we—a lot of what is most exciting about the transparency of things before us today is that there is not enough information to have a good sense of how exactly some of these platforms are making these design choices. We understand they are, but we don't know the intricacies of exactly how to fix it.

A lot of this legislation allows us that insight, and also starts to force platforms to consider ways that their algorithmic systems are designed, ways that they are—it starts, as you said, when they are prioritizing profits over people. It starts to combat that, it provides—because, ultimately, they do need incentives to do so.

Mrs. DINGELL. Thank you.

Ms. McInnis, what responsibility do tech companies have to protect children from manipulative marketing content and product recommendations and targeted advertising?

Should these companies have some level of responsibility for a failure to protect our young users?

Ms. MCINNIS. Absolutely. And thank you for the question, Representative.

We encourage tech companies to take more responsibility over the kinds of tracking that they are using online, and how that tracking encourages other third parties to target users with misinformation, disinformation, and other offers that may be inappropriate, especially for children.

Mrs. DINGELL. Thank you.

Ms. Lehman and Ms. Nkonde, do you believe that, without legislation, companies will take the necessary steps to protect children from manipulative practices on their platforms?

How would the legislation under consideration today ensure that regulators and researchers have the tools and information necessary to protect children and adolescents using these platforms?

Why don't we start with Ms. Nkonde?

Ms. NKONDE. I don't think that any of the companies are incentivized to protect children because they are publicly traded companies. Therefore, their first priority is to their shareholders. This legislation would create that hand in the same way that, in the age of robber barons, Congress had to come in and create an incentive.

In terms of transparency, knowing the harm allows us to have a targeted and appropriate remedy that can maintain innovation and business in the United States, while protecting our children, who, in my humble opinion, as a mother, are our greatest asset.

Mrs. DINGELL. Ms. Lehman, 20 seconds. Can you give us a quick answer?

Ms. LEHMAN. Yes, I would echo Ms. Nkonde.

And we know from previous hearings that platforms don't action, or don't action—maybe even three to 5 percent of hate, of violence,

and of incitement, these problems are rampant, and I think if—certainly, the transparency would lend itself to public accountability for that.

Mrs. DINGELL. Thank you, Madam Chair. I yield back.

Ms. SCHAKOWSKY. The gentlewoman yields back.

And Mr. Pence, you are recognized for 5 minutes.

Mr. PENCE. Thank you, Chair Schakowsky and Ranking Member Bilirakis, and thanks—I thank the witnesses for being here today. I am going to kind of give you a background a little bit where I am at on this with some statements.

Like many of my colleagues, I am increasingly concerned with the growth-at-any-cost mindset of Silicon Valley. Social media platforms employ algorithms that promote inflammatory, addictive content to elicit the strongest level of user engagement. You know, as we have talked about with children, that is a horrible thing.

More clicks lead to more data that fuels a more lucrative online advertising business model. Efforts to keep users glued to their screen is at the heart of this business model. You know, we know that is true, because everybody has got their nose in their phone all the time.

Our public disclosures have become overtly divisive. Our younger generations have developed unhealthy addictions to social media, and an individual's right to privacy is disregarded.

The online environment of intrusive data collection inflammatory content is not the only option. I am encouraged to hear the conversation today and the level of agreement we have on problems facing Hoosiers and all Americans as it pertains to Big Tech. It is time that we start enacting in advance holistic solutions that will rein in Big Tech and produce real results to protect our constituents online.

Our constituents should have more control over how their personal information is collected and used online, or—and this is where I deviate a little bit—receive fair compensation when their information is collected and sold, as it is happening absolutely non-stop.

Ms. McInnis, in a previous hearing I discussed whether or not a social media platform could still be profitable without the ability to monetize content that has been adjudicated to be harmful to users. Likewise, DuckDuckGo is a profitable company that claims to not engage in surveillance advertising. Concerns have been raised that, if Congress limits a platform's ability to engage in automated surveillance advertising tools, small businesses will suffer from a lack of reach, which—I wrestle with that.

However, as you referenced in your testimony, research shows only modest gains for the user of behaviorally targeted ads. I hear that a lot from the small businesses that use social media. Some it is good for, but the vast majority, it says it gets nothing for me.

And yet, oddly, advertisers are very willing to pay a premium for what they believe extends their reach. Is it reach, or extends their data collection?

If the outcome for online advertising is similar to what you can expect from other methods, the only difference becomes the amount of information Google or Facebook or any of the other Big Tech can gather from you and your business, or you personally. What has

the experience been like at DuckDuckGo for small businesses seeking to advertise their products to potential consumers, from your perspective?

Ms. MCINNIS. Thank you for the question, Representative.

Unfortunately, we syndicate our contextual ads through Microsoft. So Microsoft would have the best data on how small businesses have utilized the platform. That said, DuckDuckGo is a smaller tech company that is competing against the giants. We also use contextual ads, and we have used the contextual ads on our services, as well. So we have proven that this is a profitable model for us.

In addition, many small businesses have been using contextual ads to their benefit.

Finally, as I mentioned earlier, the ability to discriminate in the targeting of advertisements also enables companies to discriminate in the opportunities that they present to users, meaning that some smaller businesses may be discriminated against in the provision of financial resources, rental opportunities, housing agreements, and other things that make their small business possible.

Mr. PENCE. Well, I would even say—I appreciate that comment. I would even say in sales, too, they get limited. It depends on who is collecting the data, and who they are dispersing that data to. It is a real problem for me.

Ms. Nkonde, what is your answer to that same question? And that question was your experience with small businesses, the value there. Are they making money off this data collection of Big Tech?

Ms. NKONDE. I would actually agree with your assessment that the returns are actually on the tech company side, in terms of more data. Because with more data, you can create more products, you have more insight. And the rate of return can be negligible.

But that is not to say all the time. There are some businesses that are able to benefit, but not in the same way that the big giants do.

Mr. PENCE. Yes, thank you for that. You know, I think it is time we stop talking about being—us receiving some benefit for all the data that is being collected on us.

And thank you, Madam Chair, I yield back.

Ms. SCHAKOWSKY. The gentleman yields back. And now my colleague from Illinois, Congresswoman Kelly, for 5 minutes.

Ms. KELLY. Thank you, Chair Schakowsky, for holding this hearing today, and for the witnesses appearing before us.

I am delighted to see that one of the bills recommended by the E&C Racial Equity Working Group, the Algorithmic Accountability Act, will be considered here today.

Every day people go online and search or buy products, and all the while, little bits of their activity get collected and put toward creating an online profile of a user's wants, likes, and dislikes. In the real world, more and more decisions are being made by artificial intelligence from data collected from what we do online. Large amounts of data are combined to make predictions with little knowledge of the underlying data used to train the algorithm, or the potential bias that is encoded in the system. One of the more difficult conversations to have around AI—what it means for AI to be transparent or explainable.

Ms. Nkonde, in an interview last year with Stanford's Engineering's The Future of Everything podcast, you mentioned that impact assessment information would be more useful than opening up an algorithm and seeing what is inside. Can you elaborate on this?

Is it either or—is it an either/or situation, or how would the Algorithmic Accountability Act—how would it help biases in how algorithms are designed and the outcomes they produce?

Ms. NKONDE. Congresswoman Kelly, I would suggest that, because we are looking for accountability, the impact of the technology is way more important than the longitudinal algebra that it took to create the algorithm, because those statistical models are going to be visible to very few people in the population.

And from an oversight perspective, Congress just needs to know, are these products in line of the laws of our land? And for that you just need impact.

Ms. KELLY. Thank you.

Ms. Lehman, in your testimony you point out the imbalance that the FTC often faces going up against some of the largest tech companies in the world. The Digital Services Oversight and Safety Act and the Algorithmic Accountability Act include increased FTC staffs and funding, albeit at different levels.

Can you explain how the current imbalance of FTC staffing harms the ability of the government to stop bad actors?

Ms. LEHMAN. Absolutely. Thank you, Congresswoman.

So the FTC today is a fraction of the size it was 40 years ago, even while the economies from some of the largest platforms alone were unthinkable at that time. And so the kinds of resources that the FTC has to combat the systemic problems throughout these—throughout this industry is—the fact that we are still smaller than—compared to the outsized growth there, it—we can only—consumers will only benefit from a fully empowered FTC that can—that has the level of expertise and funding to effectively go after these industries.

Ms. KELLY. Thank you.

And Ms. McInnis, do you have anything to add?

Ms. MCINNIS. We likewise support a fully funded and resourced Federal Trade Commission.

One of the best things that the Federal Trade Commission and, indeed, the U.S. Government could do right now is enforce our existing rules and laws. And so we encourage the Federal Trade Commission to not only enforce their laws, but also consider where they could act to protect users, perhaps through examining new rules under the Children's Online Privacy Protective (sic) Act, or acting against patterns that we are seeing online under their section 5 authority.

Ms. KELLY. Thank you. The European Union has already started their work toward an AI law. Their bills differ in many ways from the bills being considered today, but share some important similarities.

Ms. Lehman, how would the Algorithmic Accountability Act align with European efforts to regulate AI, and how do they differ on taking risk-based approaches?

Ms. LEHMAN. Thank you, Congresswoman.

So in the EU there have been proposed legislation—there has been proposed regulation that would put algorithms into different risk buckets. And so this is where they differ insofar as they would go so far as to ban algorithms in the use of, like, the highest risk buckets, thinking more about, like, social credit scoring. There would be more regulations around how they can be used in some of the medium-risk buckets, and transparency in the lowest-risk buckets.

We are a little bit earlier on in our AI regulation discussions, and so are—in the U.S., the—we—the primary mechanism we have right now in the Algorithmic Accountability Act is impact assessments and that transparency. So getting a sense of, OK, what are the effects of these systems.

Ms. KELLY. Thank you.

And with that, Madam Chair, I yield back.

Ms. SCHAKOWSKY. And next I call on Mr. Soto for his 5 minutes.

Mr. Soto, the floor is yours.

Mr. SOTO. Thank you, Madam Chair. When we look at 7 in 10 Americans using social media platforms—that actually even sounds pretty low for me; most people I know use social media, right?

And the practice of sharing user data to target advertisements has led to discrimination based upon race and gender on occasion. Forty-two percent of Americans experienced online harassment over the past year, forty-two percent. And social media companies have consistently denied and blocked the needed data for us to do independent research and government research.

But there is hope, right? Because, while we know so many Americans are using social media, privacy online is an issue that affects most Americans. And the big headline from this hearing today is that the Energy and Commerce Committee, Democrats and Republicans, are coming together to propose bipartisan agendas, bipartisan bills to protect America's privacy online.

And Madam Chair, I thank you and the ranking member for—my fellow Floridian, Gus Bilirakis, for your leadership on this, the Banning Surveillance Advertising Act of 2021. It prohibited advertisers from targeting advertisements based upon personal information that links the consumer's connected device, basically hunting down who you are by your device, rather than by your preferences and what you avail yourself to online.

The second bill, the Algorithm (sic) Accountability Act of 2022, which would conduct impact assessments on the algorithms that are mysterious to so many folks, and have regular reporting of these results to the Federal Trade Commission to make sure they are fair against discrimination, against anti-consumer issues, against all sorts of nefarious things that can happen if we leave it just to machines to make these decisions.

The third bill, Cooperation Among Police, Tech, and Users to Resist Exploitation Act, or the CAPTURE Act. I want to give a compliment to my fellow Floridian, the ranking member, Gus Bilirakis, on this great bill on how social media companies communicate, consult, and coordinate with Federal, State, and local law enforcement to address illegal content and activity online. We have to protect our kids, we have to protect our families.

My wife is an assistant principal in central Florida, and we see kids being exposed to adult content that has really hurt their childhood, and has made it harder on educators, and particularly on parents.

Increasing consumer education of law enforcement resources, by Representative Mullin, that requires the FTC to work with the attorney generals to develop educational programs to inform the public on resources available, should they feel their safety or security was violated. Right now, many Americans don't know where to go, and this is a key part.

And then finally, the Digital Services Oversight and Safety Act of 2022, which establishes the Bureau of Digital Services Oversight and Safety, a long-time need at the FTC to beef up their oversight of social media platforms under the FTC.

Thank you, Special Agent Duffey, for being here. Welcome from Florida, at least virtually. We appreciate you testifying today. What other types of criminal acts and dangers do you see online from Floridians, from your role at FDLE?

Mr. DUFFEY. Thank you, Representative.

[Pause.]

Mr. DUFFEY. Can you hear me?

Mr. SOTO. Yes, we could hear you. So what are the types of criminal acts online that you end up seeing in Florida, and the dangers?

Mr. DUFFEY. We see everything that you could think of, and more. There is not a day that goes by that we aren't learning something new. Everything from the drug trade to individuals selling other—personal information from other people's accounts. It has really become the modern day means of communication amongst all criminal activity. They establish groups using different platforms, leveraging encryption services to hide behind a curtain that we are not privy to.

So it is increasingly becoming a challenge, as you mentioned, with today's youth, and the content that they get exposed to on a daily basis, the mental health impact that it has on them, and the lack of oversight in the amount of content that they view is growing each and every day.

So if you can think of a criminal activity, from selling somebody's house that they live in, to compromising a bank account, to title fraud, car fraud, it is all occurring in the digital environment.

Mr. SOTO. Thank you, Special Agent Duffey. Together we can empower parents, families, educators, consumers, prevent discrimination with this critical agenda.

And I yield back.

Ms. SCHAKOWSKY. The gentleman yields back. And now, Congresswoman Craig, you are recognized for 5 minutes.

Ms. CRAIG. Thank you so much, Madam Chair, for yielding.

Ms. Lehman, I want to start by thanking you for providing such thoughtful and helpful testimony across so many different areas related to holding Big Tech accountable, and for calling out Snapchat in your section 230 reform ideas.

I have raised my concerns about Snapchat serving as an illegal marketplace for drugs in prior Big Tech hearings, and I want to continue my focus on the issue during today's hearing, as well.

As my colleagues may recall, I have a constituent in Hastings, Minnesota, Bridgette Norring, who—she and her family lost their son, Devin, to a fentanyl overdose, and is asking us to do more. I am here today raising her voice and that of countless other parents in hopes that we can come together and find a solution.

Special Agent Duffey, thank you for what you do in law enforcement every single day to help to crack down on these illegal online sales. I strongly believe we need to give our law enforcement agencies the tools, resources, and funding they need to help protect our communities, both online and in the physical world, from dangerous drug overdoses.

You may have seen recent news stories online talking about changes Snapchat was taking to curb drug dealing on the app, under pressure from parents like Bridgette and other parents who called on the CEO to do more and do better. Based on your experience, though, Agent Duffey, and in training those who use apps to conduct investigations, I am hoping you can briefly walk us through what the current process looks like when you attempt to target a known drug dealer and hold them to account on an app like Snapchat.

Mr. DUFFEY. Thank you, Representative.

When we begin these types of investigations with companies like Snapchat, we are often times the ones being provided it through a citizen that becomes concerned. And in some cases, some companies will police themselves and identify content. But ultimately, they are seemingly less proactive in trying to remove some of this content, and leaving it for law enforcement to become proactive on their own site, which is a challenge as we struggle with retention of law enforcement officers around the United States.

So these investigations begin with us identifying a criminal activity. Then we begin to serve legal process, which becomes the first hurdle in trying to identify what the company has retained or what they haven't retained, which becomes the first struggle.

And then, as we progress through the app, we end up at internet service providers and cellular providers, because the means of using these apps are done through mobile devices. And so the mobile device itself, through the companies that provide the service, we run again into another issue of data retention and activity that may or may not be kept, along with these criminal activities being used with a virtual private network, meaning they are using a service that ultimately hides their internet activity in which no records are often found.

So we have run into many roadblocks. I would say we have less successes than we have incomplete cases because of those things that I mentioned.

Ms. CRAIG. Special Agent Duffey, you mentioned that the Snapchat or other platforms sometimes will proactively contact law enforcement, but most of the time it is citizens who are doing the trolling on these platforms and contacting you. And I would assume that, often times, that is because a family member has suffered some sort of catastrophic outcome, or at least some harm.

What do you think the responsibility of the social media platforms should be, in terms of being proactive on their platform?

Mr. DUFFEY. Thank you. I think the responsibility is all in their favor. They should be the ones content moderating. They should be the ones communicating and learning from law enforcement, who is learning from kids in school and friends and family. Having that open conversation will only benefit them.

Right now, we see many of the companies ignoring or not having that communication with the public and law enforcement. Things—they think that they can, in a sense, take it upon themselves to learn it, or wait to become reactive.

So I think, if you are going to build a platform environment for kids to operate on, then you need to be responsible for taking action and learning what to look for.

Ms. CRAIG. Thank you so much. Amen to that. And with that, I am sorry I am out of time, but

[inaudible] topic.

I yield back.

Ms. SCHAKOWSKY. The gentlelady yields back, and now I welcome as a waive-on to our subcommittee Mr. Walden—I am sorry, Walberg—for 5 minutes.

Mr. WALBERG. Thank you, Madam Chair, for allowing me to waive on to this hearing.

This is the third legislative hearing the committee has held on holding Big Tech accountable. But once again, I believe it fails to address one of the most pressing issues: it is personal, of course, but the need for a comprehensive national privacy and data security framework. Though many of the proposals today are admirable, they include components that should be considered in a comprehensive framework, not as a piecemeal set of bills. Members of the committee need to get back to our bipartisan work to create this framework. Privacy, and children's privacy in particular, should be a no-brainer.

Despite what the gentlelady from Florida said earlier, there already is a bipartisan COPPA bill in the House. I and my good friend, Congressman Rush, introduced the PROTECT Kids Act, which would update and modernize COPPA for the online behavior and devices of today. The legislation was introduced last Congress, and I would be glad to work with her on this issue.

This is another reason why I am disappointed that the majority denied Republicans' second request to include this legislation in today's hearing. I am committed to finding a bipartisan agreement on COPPA as a part of a larger privacy package, and I hope that the majority will work with us to find common ground on our proposals.

Ms. McInnis, my PROTECT Kids Act adds precise geolocation and biometric information as two new categories of personal information which are protected for children under COPPA. I believe that behavioral ads can be beneficial for adults, but many of those benefits do not translate when it comes to kids. And so how can companies like TikTok design their platforms to better protect this type of information for children, without the negative effects that a blanket ban on ad targeting would have for small business, small and local businesses?

Ms. MCINNIS. Thank you for the question, Representative.

We encourage companies like TikTok to stem the amount of data that they are collecting from all users, especially children.

DuckDuckGo is a search engine, and so I can't speak to many of the issues preventing social media companies, in particular. But we do think that there is more that companies could be doing proactively to protect users, and also ways they could be adjusting their algorithm to ensure that they are not causing the sort of mental health and other relevant harms that we have seen Frances Haugen speak about with regards to Facebook that we know we are being perpetrated online.

But regardless, the fact that this company can target users and adjust the algorithm in order to kind of reach users in this moment of mental health crisis, or kind of anything related to that, means that they are collecting too much information on us all, much less kids.

Mr. WALBERG. Yes, yes. Thank you for that.

My legislation also raises the age for parental consent protections for children online from 13 to 16 years of age. I have lost their votes now, but I think it is responsible, a responsible approach to take. I support raising the age of COPPA.

But Mr. Duffey, in your testimony you highlight how children and tweens frequently bypass parental consent protections in order to socialize online. Can you elaborate on the dangers that those between the ages of 13 and 16 face on social media sites, and how those dangers may differ from those under 13?

And also, what should Congress be considering to address age restrictions online?

Mr. DUFFEY. Thank you, Representative. I would offer to the committee that, when we talk about 13 to 16 years old, we—in talking with mental health professionals, I would offer up their thoughts and opinions and medical concerns, because the content that you view at the age of 13 versus the content that you are viewing at 16 is going to—what we have seen with the kids is it is going to greatly impact potential behavior

[inaudible] forward with as they grow.

When we talk about the children today circumventing the system, it is very much an issue, because I don't know that you will ever stop youth from bypassing—

Mr. WALBERG. And parents can be an asset.

Mr. DUFFEY. Yes, they very much can, but they need to be educated, as well.

Mr. WALBERG. OK, thank you. I see my time has expired.

And thank you for allowing me to waive on.

Ms. SCHAKOWSKY. Thank you, Mr. Walberg. And now I am happy to have the opportunity to waive on to this subcommittee Congresswoman Eshoo, who is the author and chief sponsor of the Banning Surveillance Advertising bill that we are considering today.

Ms. Eshoo, you are recognized.

Ms. ESHOO. Well, thank you, Madam Chair, for not only holding this hearing, but welcoming me to waive on to the subcommittee. I thank you for being with me on the Banning Surveillance Advertising Act. If our colleague, Bobby Rush, is still with us, I want to thank him, as well.

First I want to go to Ms. McInnis. Thank you for your excellent testimony, and for your support of my legislation.

To my colleagues on both sides of the aisle, you may not know, but my bill does go after the root of the social media problem, which is a toxic business model. Critics say that there can't be an internet economy without surveillance ads. They have really poured it on, you know, that, you know, the internet will implode without this.

But I view it another way. And I think so does DuckDuckGo, because it is a counter-example. So I want to respond just briefly to a few questions related to the criticism that opponents of my bill cite very often. And if you could keep your responses brief, I would really appreciate that.

So to Ms. McInnis, have you found that contextual advertising to be less effective than behavioral advertising?

Ms. McINNIS. We have not. We use contextual advertising ourselves, not only to fund the business, but also to reach new and potential users of the DuckDuckGo services.

In addition, I have spoken often about the need to invest more in the contextual advertising model. Just because the ad duopoly from Facebook and Google are asserting to us that behavioral ads work better, it is not true that contextual ads can't be just as relevant.

Ms. ESHOO. Do you hear major complaints from users that your ads are not relevant enough?

Ms. McINNIS. We syndicate our advertisements from Microsoft's Bing.

We find that users are coming to us primarily for privacy protection, and we offer them best-in-class privacy protection, relevant results, and quality services, while also protecting their privacy.

We are hopeful that, with a bill like the Banning Surveillance Advertising Act of 2022, we will have more competition in the contextual ads market, which will not only enable more companies to compete against Facebook and Google's ad duopoly, but also enable small businesses to go to more advertisers, rather than just the two big duopoly—big monopolies in town to source their advertisements.

Ms. ESHOO. Two more questions. Are small businesses able to use contextual ads to reach their customers?

And the other question is will the internet break without surveillance ads?

Maybe you should take that first.

Ms. McINNIS. The internet will not break without surveillance ads. And in fact, DuckDuckGo is proof positive that you can have a successful and profitable company without surveilling users.

In addition, small businesses can use contextual ads to reach their users. And indeed, many do, because contextual ads are cheaper, and usually provide users with the same amount of revenue in return. We have cited some studies from researchers like Alessandro Acquisti, pointing out that behavioral advertising does not, in fact, result in much added revenue for publishers. And we think that is also true for small businesses.

Ms. ESHOO. Wonderful. Let me go to Ms. Nkonde.

Thank you for your powerful testimony, and for everything that you are doing in this space. Can you State to members and whomever is tuned in about the harms that ad targeting have caused people, particularly people of color?

I think that this is—I know what the answer is, but I would like to have you put it out on the table, so that people have even more clarity about this.

Ms. NKONDE. So what we found in the election space is our adversaries really take advantage of racial divides in this country by targeting advertising online toward Black communities, and we have heard earlier in this hearing Spanish-speaking communities, when they want to divide and weaken us.

So what your bill actually does is add national security protections on top of this, on top of all the other protections, because, without that targeting—targeted advertising, it breaks down that pathway.

Ms. ESHOO. Thank you.

And I yield back, Madam Chair, and thank you for having me with you. It is a terrific subcommittee.

Ms. SCHAKOWSKY. The gentlelady yields back. I thank you—thank her for her presence with us today.

I—seeing no more members who have questions, I want to sincerely thank our witnesses for your participation today. This was really a great hearing. All of you contributed so much to the discussions that we need to be having, so I thank you.

And I want to remind members that, pursuant to committee rules, they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared to today.

And I certainly ask each witness to respond as promptly as you can to any of the questions that you may receive.

With that, before we adjourn, I request unanimous consent to enter the following documents into the record: a letter from the Association of National Advertisers; a letter from the—what is that?

VOICE. Interactive.

Ms. SCHAKOWSKY. Interactive—

VOICE. Advertising.

Ms. SCHAKOWSKY. I will start again. A letter from the Interactive Advertising Bureau; a report from New York University; a letter from the Software and Information Industry Association; a letter from the FTC—a letter to the FTC; a letter from the U.S. Chamber of Commerce.

And without objection, so ordered.

[Material submitted for inclusion in the record follows:]

Ms. SCHAKOWSKY. And I want to see if my ranking member had anything he wanted to add.

Mr. BILIRAKIS. I am good. I appreciate everything you have done today, and we hope we can—

Ms. SCHAKOWSKY. Put—yes, go ahead.

Mr. BILIRAKIS. No, thank you very much, Madam Chair. I appreciate it very much, and I want to thank the witnesses, and the panel.

And also, we want to get these bills moved forward with a markup, and get them on the floor as soon as possible, particularly when

it comes to the social media and what it is doing to our children. It is unacceptable. We have to hold these companies accountable.

So thank you for bringing it to our attention today. And again, I appreciate it very much, Madam Chair. I yield back.

Ms. SCHAKOWSKY. At this time, the subcommittee is adjourned. Thank you.

[Whereupon, at 1:28 p.m., the subcommittee was adjourned.]



February 14, 2022

Representative Anna Eshoo
272 Cannon House Office Building
Washington, DC 20515

Representative Bobby Rush
2188 Rayburn House Office Building
Washington, DC 20515

Representative Jan Schakowsky
2367 Rayburn House Office Building
Washington, DC 20515

Senator Cory Booker
717 Hart Senate Office Building
Washington, DC 20510

Dear Representative Eshoo, Representative Schakowsky, Representative Rush, and Senator Booker:

On behalf of the ANA – Association of National Advertisers (“ANA”) – we write to express our opposition to H.R. 6416, the Banning Surveillance Advertising Act of 2022, and its Senate counterpart, S. 3520 (collectively, “the proposed bills”).¹ While we strongly believe a need exists for comprehensive and preemptive federal legislation on data privacy, the proposed bills would harm consumers and the diverse businesses that serve them.

The ANA’s mission is to drive growth for marketing professionals, brands and businesses, the industry, and humanity. We serve the marketing needs of 20,000 brands by leveraging the 12-point ANA Growth Agenda, which has been endorsed by the Global CMO Growth Council. The ANA’s membership consists of U.S. and international companies, including client-side marketers, nonprofits, fundraisers, and marketing solutions providers (data science and technology companies, ad agencies, publishers, media companies, suppliers, and vendors). The ANA creates Marketing Growth Champions by serving, educating, and advocating for more than 50,000 industry members that collectively invest more than \$400 billion in marketing and advertising annually. Our members include companies of all sizes, including small and mid-sized firms, virtually all of which rely on data-driven advertising practices that give consumers access to relevant information, messaging, and advertisements at the right time and in the right place.

The ANA advocates for the passage of a comprehensive, preemptive federal data privacy standard to provide rules of the road for businesses in all industries; by contrast, the proposed bills suggest that outlawing a specific advertising practice would offer the privacy protections Americans need. If passed, the proposed bills would virtually ensure that Americans lose access to the open Internet on which they depend to provide them with information, news, products, and services for free or at a very low cost; cripple the economy and stifle competition; and likely even violate bedrock First Amendment free speech protections. Congress should enact a data privacy law that provides a complete regime rather than banning a legitimate and constitutionally protected business practice. We therefore urge you to reconsider the proposed bills’ overly restrictive approach to advertising and instead adopt more well-balanced models for preemptive federal data privacy legislation, such as Privacy for America’s Principles for Privacy Legislation, which the ANA strongly supports.² We outline some of our significant concerns with the bills below.

- **Consumers Desire Relevant Advertising and Benefit from the Data-Driven Advertising Industry.**
Consumers can access practically limitless free and low-cost information and offerings through the Internet because of data-driven advertising. Without data-driven advertising, many online providers could be forced to shift to a subscription-based model where much of the online world would be accessible to a consumer only upon payment of a fee. An increase in subscription-based services (the predictable result of the proposed bills) would change the egalitarian nature of the Internet by which consumers of all economic

¹ Banning Surveillance Advertising Act of 2022, H.R. 6416, 117th Cong. (2022) (hereinafter, “Act”); see also S. 3520, 117th Cong. (2022).

² Privacy for America, Principles For Privacy Legislation, <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/> (hereinafter, “Framework”).

backgrounds can access content and offerings on a relatively equal basis. Understandably, consumers prefer today's Internet. A recent survey of consumer attitudes towards data-driven advertising found that consumers assign a value of over \$1,400 per year to virtually free content and information they access online due to data-driven advertising, and 88 percent of respondents stated they find advertising useful for finding new products.³ In addition, data-driven advertising generates jobs and supports Americans' livelihoods.⁴ For example, advertising supported \$2.1 trillion in Americans' salaries and wages in 2020, a figure that represents 18.2% of total labor income in the United States.⁵ As a result, a ban like the one proposed in H.R. 6416 and S. 3520 could threaten Americans' livelihoods and salaries at a time of significant economic stress.⁶

- **Data-Driven Advertising Allows Diverse Businesses to Reach Interested Audiences and Grow, Thereby Contributing to a Vibrant and Competitive Economy.** Data-driven advertising enables businesses of all sizes to reach current and potential customers with relevant messaging, services, and products efficiently and inexpensively. The practice helps today's small and start-up companies evolve into flourishing businesses that lend value to everyday Americans' lives. Additionally, nonprofits use advertising to solicit donations to further their charitable missions. Surveys show that 74% of small and mid-size entities believe that data-driven advertising is "important to the success of their business."⁷ These businesses rely on data-driven advertising to generate sales and revenue to a much greater degree than their larger business counterparts.⁸ A ban of the type contained in the proposed bills would cause many companies, including nonprofits and charities, that use data-driven advertising to reach audiences and compete to lose an essential method of making contact with existing and new customers. In turn, consumers' access to offerings would be severely limited and they would not benefit from receiving messaging and advertisements from a wide variety of firms. Small businesses would disproportionately shoulder these detrimental impacts. New businesses may never have the opportunity to get off the ground. Only the large, well-resourced companies that could afford to reach customers through means other than data-driven advertising would be able to function in the economy. A ban of the type that H.R. 6416 and S. 3520 propose could consequently lead to "more concentrated" control of the ad-supported Internet,⁹ where large companies could find a way to live with the ban, while smaller firms would likely die out or shut down due to a lack of customer acquisition and engagement.
- **A Private Right of Action Should Have No Place in Comprehensive Privacy Legislation.** The proposed bills would permit private litigants to bring lawsuits. We strongly believe private rights of action have no place in privacy legislation, and enforcement should be vested only in the Federal Trade Commission ("FTC") and/or state attorneys general. Including a private right of action in the proposed bills would not provide any real avenues for meaningful consumer redress but would be an unjustified windfall to the plaintiffs' bar. Additionally, a private right of action would discourage businesses from innovating for fear of potential expensive litigation costs. The possibility of a private lawsuit would force smaller companies to agree to settle claims to avoid "bet-the-company" litigation, even if such claims are entirely without merit.

³ Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at \$1,400/Year; Annual Value Jumps More Than \$200 Since 2016* (Sept. 28, 2020), located [here](#).

⁴ See generally IHS Markit, *The economic impact of advertising on the US economy 2018 – 2026* (Nov. 2021).

⁵ *Id.* at 11-12.

⁶ Annie Nova, "'6% inflation is devastating' to everyday Americans, rising prices need to be curbed, expert says," CNBC (Dec. 8, 2021), located at <https://www.cnbc.com/2021/12/08/6percent-inflation-is-devastating-to-americans-financial-expert-says.html>.

⁷ Deloitte, *Dynamic Markets: Unlocking small business innovation and growth through the rise of the personalized economy* at 2 (May 2021).

⁸ Digital Advertising Alliance, *Summit Snapshot: Data Drives Small- and Mid-sized Business Online, It's Imperative that Regulation not Short-Circuit Consumer Connections* (Aug. 17, 2021), located [here](#).

⁹ See e.g., John Deighton, *The Socioeconomic Impact of Internet Tracking*, IAB at 4 (Feb. 2020), <https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf>.

- **The Proposed Ban Runs Afoul of the First Amendment.** The United States Constitution protects a business's right to disseminate data and messages under First Amendment commercial free speech doctrine.¹⁰ For a law restricting commercial speech to pass constitutional muster, the state must assert a substantial interest in restricting the speech, the law must directly and materially advance that interest, and the law must be narrowly tailored to serve that interest.¹¹ The proposed bills assert no clear government interest through this draconian ban; they are also far from narrowly tailored but instead take the most severe approach possible by proposing to completely outlaw an otherwise legitimate and beneficial advertising activity. For these reasons, the proposed bills would almost certainly be vulnerable to legal challenges alleging violations of First Amendment commercial free speech protections. We therefore urge you reconsider the proposed bills' approach and instead adopt more balanced models for a preemptive, national standard for consumer privacy.
- **The Privacy for America Framework Model for Federal Privacy Legislation Offers a Preferable Preemptive and Comprehensive Approach.** H.R. 6416 and S. 3520 offer a blunt tool to regulate the highly nuanced subject of consumer privacy by affording no consideration to the benefits data-driven advertising provides to consumers, businesses of all sizes, and the economy at large. Because a flat ban on data-driven advertising would severely and detrimentally impact consumers and businesses alike, more balanced approaches should be considered to protect consumer privacy and preserve the benefits of advertising. The Privacy for America Framework ("Framework") is an example of an approach to regulating consumer privacy that prioritizes consumer protection while also allowing beneficial uses of data to power the economy and facilitate access to a vibrant online ecosystem. The Framework takes the approach of defining reasonable and per se unreasonable uses of personal information.¹² For other uses of personal information, the Framework calls on the FTC to exercise authority to issue regulations as needed to clarify permissible and impermissible activities based on specific criteria.¹³ The Framework also recognizes that some consumers may choose not to participate in certain data driven practices, and so individuals could opt out of some data-driven activity.¹⁴

* * *

Thank you for your consideration of this letter. We welcome opportunities to work with you and your colleagues to develop comprehensive preemptive privacy legislation. Please contact me with any questions or requests for assistance.

Sincerely,



Christopher Oswald | Executive Vice President, Government Relations
202.296.1883
coswald@ana.net | www.ana.net | @ANAGovRel

¹⁰ *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001); see also *Central Hudson Gas and Electric Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 566 (1980).

¹¹ See *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001); *Boetler v. Advance Magazine Publishers Inc.*, 210 F. Supp. 3d 579, 597 (S.D.N.Y. 2016); *Sorrell et. al. v. IMS Health Inc.*, 564 U.S. 552, 571-72 (2011).

¹² Framework at Part 1, Sec. 3.

¹³ Framework at Part 2, Sec. 2.

¹⁴ Framework at Part 1, Sec. 6.

Enhancing the FTC's Consumer Protection Authority to Regulate Social Media Companies

BY PAUL M. BARRETT AND LILY WARNKE

 **NYU STERN**

Center for Business
and Human Rights

February 2022

Table of Contents

Executive Summary	2
1. Introduction	3
2. General Principles	4
3. Policy Proposals.....	5
4. Conclusion	12

Authors

Paul M. Barrett is the deputy director of the NYU Stern Center for Business and Human Rights and an adjunct professor at the NYU School of Law.

Lily Warnke, a former fellow at the Center, contributed important research and analysis to this paper.

Acknowledgments

We are grateful to Craig Newmark Philanthropies and the Open Society Foundations for their continued support for our work on the technology sector.

NYU Stern Center for Business and Human Rights
 Leonard N. Stern School of Business
 44 West 4th Street, Suite 800
 New York, NY 10012
 +1 212-998-0261
 bhr@stern.nyu.edu
 bhr.stern.nyu.edu

© 2022 NYU Stern Center for Business and Human Rights
 All rights reserved. This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License. To view a copy of the license, visit:
<http://creativecommons.org/licenses/by-nc/4.0/>.



To reduce the level of hate speech, health misinformation, incitement to political violence, and other forms of harmful content spread by social media platforms, Congress should pass legislation to achieve the following goals:

- Enhance the consumer protection authority of the Federal Trade Commission and direct the agency to conduct sustained oversight of social media companies.
- Empower the FTC to enforce a new mandate that the companies maintain procedurally adequate content moderation systems, which deliver on promises made to users about platform rules and enforcement practices.
- Direct the agency to enforce new transparency requirements, including that social media companies disclose how their algorithms rank, recommend, and remove content, as well as information about the kind of content that reaches large audiences and the factors that cause such content to “go viral.”
- Oblige social media companies to maintain comprehensive, searchable advertising libraries, which disclose who has paid for each ad.
- Respect the First Amendment by prohibiting the FTC from any involvement in substantive content decisions, including decisions to take down or leave up content.
- Amend Section 230 of the Communications Decency Act of 1996 to clarify that its terms do not shield social media platforms from FTC enforcement actions or from private civil claims related to categories of particularly harmful content for which Congress determines platforms must be held accountable.

1. Introduction

Congress is considering dozens of bills designed to rein in social media platforms such as Facebook, Instagram, YouTube, and Twitter. The profusion of proposed legislation reflects a broadly held view that the companies that own these platforms have failed to self-regulate adequately. This failure has resulted in the amplification of misinformation, hate speech, incitement of political violence, and other harmful content. By intensifying the extreme polarization that now characterizes U.S. society, the platforms are undermining trust in elections and public health policies and blurring the distinction between provable facts and ideologically motivated falsehoods.

Remarkably, no arm of the federal government exercises sustained oversight of the social media industry in the way that the Federal Communications Commission regulates television and radio and the Securities and Exchange Commission oversees equity markets. In congressional testimony in the fall of 2021, Facebook whistleblower [Frances Haugen compared](#) the current regulatory environment for social media to “the Department for Transportation regulating cars by watching them drive down the highway.”

While most lawmakers apparently agree that something must be done about the malign effects of social media, there isn’t a consensus on how to proceed. The surfeit of legislative proposals reflects clashing motivations and competing regulatory strategies.¹

But even in what promises to be a rancorous midterm election year, there is an opportunity to move past overheated rhetoric and make progress on real reform. This paper does not endorse any specific legislation, although we refer to a number of bills that contain worthy ideas. The [Digital Services Oversight and Safety Act](#), for example, would create an appropriately staffed and funded digital bureau within the Federal Trade Commission to regulate the social media industry.

What follows are principles and policy goals intended to clarify the debate in Congress and shape an agenda for the FTC. We recommend that Congress direct the FTC to oversee the social media industry under the consumer protection authority that the agency already exercises in its regulation of other industries. Specifically, the agency ought to have the ability to require social media companies to maintain procedurally adequate content moderation policies and procedures, which deliver on promises made to users. Legislation also should authorize the FTC to require these companies to disclose information about how they rank, recommend, and remove content, as well as about the kind of content that reaches large audiences and the factors that cause such content to “go viral.” If applied prudently, this model for fostering transparency in the service of greater accountability could reduce the harms currently caused by a powerful and pervasive industry. All of this must be accomplished with due respect for the First Amendment’s prohibition of government speech restrictions.

Definitions

- **“Social media platforms”:** We are referring to social-networking sites like Facebook, Twitter, and Reddit, where users can post content and interact with other users; video-sharing services like YouTube and TikTok; and WhatsApp and other messaging services. We are *not* addressing search engines, such as Google, or online marketplaces, such as Amazon which, in our view, present distinctive problems that deserve separate legislative attention.
- **“Large platforms”:** Complying with some of our regulatory proposals would be onerous for smaller platforms with limited resources. To avoid inadvertently squelching innovation and further entrenching industry giants, Congress should limit application of these new regulations to large platforms, which lawmakers should define using a combination of factors, including number of monthly users, annual revenue, and workforce size.

¹ While grandstanding has eclipsed legislating in the U.S., the European Parliament in January approved a broad [Digital Services Act](#) that seeks to accomplish the kind of transparency and accountability we advocate in this paper. The DSA could take effect later in 2022, after negotiations between the Parliament, European Union member states, and the European Commission.

2. General Principles

Our policy proposals rest on the following principles:

- **Protecting free speech:** The [First Amendment to the U.S. Constitution](#) prohibits government restriction of social media users' online speech. It also forbids official interference with the choices social media companies make about which content to host—a protection similar to that enjoyed by a newspaper in its editorial choices. Our proposals are grounded in deep respect for this wise constitutional limit on government power. At the same time, the likelihood that even the most painstaking effort to regulate social media will elicit claims of First Amendment violations should not shut down discussion of potential reforms.
- **Imposing *procedural*, not substantive regulation:** To mitigate free-speech concerns, enhanced regulation should impose procedural, not substantive, obligations on social media companies. Apart from enforcing prohibitions on conspiracy, fraud, and other unlawful speech, the government should not make decisions about what content platforms host or amplify. Instead, legislation should require that if large platforms maintain content moderation systems, they include clearly explained rules, enforcement mechanisms, and means for appealing decisions. The platforms would continue to determine the substance of their content moderation systems. The FTC would ensure that once such systems exist, they have the human and automated resources needed to uphold the rules that platforms have promised users they will apply. In addition, the agency would oblige platforms to disclose key aspects not only of when and how they remove certain content, but also how they rank and recommend it for users.
- **Protecting consumer interests:** Building on the FTC's existing consumer protection authority offers the most promising strategy for reducing harms associated with social media.² [Section 5 of the Federal Trade Commission Act](#) provides the FTC with authority to stop acts or practices that are “unfair or deceptive” to consumers. Congress should pass legislation that defines the failure to maintain a procedurally adequate content moderation system as an unfair practice and therefore one that is unlawful. The legislation likewise ought to make clear that failure to disclose key aspects of the ranking, recommending, and removal of content constitutes a deceptive practice under Section 5. While U.S. legal concepts provide ample foundation for what we have in mind, the proposed [Digital Services Act](#) approved by the European Parliament in January 2022 provides complementary ideas about transparency and accountability.
- **Incentivizing industry vigilance:** It would have been preferable for social media companies themselves to have adequately policed the spread of harmful content, without government intervention. Voluntary self-regulation minimizes potential First Amendment complications. But the industry has not regulated itself sufficiently, necessitating action by Congress and the FTC. Still, the procedurally oriented consumer protection model we advocate will succeed only if social media companies commit to establishing and enforcing more stringent standards and procedures for removing and down-ranking harmful content. As a practical matter, only the companies themselves have the technological capacity to filter the billions of items their users post every day. Large mainstream tech companies, including Meta, which owns Facebook, Instagram, and WhatsApp, and Google, the owner of YouTube, already feature extensive moderation systems. Mainstream platforms know that without these systems they would be inundated by spam, pornography, hate speech, and other forms of unwelcome content that would drive away users and advertisers alike. To protect their business interests, the platforms will continue to moderate content on a large scale. The purpose of government oversight is to ensure that they do so more transparently and effectively.

² Mark MacCarthy, a senior fellow at the Institute for Technology Law and Policy at Georgetown Law School, has [trenchantly analyzed](#) the consumer protection approach to regulating content moderation.

Disclaimers

- **Limits of this paper:** Our proposal for enhanced FTC consumer protection does not address other potentially important avenues of reform. These include efforts to [update and strengthen antitrust enforcement](#), [shield user privacy](#), and [prevent various harms to children and teenagers](#). These topics deserve urgent attention and are the subject of a number of pending bills. But they are beyond the scope of this paper.
- **Fear of government overreach:** Skeptics of enhanced FTC oversight may raise the potential danger that a president could use the agency to punish social media companies and censor free speech. Would one want a politically appointed FTC chairman harassing Facebook, YouTube, or Twitter at the behest of a president who believes he has been wronged by the platforms? Not any more than one would want a vengeful president setting enforcement policy for the Internal Revenue Service, commanding the military, or exercising any of the other awesome powers entrusted to the nation's chief executive. But the possibility that regulatory authority, or other powers, might someday be abused can't be a determinative argument against providing a federal agency with the ability to accomplish its mission—in this case, consumer protection in a fast-evolving information marketplace.

3. Policy Proposals

The nature of the problem

All large tech platforms already publish extensive content moderation standards and policies for enforcing them. Unfortunately, the standards are both prolix and cryptic, often confusing, and sometimes downright misleading. Enforcement ranges from overly broad to feeble to haphazard, especially in languages other than English.³

The sheer scale of social media traffic—billions of posts each day, in scores of languages—means that no system will provide perfect filtering. Some harmful content inevitably will surface and spread. But this problem of scale is one of the industry's making. In a short span of years, Mark Zuckerberg, the founder and CEO of Meta, and other social media moguls stressed growth at all costs without incorporating adequate safety precautions.

The consequences are now familiar: Facebook groups kindle baseless claims of a “stolen” election and calls for a violent revolt, fueling the [January 6 insurrection](#). YouTube provides “[one of the major conduits of online disinformation and misinformation worldwide](#),” amplifying hate speech against vulnerable groups, undermining vaccination campaigns, and propping up authoritarians from Brazil to the Philippines. Twitter fosters a “[disinformation-for-hire industry](#)” in Kenya, stokes civil war in Ethiopia, and spreads “fake news” in Nigeria.

We see the industry's malign effects, but we know very little about how its technology works or the choices company executives make. Social media companies offer transparency reports, but these turn out to be highly curated collections of [often-manipulated and unrevealing data points](#). Social media remains a black box.

Consider “engagement.” The major platform companies have consciously designed the algorithms that rank and recommend content to prioritize posts that users will “like,” share, and comment on. These posts are more likely to go viral and, in a self-reinforcing feedback loop, are prone to be recirculated and otherwise engaged with by larger audiences. As various studies have shown, [users tend to engage with](#)

³ The detailed [decisions of the Facebook Oversight Board](#) provide numerous illustrations.

content that elicits anger and fear. As a result, ranking algorithms amplify this kind of sensationalistic and extreme content. Maximizing engagement increases partisan hatred, one group of researchers found, “in part because of the contagious power of content that elicits sectarian fear or indignation.” Social media companies boost user engagement, not because they want to intensify political polarization, but because the amount of time users spend on a platform interacting is also the amount of time they spend looking at the paid advertising that comprises the lion’s share of revenue for the major platforms.

“

Documents brought to light in the fall of 2021 by Facebook whistleblower Frances Haugen underscored that the platforms’ secrecy cloaks evidence that they are less effective than they would like to admit in filtering out harmful content.

”

But without access to the data, we don’t know the degree to which the algorithm designers and their corporate bosses seek to boost engagement. On rare occasions—for instance, during the attempt by former President Trump and some of his supporters to undermine the November 2020 election—tech companies have announced adjustments they’ve made to lower levels of fear and indignation among users. But when the immediate crisis recedes, the algorithmic dials typically are turned back to their normal positions to once again rev up engagement.⁴ Even when social media companies publicly acknowledge their ability to fine-tune the content mix, they closely guard the specifics, with corporate spokespeople citing the need to protect trade secrets from prying rivals.

Documents brought to light in the fall of 2021 by Facebook whistleblower Frances Haugen underscored that this secrecy cloaks evidence that the platforms are less effective than they would like to admit in filtering out harmful content. All of the major platforms ban dehumanizing attacks on people based on race, gender, religion, and certain other protected categories. Trying to demonstrate its vigilance, Facebook boasts publicly that more than 95% of the hateful content it takes down is removed by automated filtering before a user or paid human moderator notices it. But that impressive-sounding take-down rate means less than executives would have you believe. It applies not to *all* hate speech on the platform, but only to the offending content *that Facebook detects*. So, that’s 95% of—well, we have no idea, because Facebook doesn’t disclose the extent of hate speech on the platform. According to *one of Haugen’s leaked documents*, the company’s own analysts “estimate that we may action as little as 3-5% of hate...on Facebook.” Little wonder that Facebook has stoked extremism and violence in countries ranging from the U.S. to Myanmar and Ethiopia.

A realistic response to the problem

The most effective way to diminish social media’s tendency to amplify harmful content would be for the companies to replace their engagement-based business model. They could, for example, try selling subscriptions to users. But most users, conditioned to think of social media as “free,” probably would refuse to pay.⁵ Advertising would plummet; social media sites would shrivel.

Tech companies have shown no interest in sacrificing a large percentage of their revenue in a public-spirited attempt to reduce harmful content. And the government cannot force them to do so. The First Amendment would prohibit an order from Washington that social media companies change their fundamental strategy to alter the mix of content they host. Apart from free-speech concerns, a bipartisan fear of losing Silicon Valley financial support would make such an order politically infeasible.

Instead, what government can do is take measured steps under the familiar banner of consumer protection to shield social media users, and society at large, from the consequences of harmful content.

⁴ After the 2020 election, when President Trump and his supporters spread falsehoods about rogue ballots and fixed voting machines, Facebook made adjustments to calm the tone and content of users’ News Feeds. But in mid-November, a company vice president told journalists that the algorithmic changes would be reversed. See *An Ugly Truth* by New York Times reporters Sheera Frenkel and Cecilia Kang (<https://www.harpercollins.com/products/an-ugly-truth-sheera-frenkelceilia-kang?variant=32999376551970>).

⁵ In fact, users already pay—with their attention, as well as personal data on buying tendencies, political leanings, and web-surfing history.

These real-life consequences include the vicious and sometimes violent conduct incited by hate speech; the erosion of trust in elections caused by political disinformation; and the mass illness and death, as well as economic and educational disruption, exacerbated by misinformation about pandemic-era public health policies.⁶

These steps would not eliminate the harmful side effects of social media use. The enormous scale of the major platforms makes it difficult to imagine, let alone implement, systems that would comprehensively prevent the spread of harmful content. What Congress can do is seek modest but meaningful reform by augmenting the FTC's consumer protection authority.

Transparency and accountability

It is difficult to chart a regulatory course in the dark. This remains true even in the wake of the Frances Haugen revelations. To paraphrase Donald Rumsfeld, when it comes to social media, there are things we know we don't know, and then there are the *unknown unknowns*—things we're not even aware we don't know. By requiring the industry to divulge more of its currently secret data—with stringent safeguards to protect user privacy and forestall government misuse of the information for surveillance purposes—regulation could help outside researchers better understand and describe the harmful effects of social media, which in turn, would assist policymakers in crafting more effective responses.

Voluntary attempts to facilitate independent social media research have sputtered. In one program known as *Social Science One*, Meta gave researchers access to a large batch of internal information, only to announce in the summer of 2021 that the dataset had significant errors. In another incident last year, Meta cut off the personal accounts of NYU researchers and *shut down their study* of how misinformation spreads via political advertising on the platform.

Karen Kornbluh of the German Marshall Foundation and Ellen Goodman of Rutgers Law School have argued that, as a society, we need to *demand of social media what has been required of other industries* ranging from pharmaceuticals to airlines to chemicals: “These include responsibilities to disclose information, to demonstrate the safety of their products, to mitigate harm, and to comply with their own promises.” The European Union, which is several steps ahead of the U.S. in formulating regulatory strategy for social media, has emphasized similar ideas in its proposed *Digital Services Act*. The DSA would oblige large platforms to reveal more about their content-recommendation systems, allow independent audits of their risk-management efforts, and share key data with outside researchers, among many other provisions.

Fortifying the FTC's consumer protection authority

The FTC already has experience investigating unlawful practices by major social media companies and enforcing settlements requiring changed corporate behavior and payment of penalties. These cases generally have grown out of one-off investigations of privacy violations, rather than as part of a systematic exercise of industry-wide oversight authority.

In 2019, Facebook, now part of Meta, agreed to pay \$5 billion and change certain company practices to *settle FTC charges* that it violated an earlier agency order and deceived users about their ability to control the privacy of their personal information. The case grew out of the scandal involving Cambridge Analytica, a British data analytics firm that Facebook admitted had improperly harvested and saved user information. In a separate 2019 settlement, Google agreed to pay \$170 million to *resolve allegations by the FTC* and the New York Attorney General that its YouTube subsidiary illegally collected personal information from child users.

⁶ The term “disinformation” refers to intentionally false or misleading information intended to sow divisiveness and confusion. “Misinformation” refers to such content created or spread by people who may not understand that it is untrue. In either case, the false content may be intermingled with truthful statements, making it seem more credible.

Expanding its reach beyond these privacy cases, the FTC should rely on its consumer protection authority to oversee the social media industry on an ongoing basis. To clarify the appropriateness of this application of Section 5 of the FTC Act, and to strengthen the agency's position in federal court litigation, Congress needs to direct the agency explicitly to use its consumer protection authority in this manner.

“

The FTC already has experience investigating unlawful practices by major social media companies and enforcing settlements requiring changed corporate behavior and payment of penalties.

”

Section 5(a) protects consumers by providing that “unfair or deceptive acts or practices in or affecting commerce” are unlawful. An unfair act is one that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” Deceptiveness involves “a material representation, omission, or practice that is likely to mislead a consumer acting reasonably in the circumstances.” In a consumer protection ruling in 2015 that favored the FTC, the [U.S. Court of Appeals for the Third Circuit](#) observed that, as a practical matter, “facts relevant to unfairness and deception frequently overlap.”

To further fortify the FTC's authority, Congress should clarify how the agency's enhanced authority comports with existing elements of a

Section 5(a) violation. The “substantial injury” in question is users’ unwelcome exposure to harmful content that has real-world consequences: violence based on religious animus, racial discrimination, doubt cast on elections, misinformation that erodes public health policies, and so forth. This kind of substantial injury is not “reasonably avoidable,” short of consumers avoiding social media entirely.⁷

Addressing the possibility of “countervailing benefits to consumers or to competition,” Congress could concede that some consumers might prefer digital communication unfettered by content moderation, but the sort of restrained FTC oversight proposed here would not impinge on this interest. The government would not propose substantive content rules or enforce such rules; these would remain under the control of the social media companies. The government's purview would be strictly limited to superintending procedural adequacy and data disclosure. As for the effects on competition, the safe harbor provisions discussed earlier in this paper, which would limit the reach of regulation to companies whose revenue, user headcount, and workforce exceed certain thresholds. This would protect against inadvertent economic harm to smaller rivals of the large platforms.

In similar fashion, Congress ought to underscore that, while the FTC has traditionally focused on marketplace “injuries” measured in dollars lost or physical harm, the analysis for social media needs to be different. It should encompass more intangible forms of injury—such as, psychological trauma and erosion of free and fair elections—which are associated with an unusually pervasive form of technology.

Although platform companies don't receive monetary payment from users, there is a merchant-consumer relationship justifying application of consumer protection law. “Facebook takes its users’ time, attention, and personal data; in exchange, Facebook gives those users access to and use of Facebook's social network, which Facebook itself deems a ‘product.’” This apt analysis came from a [trio of consumer-advocacy organizations](#) in a December 2021 friend-of-the-court brief supporting a pending lawsuit against Facebook in the Superior Court of the District of Columbia.⁸

If Congress determines that a broader or different definition of unfairness or deceptiveness under Section 5(a) is needed to undergird specific statutory authority for FTC regulation, lawmakers could expand the reach of these concepts based on the novel challenges posed by social media.

⁷ It's worth pointing again to Mark McCarthy's [paper on regulating content moderation](#).

⁸ The pro-consumer groups Consumer Reports, Public Knowledge, and Uptum filed their amicus brief in support of Muslim Advocates, an organization that sued Meta.

Applying consumer protection standards to social media platforms

To oversee new requirements concerning social media, Congress should create a Bureau of Digital Services Oversight and Safety within the FTC and appropriate annual funding sufficient for the bureau to undertake its challenging mission.⁹ The FTC is relatively small and already stretched to the limit by the demands of its existing antitrust and consumer protection duties, including its ongoing [monopolization lawsuit against Facebook](#).¹⁰ To respond to the inevitable industry legal challenges to new regulation and to ensure the effectuation of congressional intent, the FTC's budget must expand. President Biden's stalled Build Back Better bill contained [\\$500 million in additional annual FTC spending](#). Something in that ballpark seems appropriate, given the scale of the industry and its negative effects on consumers.

The FTC's digital bureau would oversee the procedural adequacy of content moderation and new data-disclosure requirements:

Procedurally adequate content moderation: Congress should define procedurally adequate content moderation as a system based on clearly articulated rules, enforcement practices, and mechanisms for user appeals. Failure to meet these requirements, as determined by the FTC, would constitute unfair or deceptive acts or practices and be grounds for agency enforcement action. FTC enforcement could entail administrative proceedings or civil litigation seeking a federal judicial injunction and potential monetary penalties. In a significant April 2021 ruling, the Supreme Court [limited the FTC's ability to seek monetary relief](#) in federal court for violations of the FTC Act. Congress needs to clarify that the agency has this statutory authority. The legislation also should make clear that new federal mandates don't preempt application of state consumer protection standards.

As noted, Congress and, in turn, the FTC must frame the new oversight as procedural, not substantive. To mitigate First Amendment complications, legislation should ban the FTC from telling platforms what substantive moderation rules to establish, let alone dictate particular decisions about content. Social media companies would retain full First Amendment protection to determine what they host on their sites. Users' speech would not be subject to government restriction. By forbidding FTC involvement in crafting or applying substantive content standards, Congress can squarely position the agency's oversight as a form of consumer protection, not unlike the FTC's policing of loans with hidden fees or misleading product warranties that don't cover commonly needed repairs.¹¹

This procedural approach would not provide the proverbial silver bullet for harmful content. Platforms would not be obliged to moderate content aggressively. Sites like [Gab](#), [Parler](#), and [Rumble](#), which market themselves as imposing few limits on users and have become havens for right-wing conspiracy theorists, would not necessarily have to change their policies. But they would have to maintain moderation systems sufficient to deliver on the promises they have made to users.

While not a panacea, a requirement of procedural adequacy would nevertheless be meaningful. Social media companies would have to follow through on assurances they make in their community standards and terms of service. They would do this by providing clear rules, easily understood enforcement procedures, and ways for users to appeal moderation decisions. As a practical matter, mainstream social media companies are extremely unlikely to eliminate or even significantly roll back the extensive—but nevertheless inadequate—moderation systems they currently operate. Doing so would lead to inundation by spam, pornography, hate speech, and other unwelcome content that would drive away users and advertisers.

⁹ We borrow the name from the recently introduced [Digital Services Oversight and Safety Act](#). Another bill, the [Algorithmic Accountability Act](#), also would create a digital bureau that would oversee newly mandated self-assessment and disclosure by social media companies and other firms that rely on automated decision making. The latter legislation would reach beyond content moderation to cover a wide range of "critical decisions" concerning health, finance, housing, and education.

¹⁰ According to the advocacy arm of Consumer Reports, the size of the American economy has tripled since 1979, while the FTC's capacity has decreased 37%.

¹¹ The bipartisan [Platform Accountability and Consumer Transparency Act](#) contains useful language on ensuring that the FTC plays a purely procedural role.

FTC oversight would force tech companies to clarify moderation policies and practices that are often opaque and contradictory. Facebook’s quasi-independent [Oversight Board](#) repeatedly has urged Facebook to make it easier for users to understand [why posts were taken down \(or left up\) or accounts were removed](#). At present, this is frequently impossible, in part, because Facebook [keeps many guidelines used in content decisions secret](#).

“
To mitigate First Amendment complications, legislation should ban the FTC from telling platforms what substantive moderation rules to establish, let alone dictate particular decisions about content.
”

The new digital bureau should also look into the adequacy of how human content reviewers do their jobs, including how their determinations relate to the far larger body of decisions driven by artificial intelligence. One potentially fruitful line of inquiry would be whether the widespread practice among social media companies of outsourcing human content review diminishes the quality of that crucial work. Based on [research by our Center](#), we have advocated bringing currently outsourced reviewers into social media companies as direct employees who would be more likely to receive effective training, supervision, and mental health counseling, in light of their exposure to traumatizing online material.¹²

Mandated data disclosure: The other main goal of FTC oversight should be the disclosure of currently nonpublic information about how content moderation actually works. This would include how platform algorithms rank, recommend, and remove content, as well as information about the kind of content that reaches large audiences and the factors that cause such content to go viral. These disclosures would help users and advertisers make better-informed choices about which platforms to patronize. Researchers and policymakers would gain insights that point to possible further reform.

Disclosure of data on the influence of algorithms, for instance, could help reveal whether certain harmful content is reaching a wide audience because users are searching for it, platforms are ranking it prominently in user feeds, or recommendation engines are urging particular users to view it. Openness about the mechanics of content amplification might lead to public pressure for platforms to ease their algorithmic drive for user engagement and thereby diminish the spread of hateful, sensationalistic, and patently false content. The FTC-enforced transparency requirements included in the [Digital Services Oversight and Safety Act](#) would go a long way toward achieving these aims.

Congress and, in turn, the FTC should distinguish between disclosure requirements leading to information becoming entirely public versus data which, because of user-privacy concerns or the need to protect proprietary intellectual property, would become available only to regulators and qualified researchers. The [Digital Services Oversight and Safety Act](#) grapples with these distinctions, as does the narrower [Platform Transparency and Accountability Act](#). The latter legislation, which has bipartisan backing, would direct the FTC to require that tech companies provide data to certified outside researchers, subject to certain restrictions protecting user privacy. The FTC would work with the National Science Foundation to determine which inquiries proposed by outside researchers qualify; the companies would have no say. The legislation defines failure to comply with this data-sharing system as “unfair or deceptive” under Section 5(a) of the FTC Act. Disclosure for research purposes would complement the salutary effects of the [Honest Ads Act](#), bipartisan legislation that would make digital political advertising subject to the same transparency obligations now imposed on broadcast political ads.

Lessons from corporate cyber-security cases

Since 2000, the FTC has litigated or settled dozens of enforcement actions against companies that promised customers they would maintain reasonable information-security protections and then failed

¹² The FTC also could mandate disclosure of the size of human moderation workforces and require allocation of sufficient resources to operate moderation systems commensurate with the scale of large platforms.

to do so. Customers whose personal and financial data were exposed by digital breaches were subject to significant potential harm and were not in a position to protect themselves.

A 2015 case involving the Wyndham hotel chain provides an example. The FTC sued Wyndham, alleging that the company's data-security failures led to breaches resulting in millions of dollars of fraudulent charges on consumers' credit and debit cards. Wyndham fought the suit, arguing that the alleged lapses didn't amount to an "unfair" commercial practice. Clearing the case for trial, the U.S. Court of Appeals for the [Third Circuit](#) ruled that the FTC had identified overlapping elements of unfairness and deceptiveness in the hotel chain's conduct: "A company," the court said, "does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."

Analogously, a social media company does not act equitably when it publishes a content moderation policy to attract users concerned about exposure to hate speech, misinformation, and violent incitement; fails to make good on that promise by maintaining a procedurally inadequate moderation system and thereby exposes unsuspecting users to harmful content; and retains the profits derived from digital advertising targeting those users. (In the Wyndham case, the hotel chain ultimately [settled](#), agreeing to maintain a comprehensive information-security program.)

A final word on the First Amendment

Confronted with enhanced oversight by the FTC, deep-pocketed social media companies will file First Amendment court challenges. If the judiciary responds by categorizing the regulation as an exercise of consumer protection, it ought to survive. But if courts see regulation of social media as an indirect attempt to restrict expressive content, they will subject it to "strict scrutiny," which is typically fatal for the government action in question. To survive, a challenged regulation must promote a "compelling government interest" in a "narrowly tailored" manner.

The compelling interest in this case is protecting consumers from unfair and deceptive practices that engender unwanted hateful speech and conduct, political disinformation and erosion of democratic norms, and incitement of political violence. Narrow tailoring is seen in the regulation's emphasis on procedural rather than substantive requirements. Mandatory data disclosure for research purposes is analogous to constitutionally sound data demands the government makes of a vast array of industries in the name of customer safety and product effectiveness.

Social media companies also would attack new regulation as disfavoring them in comparison to traditional news organizations. But this distinction is justified. With some exceptions, *The New York Times* makes a specific decision about each piece of expressive content it places on its website or in its print edition. In contrast, social media platforms are designed so that they can host billions of user-generated posts that appear almost instantaneously and typically without human review. Social media technology created a novel challenge in the potential for harmful content to go viral with dire real-world consequences. Social media companies have responded by building moderation systems, but these systems routinely fall short. This situation necessitates the kind of judicious, non-content-based government oversight we propose.

Section 230

For nearly five years, the congressional debate about regulating social media companies has revolved around [Section 230 of the Communications Decency Act of 1996](#). Revising the 26-year-old provision is not a centerpiece of our policy recommendations, but it deserves mention as an adjunct to enhanced FTC oversight. In brief, we urge Congress to curtail Section 230 in order to incentivize companies to increase their vigilance in moderating forms of hateful content that have proven particularly dangerous.

Section 230 protects providers of “interactive computer services” from being sued over content posted by users or moderation decisions concerning such content. This liability shield has encouraged social media companies to give users wide latitude in what they post without being held legally responsible for the consequences. The second part of the provision provides yet more protection, holding platforms harmless for decisions to take down content or leave it up. Defenders of Section 230 contend, rightly, that it helped the social media industry get aloft in the 2000s and that even today it benefits smaller sites that lack the resources to defend against costly lawsuits. Critics of the law observe, correctly, that its authors couldn’t have anticipated the rise of leviathans like Facebook and Google or the volume of toxic content they spread. These giants, the critics add, now hide behind Section 230 when faced with legitimate allegations that this toxic content has caused real-world damage.

Our view is that Section 230 still fosters free-wheeling expression. It plays an important role shielding platforms—ranging from the user-generated encyclopedia Wikipedia to consumer-review site Yelp—that might otherwise have trouble surviving if confronted by waves of litigation. On the other hand, blanket application of Section 230 to the benefit of Facebook or Google, with their bottomless legal budgets, seems problematic. Legislation should address two goals:

- **Clarify that Section 230 is not a defense against FTC enforcement:** When seeking to hold platforms responsible for protecting consumers by sharing data and/or maintaining procedurally adequate moderation systems, the FTC should not encounter a Section 230 wall.
- **Remove the liability shield for claims related to certain harms:** Several pending bills “carve out” exceptions to Section 230 for suits based on specified types of harmful content.¹³ The [Protecting Americans Against Dangerous Algorithms Act](#), for example, would lift liability protection for suits alleging involvement in foreign or domestic terrorism. It would apply only when such suits point to algorithmic amplification of harmful content, as opposed to chronological ranking or search results. The [SAFE TECH Act](#) would remove the shield for suits involving ads and other paid content, stalking, harassment, and civil rights violations. Congress could adopt all or some of the carve-outs found in these two bills. We agree with the authors of the dangerous algorithms act that carve-outs ought to come into play only in suits alleging that automated systems have amplified harmful content.¹⁴

4. Conclusion

With dozens of competing bills pending in the House and Senate, it isn’t clear which ones will make headway at the committee level or whether congressional leaders will make room on the legislative calendar for floor debate. Still, reining in social media—*somehow*—is the rare issue on which there is some real momentum on both sides of the aisle. It would be a shame if the profusion of legislative proposals went totally for naught.

Our hope is that the ideas in this paper will help clarify the legislative debate and subsequently shape FTC action—if not this year, then eventually. Online consumer protection is the sort of goal that ought to attract support on both sides of the aisle. But even if the extreme polarization of the moment—exacerbated, not incidentally, by social media—continues to hinder progress in the short run, the need for digital regulation will persist. Sooner or later, we will have to come to grips with the societal toll this alluring technology has taken.

¹³ Several carve-outs to Section 230 are already incorporated into the law: Platforms are legally responsible for civil claims related to federal crimes, sex trafficking, and intellectual property violations.

¹⁴ The [Justice Against Malicious Algorithms Act](#) employs a roughly similar mechanism, removing Section 230 protection when a platform “knowingly or recklessly” promotes harmful content.



February 28, 2022

The Honorable Jan Schakowsky, Chair
 The Honorable Gus Bilirakis, Ranking Member
 Subcommittee on Consumer Protection and Commerce
 Committee on Energy & Commerce
 U.S. House of Representatives
 2125 Rayburn House Office Building
 Washington, DC 20515

Re: Hearing on “Holding Big Tech Accountable: Legislation to Protect Online Users”

Dear Chair Schakowsky, Ranking Member Bilirakis, and Members of the Subcommittee:

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide input on the bills that will be addressed at the Subcommittee’s March 1 hearing, *Holding Big Tech Accountable: Legislation to Protect Online Users*.

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services.

SIIA’s comments focus on two of the five bills listed for that hearing: H.R. 6580, the “Algorithmic Accountability Act of 2022” (AAA), and H.R. 6416, the “Banning Surveillance Advertising Act of 2022” (BSAA). These comments are intended to reflect high-level input on the AAA and BSAA. They do not reflect the totality of our comments and we would welcome the opportunity to discuss both bills in further detail with you and your staff.

Comments on H.R. 6580 – The Algorithmic Accountability Act of 2022

We are pleased by the introduction of the AAA. The bill reflects a serious engagement with the challenging issues presented by artificial intelligence (AI) in a range of private sector activities. We believe the focus on impact assessments for the most high-risk applications of automated decision making is an important step towards fostering responsible, trustworthy, and ethical AI while protecting innovation. Importantly, automated decision systems have the potential to improve fairness outcomes over existing human-based-decision processes and any rules should support the development of these systems.

The use of impact assessments is widespread in the private sector, particularly among those companies that would be considered “covered entities” under the AAA. We believe that any statutory framework should complement efforts currently underway, such as the efforts by the National Institute of Standards and Technology (NIST) to create a framework for trustworthy AI, and provide guidance not only to the

private sector but to the Federal Trade Commission (FTC) and other federal agencies that will have a role in any regulatory framework that arises out of the AAA.

We provide the following comments in a spirit of improving the legislation as it proceeds through the House. We believe the edits proposed will help to foster innovation and minimize the regulatory burden on companies, support the overarching goals of protecting individuals, improve outcomes relative to existing human-based processes for sensitive decisions, ensure a more efficient allocation of limited government resources and technical expertise, and support regulatory interoperability.¹

1. Incorporate an Explicit Risk-Based Framework for Categorizing Automated Decision Systems

The global nature of the innovation economy and the real possibility that foreign jurisdictions and non-federal jurisdiction in the United States may enact binding rules before the U.S. government does underscore the importance of Congress advancing a framework that is compatible with terminology and accepted best practices. The breadth of work on risk-based approaches to managing automated decision systems means that a legislative framework taking a different approach or using unique terminology could generate challenges for regulatory interoperability.

Because of this, we recommend amending the AAA to incorporate a risk-based framework for regulating automated decision systems. While we appreciate the distinction between systems used to render “critical decisions” and systems used in other manners, we believe, following a growing literature of practice and expert analysis in this area, that a risk-based framework is critical to improve regulatory interoperability, promote development of responsible AI, minimize implementation challenges for the government and private sector alike, and provide stronger and more meaningful protections to individuals.

A risk-based framework recognizes that automated decision systems present different risks depending on where, when, and how they are used; the level of human judgment involved in their application; the potential impact of systems on individuals; and the development stage of the system. A risk-based framework has broad consensus among academics, civil society, private industry, and lawmakers who have grappled with the challenges of automated decision making.² This is the approach being taken by NIST, which has embarked on an ambitious, expert-driven process to establish a risk management framework for AI that reflects input from a range of stakeholders, including from across the interagency and the general public.³ It also forms the core of the proposed Artificial Intelligence Act under

¹ The carve out for “passive computing infrastructure” (section 2(13)) is too limited to address this concern. The bill defines “passive computing infrastructure” to exclude any intermediary technology that influences a decision – even if the decision is ultimately made by a human.

² See, e.g., OECD, [Framework for Classification of AI Systems](#) (Feb. 22, 2022); Future of Privacy Forum, [Automated Decision Making Systems: Consideration for State Policymakers](#) (May 12, 2021); Ada Lovelace Institute, [Regulation to innovate](#) (Nov. 2021).

³ See NIST, [AI Risk Management Framework Concept Paper](#) (Dec. 13, 2021); NIST, [A Proposal for Managing and Identifying Bias in Artificial Intelligence](#) (June 2021).

consideration in the European Parliament, efforts in Canada, and legislative efforts in several U.S. states.⁴ And, many SIIA members have already implemented measures to assess automated decision systems during development and use phases using risk-based frameworks.⁵

With this background, we consider the AAA to provide a framework for requiring impact assessments, summary reports, additional transparency measures, and training for “high risk” applications of automated decision systems – what the bill describes as “critical decisions.” Following are additional recommendations that we believe will help to focus the scope of the AAA to achieve this goal.

2. Focus the Definitions of “Automated Decision System” and “Augmented Critical Decision Process”

First, we recommend that the AAA focus on automated decision systems that render decisions without human input. As written, the AAA would include the use of automated decision systems that *assist* in human decision-making. Uses of systems in that way do not present the same level of risk as those that are rendered without human involvement. While there may be value in requiring impact assessments of certain such systems to minimize the potential for algorithmic bias in the systems relied on by humans, under a risk-based approach, those requirements should be tailored to the potential risk.

To address this, for high-risk applications—those that are used in rendering “critical decisions”—we recommend focusing the definition of “automated decision system” to apply to fully automated systems without a human in the loop. Including any decisions that utilize automated decision systems even if a human ultimately makes the decision—i.e., those without a human “check”—is likely to generate a significant volume of impact assessments and reporting that do not present the same heightened risk to individual legal rights that fully automated systems may present. This will lead to significant burdens on limited government resources as well as the private sector. Even a regulatory body with increased funding and staff will have difficulties assessing the potential reporting volume.

We believe this concern can be addressed with revisions to two definitions, as follows:

- | |
|--|
| (1) AUGMENTED CRITICAL DECISION PROCESS.—The term “augmented critical decision process” means a process, procedure, or other activity that solely employs an automated decision system to make a critical decision. |
| (2) AUTOMATED DECISION SYSTEM.—The term “automated decision system” means any |

⁴ See, e.g., European Commission, [Proposal for a Regulation laying down harmonised rules for artificial intelligence](#) (Apr. 21, 2021); Government of Canada, [Directive on Automated Decision Making](#) (Apr. 1, 2021) (cf. Government of Canada, [Algorithmic Impact Assessment Tool](#)); U.S. Food and Drug Administration, [Artificial Intelligence and Machine Learning in Software as a Medical Device](#) (Sept. 22, 2021); [California Assembly Bill 13: Public Contracts: automated decision systems](#) (last amended July 15, 2021).

⁵ See, e.g., Jared Council, [How Adobe’s Ethics Committee Helps Manage AI Bias](#), Wall Street Journal (May 5, 2021); Adobe, [Ethical Approach to AI](#); Google, [Building a responsible regulatory framework for AI](#).

system, software, or process (including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques) that **solely** uses computation (excluding passive computing infrastructure) to make, **facilitate, or inform** a decision or judgment.

In addition, we would urge a close review of the legislative text to ensure that the processes and procedures required of what we refer to as “high risk” systems are not applied more generally to all automated decision systems, as appears in several provisions within section 3(b). By way of example, the California legislature last year introduced Assembly Bill 13, which would distinguish between high and low risk automated decision systems and apply to systems that “substantially assist or replace human discretionary decisionmaking and that materially impacts natural persons.”⁶

3. Clarify the Definition of “Critical Decision”

Second, we recommend clarifying the definition of “critical decision” to align better with our current understanding of congressional intent, that is, on decisions that have a direct and potentially significant effect on legal or other material rights. The definition currently lacks a guiding principle and does not reflect how automated decision systems can be used in the categories listed in section 2(8) in ways that do not raise high-risk concerns. There are countless routine uses of automated decision systems that may “relate to” issues around access, cost, terms, and availability that have no material impact on legal rights, the availability of services, and anti-discrimination, such as systems used to change utility rates to reflect inflation and other fixed costs; models used by financial investors; and online travel booking tools. As others grappling with these challenges have recognized, automated decision systems that do touch on material rights may not always have significant impacts on those rights.⁷

We propose the following revision to section 2(7) to address this:⁸

(7) CRITICAL DECISION.—The term “critical decision” means a decision or judgment that has **any** **a direct** legal or similarly significant effect on a consumer’s life and relates to ~~access to or the cost, terms, or availability of~~ **eligibility determinations about or the cost or terms of --**

⁶ [California Assembly Bill 13](#). The notice for preliminary comments on the proposed rulemaking under California Privacy Rights Act of 2020 also included questions about how the legislature can tailor policy to a risk-based standard and the legislature is in the process of codifying this. SIIA comments can be found [here](#).

⁷ In this regard, the work done by Canada’s Treasury Board provides a worthwhile comparison. See Government of Canada, [Responsible use of artificial intelligence \(AI\)](#) (resource page); Government of Canada, [Directive on Automated Decision Making](#) (Apr. 1, 2021).

⁸ A similar approach is taken by the EU GDPR. Article 22 of the GDPR protects consumers from decisions “based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.” GDPR, [Art. 22](#).

4. Ensure Expert Involvement in the Development of Impact Assessment Requirements

We appreciate the AAA's mandate for the FTC to seek input from NIST, the National Artificial Intelligence Initiative (NAII), and the Office of Science and Technology Policy (OSTP).⁹ Given the expertise embedded in those agencies and their substantial work to date on the issues reflected in the AAA, we would urge Congress to create a greater role for those agencies in developing regulations to guide impact assessments for algorithmic decision making and a regulatory structure for reviewing those assessments and summary reports. Other agencies, such as the Department of Education, will be essential for understanding appropriate requirements for assessments on high-risk education technology systems.

We also encourage Congress to explicitly align the AAA with the risk-based framework that NIST is currently developing. As noted above, this effort benefits from deep engagement with experts within and outside of government. It represents the most comprehensive effort by the U.S. government to provide guidance to industry and is expected to be finalized in 2023.¹⁰ This approach also will enable the FTC to align rulemaking with state-of-the-art processes and procedures being incorporated already in the private sector to minimize bias and foster responsible, trustworthy AI.

5. Refine the Definition of "Biometrics"

In addition, we would urge Congress to revisit the AAA's definition of biometrics contained in section 2(3). This definition goes well beyond definitions in use in other jurisdictions. We advise the Subcommittee to compare this definition to the one in H.R. 6796, another bill that will be addressed at the March 1 hearing, and also to consider the points that SIIA has made in a recent submission to OSTP.¹¹

Comments on H.R. 6414 – The Banning Surveillance Advertising Act of 2022

To the extent that there is a concern about targeted advertising that occurs without transparency or user consent, we recommend proceeding through focused rulemaking or legislation around privacy and to prevent specific abuses. SIIA strongly supports a comprehensive federal privacy law that would address concerns about how consumer data is used, provide needed clarity for businesses and consumers alike, and foster a stronger innovation environment in the United States while maintaining our global competitiveness.

The BSAA does not come remotely close to meeting this standard. The scope of its proposed ban on "surveillance advertising", notwithstanding the carve out for "contextual advertisements," would prohibit a large amount of advertising on the internet that results from user-identified preferences and consent.

⁹ Sections 3(b)(1), 7(a); see also section 7(b)(3).

¹⁰ NIST has also proposed a model that shapes nine principles that can reaffirm user trust in artificial intelligence: accuracy, reliability, resiliency, objectivity, security, explainability, safety, accountability, and privacy. NIST, [Trust and Artificial Intelligence](#) (Mar. 2021).

¹¹ SIIA, [Comments on RFI for Public and Private Sector Uses of Biometric Technologies](#) (Jan. 14, 2022).

The internet of today and the free online services made available to consumers are reliant on advertising, including personalized or targeted advertising. Targeted advertising is a widespread practice and not one that is the exclusive domain of the large technology companies identified in the Petition. Indeed, numerous U.S.-based retailers have their own ad networks and ad tech. Disruption of that advertising will certainly cause damage to small- and medium-sized companies and consumer welfare. In a contextual-only world where advertisers are looking for the right context to target ads, publishers with the largest and most varied web presence will have the biggest range of context for advertisers to target. The inevitable result would be less revenue for smaller publishers and creators (such as bloggers, newsletter publishers, and video content creators) and developers who rely on ads for funding. This will in turn reduce the diversity of content available online as they find it difficult to find contextually relevant advertisers. The effect of what Accountable Tech is proposing would be to shut down large swaths of the internet, increase costs of consumers who would be forced to pay subscription fees to access services that they now enjoy for free, and require small and medium sized businesses to develop entirely new means to reach consumers.

In addition, we have significant concerns about the proposed inclusion of a private right of action. As seen in the context of private enforcement of state privacy laws, a private right of action for statutory damages can generate an enormous amount of litigation leading to costs that are passed on to consumers. The potential for litigation relating to online advertising is exponentially greater and we strongly urge Congress to hold hearings on this issue, and gather further input from the public, prior to proceeding with markup.

Conclusion

We appreciate your consideration of our views. We look forward to working with the Subcommittee members and staff as these bills proceed in Congress.

Respectfully submitted,



Paul Lekas
Senior Vice President, Global Public Policy
Software & Information Industry Association (SIIA)

FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

CATHY McMORRIS RODGERS, WASHINGTON
RANKING MEMBER

ONE HUNDRED SIXTEENTH 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

February 28, 2022

The Honorable Lina Khan
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Chairwoman Khan:

We are closely following the news of the discovery of vulnerability in the open-source software known as Apache Log4j. We are also aware that on January 4, 2022, the Federal Trade Commission (FTC) warned in a blog post that it “intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of the Log4j vulnerability, or similar known vulnerabilities in the future”¹.

We appreciate that you share our commitment to data security and hope this is a sign that your agency, the Biden Administration, and Congressional Democrats finally will support a bipartisan privacy and data security solution, much like Republican members of the Energy and Commerce Committee outlined in the “Control Our Data Act” last November. The “go-it-alone” approach that Democrats have followed since President Biden’s inauguration has either failed or contributed to severe, negative consequences. Despite the temptation, we encourage you to work with us instead of trying to contort existing FTC authorities to achieve your policy goals.

We also note that the Cybersecurity and Infrastructure Security Agency (CISA) recently warned federal agencies that their systems and systems they interface with may be exposed to

¹ Federal Trade Commission, *FTC warns companies to remediate Log4j security vulnerability* (Jan 4, 2022) available at: <https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability>

Letter to Chairwoman Lina Khan
Page 2

this vulnerability.² After the initial public disclosure, security researchers noticed nation-state threat actors, including China, Russia, Iran, North Korea, and Turkey, attempting to exploit the vulnerability. The Apache Software Foundation released a full solution to the Log4j vulnerability approximately two weeks after the disclosure.

On December 11, 2021, CISA Director Jen Easterly stated that “this vulnerability, which is being widely exploited by a growing set of threat actors, presents an urgent challenge to network defenders given its broad use.”³ She later added, “[t]o be clear, this vulnerability poses a severe risk. We will only minimize potential impacts through collaborative efforts between government and the private sector.”⁴

On December 17, 2021, CISA issued Emergency Directive (ED) 22-02 requiring federal civilian departments and agencies to assess their internet-facing network assets for the Apache Log4j vulnerabilities and immediately patch these systems or implement other appropriate mitigation measures.⁵ Additionally, the Federal Bureau of Investigation (FBI) asked organizations and agencies to report any compromises as the result of the Log4j vulnerability.⁶

Over the past several years, the Committee has done extensive work on cyber threats, including hearings and investigations examining the information security programs and controls over key computer systems and networks at multiple agencies under the Committee’s jurisdiction. Because the Log4j vulnerability is widespread and can affect enterprise applications, embedded systems and their sub-components, the Committee is seeking to gain a fuller understanding of the scope of the vulnerability and actions being taken to mitigate its effects. The risk to federal network security is especially concerning because nation-state threat actors have attempted to exploit this Log4j vulnerability.

Accordingly, please provide written answers and any necessary documentation to the following questions by March 7, 2022:

1. Does your agency employ Apache Log4j? If so, how many software products employed by the agency include the Log4j vulnerability?
2. How many of those software products have adopted the patch for the Log4j vulnerability?

² Cybersecurity and Infrastructure Security Agency, *Emergency Directive 22-02 Mitigate Apache Log4j Vulnerability* (Dec 17, 2021) available at: <https://www.cisa.gov/emergency-directive-22-02>

³ Cybersecurity and Infrastructure Security Agency, *Statement From CISA Director Easterly on “Log4j” Vulnerability*, (Dec 11, 2021) available at: <https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability>

⁴ *Id.*

⁵ Cybersecurity and Infrastructure Security Agency, *CISA Issues Emergency Directive Requiring Federal Agencies To Mitigate Apache Log4j Vulnerabilities*, (Dec 17, 2021) available at: <https://www.cisa.gov/news/2021/12/17/cisa-issues-emergency-directive-requiring-federal-agencies-mitigate-apache-log4j>

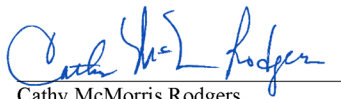
⁶ Federal Bureau of Investigations, *FBI Statement on Log4j Vulnerability*, (Dec 15, 2021) available at: <https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-log4j-vulnerability>

Letter to Chairwoman Lina Khan
Page 3

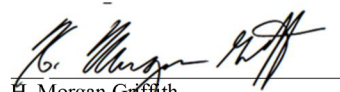
3. Do you know the number of recent downloads of Apache Log4j within your agency? Do these recent downloads of Apache Log4j contain the Log4j vulnerability?
4. What is your agency's schedule for identifying and mitigating any Log4j vulnerabilities?
5. Does your agency have a software bill of materials (S-BOM) that identifies all of its assets? If so, how often is it updated and does it contain Apache Log4j?
6. When did your agency first learn of the Log4j vulnerability? What incident alert thresholds does your agency have, and what are your requirements for escalating and reporting anomalies?
7. Does your agency have a specific plan to identify and remediate, on an ongoing basis, software that it uses to ensure the agency is not currently using software vulnerable to a cyber threat?

Your assistance in this urgent matter is appreciated. If you have any questions, please contact Brannon Rains and Marissa Gervasi on the committee staff.

Sincerely,


Cathy McMorris Rodgers
Republican Leader


Gus Bilirakis
Republican Leader
Subcommittee on Consumer Protection
and Commerce


H. Morgan Griffith
Republican Leader
Subcommittee on Oversight
and Investigations



U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

March 1, 2022

The Honorable Janice D. Schakowsky
Chair
Consumer Protection
& Commerce Subcommittee
House of Representatives
Washington, DC 20515

The Honorable Gus M. Bilirakis
Ranking Member
Consumer Protection
& Commerce Subcommittee
House of Representatives
Washington, DC 20515

Dear Chair Schakowsky and Ranking Member Bilirakis:

The U.S. Chamber of Commerce is disappointed that today's hearing about consumer protections and technology fails to address national data privacy legislation and instead focusses on bills that have the potential to harm the nation's vibrant e-commerce systems, and stifle innovation and competition in crucial emerging technologies like artificial intelligence. We urge the Subcommittee and Congress to instead focus on protecting consumer privacy, which the vast majority of Americans agree is needed.

The Chamber opposes H.R. 6416, the so called "Banning Surveillance Advertising Act of 2022," which would harm the online advertising ecosystem that has contributed to a thriving internet-based economy. In particular, small businesses would be hard hit by this legislation. Efficient and cost-effective online advertising—across a range of websites, apps, and technologies—saves US small businesses an estimated \$163 billion annually.¹ Additionally, consumers preferred tailored and relevant advertising.² Small companies increasingly used digital tools as a lifeline to reach consumers during the pandemic.³

It is critically important Congress gets artificial intelligence policy right. AI is helping secure networks, develop vaccines, and expand financial inclusion. Before imposing new, burdensome regulation of AI, Congress should first focus on ensuring a flexible U.S. regulatory framework is developed. There is important work already underway to provide Congress with important insights, including multistakeholder approaches like the U.S. Chamber's AI Commission on Competitiveness, Inclusion, and Innovation⁴ and NIST's Risk Management Framework⁵ to run their course to inform the development of bipartisan solutions.

The Chamber opposes H.R. 6580, the "Algorithmic Accountability Act," which would frustrate the development and deployment of beneficial technologies with new layers of

¹ <https://sbecouncil.org/2019/09/10/online-advertising-delivers-big-benefits-for-small-businesses/>

² <https://www.marketingdive.com/news/study-71-of-consumers-prefer-personalized-ads/418831/>

³ <https://about.fb.com/wp-content/uploads/2020/10/Deloitte-Digital-Tools-in-Crisis-and-Recovery-SMB-Report-Oct-2020.pdf>

⁴ <https://americaninnovators.com/aicommission/>

⁵ <https://www.nist.gov/itl/ai-risk-management-framework>

bureaucracy and approvals for an already heavily regulated industry by creating an ill-conceived new burdensome impact assessment regime for all automated decision systems, rather than just high-risk applications. Under H.R. 6580, a large number of companies likely would be stuck waiting for Federal Trade Commission approval on unnecessary low-risk automated systems which companies are relying on to help grow, innovate and compete.

The Chamber also has significant concerns about H.R. 6796, the “Digital Services Oversight and Safety Act of 2022,” as significant unresolved questions remain over exactly how wide the scope of the bill is and what industries are actually affected.

We strongly believe the Subcommittee and Congress should prioritize protecting consumer’s privacy. There are many privacy proposals in Congress today that could provide durable, bipartisan solutions that give consumers meaningful data rights like Representative Suzan DelBene’s Information Transparency & Personal Data Control Act⁶ and the recently announced privacy draft⁷ released by Ranking Member Cathy McMorris Rodgers.

Sincerely,



Neil L. Bradley
Executive Vice President, Chief Policy Officer, and
Head of Strategic Advocacy
U.S. Chamber of Commerce

cc: Members of the House Committee on Energy and Commerce’s Subcommittee on Consumer Protection and Commerce

⁶ <https://www.congress.gov/bill/117th-congress/house-bill/1816/text?q=%7B%22search%22%3A%22H1816%22%5D%7D&r=1&s=10>

⁷ <https://republicans-energycommerce.house.gov/wp-content/uploads/2021/11/2021.11.02-Republican-CODA-Draft-.pdf>

Mr. Mike Duffey
Page 3

Attachment—Additional Questions for the Record

**Subcommittee on Consumer Protection and Commerce
Hearing on
“Holding Big Tech Accountable: Legislation to Protect Online Users”
March 1, 2022**

Mr. Mike Duffey, Special Agent Supervisor, Florida Department of Law Enforcement

The Honorable Anna Eshoo (D-CA)

1. Your testimony identified tech companies’ data retention practices as an inhibitor of investigations into cases involving child sex abuse materials (CSAM).

- a. Federal law requires companies reporting to NCMEC’s CyberTipline to retain data for 90 days after a submission (18 U.S.C. §2258A(h)(1)). Would you support an extended retention requirement of 180 days?

RESPONSE: Representative Eshoo- I would support the extension to 180 days. In some instances, information or leads are reported to law enforcement beyond the 90 day period, which leaves law enforcement with no way to obtain additional information to initiate or further an investigation.

- b. The *Invest in Child Safety Act* is my bipartisan and bicameral legislation that extends the CyberTipline data retention requirement to 180 days and also directs \$5 billion in mandatory funding to investigate and target individuals who create and share CSAM, including funding for additional personnel in federal, state, and local law enforcement agencies, along with NCMEC, dedicated to combating CSAM. Would this bill aid your efforts to combat CSAM and do you think Congress should pass this legislation?

RESPONSE: Representative Eshoo- I fully support the “Invest in Child Safety Act”. This Act will allow for all entities involved to expand their growing efforts to protect children and allow law enforcement to add expertise to combat CSAM. This would help as we continue to struggle to keep up with today’s technology and how its used to produce, self-produce and distribute CSAM on these platforms.

Improvements to data retention and additional funding are not a complete solution, however. There are companies who by the nature of their network architecture won’t be able report CSAM as it won’t be visible to them. The latest publicly reported numbers from NCMEC reveal a significant disparity in reporting based on the design decisions made by individual companies. For

Mr. Mike Duffey
Page 4

example, Apple reported only 160 instances while Facebook reported 22,118,952 instances. If companies are permitted to intentionally blind themselves to CSAM on their networks, increased retention periods and more funding will do law enforcement only limited good.

2. You testified that encrypted messaging inhibits investigations. Please answer the following questions regarding your agency's investigations in the last 12 months (or for another similar time period for which your agency collects such data) that were inhibited due to encrypted messaging:
 - a. How often did your agency access or request metadata associated with encrypted messaging related to crimes from technology companies, wireless providers, or other companies?

RESPONSE: Representative Eshoo- We request this information as the specific case dictates. We are aware of the various platforms that are already engaging in end-to-end encryption and as such we try to determine if the potential metadata retained is of value to the case. In some cases, suspects use virtual private networks (VPNs) to further hide their internet protocol address which often results in another roadblock in an investigation. The reality is that metadata, while useful in many cases, is not a substitute for content for several reasons. First, it is not always available; for example, if investigators are seeking evidentiary conversations on an encrypted chat platform, even where metadata is available from the provider in some cases, if the evidence is in transit on the data side of the device off the carrier's network (i.e. on public or private wifi) it may not be reflected in what companies provide in response to our legal demands. Second, metadata itself is not an evidentiary substitute for content. Criminal prosecutions require proof of a subject's mental state, for example, and metadata by itself cannot easily be used to prove motive or malice. Finally, metadata isn't an effective substitute for content even if prosecution is a secondary consideration to mitigation of violence. If a group of individuals is plotting to carry out some kind of violent behavior, a pattern of communication that we might glean from metadata won't reveal their targets, methods, or indeed the planned time and date of their intended attack, which makes it less useful from a violence prevention standpoint.

- b. What portion of these requests are informal and what portion involve formal legal processes (e.g., subpoenas)?

RESPONSE: Representative Eshoo- All of our requests to Electronic Service Providers (ESP) and Internet Service Providers (ISP) are formal processes that often start with data preservation requests, which then lead to additional formal legal process for content and other data possessed by the platforms. Our requests for this information are often time-intensive. To obtain content we must get a court order and search warrants as required by Federal law.

Mr. Mike Duffey
Page 5

- c. How often did companies comply with these (i) informal requests and (ii) formal requests?

RESPONSE: Representative Eshoo- Generally all formal legal requests are responded to by the various companies. The issue is what data they retain as a matter of business practice; some types of data that would be helpful in an investigation is not retained, and this varies from platform to platform. With no regulatory framework mandating the retention of specific types of data, there are inconsistencies in what our legal demands will produce. There are also instances where data exists, but some platforms don't have the ability to extract this data in a timely manner because the companies have not built tools to extract the data requested during a specific time period.

- d. How many cases was your agency ultimately unable to solve because of encrypted messaging?

RESPONSE: Representative Eshoo- This varies depending on the crime type and platform type, as the most popular messaging apps and platforms have only talked about implementing end-to-end encryption for messaging. If and when they implement encrypted messaging, it will turn successful cases into unsuccessful ones and will allow those preying upon our children to operate with the full protection of encryption. We see encrypted messaging platforms being used routinely in illegal narcotics cases since traffickers believe their activities are more effectively protected.

In some instances, law enforcement has decided to not issue legal process in the first place because they know the platform deploys end-to-end encryption, which would likely result in no information being provided. As a practical matter, law enforcement does not generate legal demands that we know are futile. We are too busy with cases to spend time trying to access evidence that we know companies cannot produce. If a particular platform or technology is known to be inaccessible, investigators will explore other avenues or, if they hit a dead end, other cases. Criminal investigations are often too complex and nuanced to attribute their outcome to one factor like encryption. In many cases where a subject is still identified and prosecuted, the case takes longer to make and requires more effort. Those are law enforcement resources that could be going to something else... working through a cybertip backlog, for example. That might not be a case law enforcement was unable to solve, but it was certainly a significant negative impact on public safety caused by warrant-proof encryption.

3. Please answer the following questions for your agency's investigations in the last 12 months (or for another similar time period for which your agency collects such data) that involved accessing *un*encrypted messages:

Mr. Mike Duffey
Page 6

- a. How often does your agency access or attempt to access unencrypted messages?

RESPONSE: Representative Eshoo- We regularly serve legal process to Internet Service Providers and Electronic Service Providers for data they retain. This data is often returned to law enforcement in a format that is determined by each company – responses do not come in a standard format. As a result, law enforcement then must use various analytical tools to review and make sense of the data to determine if it is relevant to the legal process. This often requires a third-party paid service, and these paid services are another cost that our agencies must bear to ensure we can make the most of the evidence we are able to obtain.

- b. What portion of these unencrypted messages does your agency access directly (i.e., from an unlocked phone) and what portion does your agency access by requesting messages from a company?

RESPONSE: Representative Eshoo- It ends up being both – examining information from an unlocked device that was obtained using extraction tools, and also serving legal process on the platform for this data. With today's users being able to delete messages from a device after messages are sent, and users being able to send messages that disappear after they are read, it is important that law enforcement examine both sets of data as individuals and platforms can choose to remove content. In some instances, this data might have been deleted on the recipient's device but not deleted from the platform's cloud or on the platform's site.

Since February of 2021, FDLE has documented 119 locked mobile devices that have been part of criminal investigations, but the contents of which we were unable to access. These devices were involved in all types of crimes. The 119 devices is only a FDLE snapshot and does not account for all of Florida law enforcement.

- c. What portion of requests to companies are informal and what portion involve formal legal processes (e.g., subpoenas)?

RESPONSE: Representative Eshoo- All of our requests to Electronic Service Providers (ESP) and Internet Service Providers (ISP) are formal processes that often start with data preservation requests, which then leads to additional formal legal process for content and other data possessed by the platforms. If the subject's mobile device that is part of the investigation is locked, agencies must purchase costly third party tools to ensure data on the device is available to identify additional details related to the crime.

- d. How often did companies comply with these (i) informal requests and (ii) formal requests?

Mr. Mike Duffey
Page 7

RESPONSE: Representative Eshoo- Generally all formal legal requests are responded to by the various companies. The issue is what data they retain or as a matter of business practice; some types of data that would be helpful in an investigation are not retained, and that varies by platform. With no regulatory framework mandating the retention of specific types of data, there are inconsistencies in what our legal demands will produce. There are also instances where data exists, but some platforms don't have the ability to extract this data in a timely manner because the companies have not built tools to extract the data requested during a specific time period.



2021 CyberTipline Reports by Electronic Service Providers (ESP)

NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children, including child sexual abuse material, child sex trafficking and online enticement. In 2021, the CyberTipline received more than 29.3 million reports. 29.1 million of these reports were from Electronic Service Providers that report instances of apparent child sexual abuse material that they become aware of on their systems.

Higher numbers of reports can be indicative of a variety of things including larger numbers of users on a platform or how robust an ESP's efforts are to identify and remove abusive content. NCMEC applauds ESPs that make identifying and reporting this content a priority and encourages all companies to increase their reporting to NCMEC. These reports are critical to helping remove children from harmful situations and to stopping further victimization.

The following is a breakdown of reports by electronic service providers.

ESP	Number of Reports
4chan	973
4shared	75
7web	1,908
Absolute Software Corporation	3
Adobe Systems Incorporated	1,066
Affinity Apps	869
Afilias USA	203
Airbnb	62
Airtime Media	95
Alpha Exploration Co (Clubhouse)	620
Amazon	99
Amazon Games	4
Amazon Photos	27,101
Amino Apps	75
animebw	16
Apple	160

2021 Reports by ESP 2

ESP	Number of Reports
Apricot Digitals	1
Arctic Wolf Networks, Inc.	3
Ariemgroup Limited	32
Ask.fm	117
Asurion Corporation	2
AT&T WorldNet Service	1
Badoo	475
Bark Technologies Inc	282
BigBang Media	225
Blizzard Entertainment (World of Warcraft)	4
Blue Vision	43
Box	2,599
Bubblup	13
Canva	1
Care.com	2
Chatango LLC	2
Checkstep	127
Classmates Online	1
Cloudflare	12,932
Comcast Cable Communications	8
Cyveillance	5
deviantART	6
Digital Ocean	200
Discord	29,606
Dreamstime.com	2
Dropbox	48,371
Easynews/Newshosting/Usenetserver	21
EasyOnlineSolutions/MojoHost/ North Tone/Hosthead	41
Ebay	19
Electronic Arts	7
Ello.co	4
Endurance International Group	103
Enom	56
Etsy	6
Facebook	22,118,952
Fenix International Limited	2,984

ESP	Number of Reports
Fotoloco	9
FreeDNS.Afraid.org	3
Gaggle	4,656
Get Together (IRL)	1
GF Networks	12
Giphy	229
GitHub	4
Globtech	4,078
GLU MOBILE	2
GoDaddy	32
GoFundMe	1
GoGuardian	21
Google	875,783
Grindr	10,671
Gumroad	2
Hacker Factor	386
Hewlett Packard Enterprise	5
Hinge.co	6
Hosting Services Inc/Midphase/ WestHost/Autica/VPS	33
HowlogicKFT	3
Imagebam/Flixya Entertainment/Videobam	54,742
Imgur	47,274
IMVU	10
Indeed	2
InfraWeb Solution Limited	7
INHOPE	130,723
Instagram	3,393,654
Internap Corporation (INAP)	15
Internet Archive	188
Interspace Technologies (Byte)	11
Intrado Interactive Services Corporation	184
JMS Internet	1
JNJ Mobile (MocoSpace)	33
Joyo Technology Pte	1
Kaleton Web S.R.O	1
KnownHost/PrivateSystems Networks	1

ESP	Number of Reports
Lain.la	2
LBRY INC	2
LegitScript	1
LEGO System	37
Life on Air (Houseparty)	8,575
Linden Lab (SecondLife)	30
LinkedIn	110
Linode	28
Luftgescheft	5,270
Marbore Web Solutions Limited	4
Marinus Analytics (Traffic Jam)	9
Match Group	158
Medal.tv	26
MediaFire	3,506
MediaLab (Kik)	33,619
Medium	113
MeetMe	2,930
MeWe	1,444
MG Freesites	16
MG Freesites (Pornhub)	9,029
MG Freesites (Redtube)	21
MG Freesites (Tube8)	6
MG Freesites (Youporn)	31
Microsoft	78,603
Microsoft - Xbox	170
MMGuardian	54
Momentive	3
motherless	3,110
Movie Star Planet	5
Mozilla Corporation	2
Multi Media/Zmedianow/Chaturbate	532
Name.com	1
NameCheap	5
National Center on Sexual Exploitation	14
NEOSOLUT WEB SERVICES	3
Nexeon Technologies	8
NextDoor	2

ESP	Number of Reports
Niteflirt/Phrendly.com/Platphorm	22
NorfexHoldingsLimited	7
Northlock Holdings Limited	2
Notion Labs	1
Novi	1
OfferUp	1
Okcupid	178
Omegle	46,924
Orbiseen s.r.o	2
Outschool	1
OVH US	25
Padlet/Wallwisher/Cloudfront	235
Patook	2
Patreon	37
PayPal	970
People Media	1
Photobucket	10
PicsArt	316
Pinger	2
Pinterest	2,283
PocketStars	1
Pokemon	2
Porkbun	1
PORTICATO MEDIA	13
ProBoards	5
Public Interest Registry	183
Quora	25
RealNetworks	4
Redbubble	41
Reddit	10,059
Redgifs	87
Reflected Networks	124
RingCentral	1
Roblox	4,684
Scratch Foundation	20
Scruff App (Perry Street Software)	19
sendvid	703

ESP	Number of Reports
SimilarWorlds	94
Skout	1,203
Slack Technologies	1,263
SmugMug-Flickr	1,169
Smule	2
Snapchat	512,522
Sniffies	9
Softlayer	1
Sohosolutions	2
Sony Interactive Entertainment	2,071
Spotify USA	258
Squarespace	1
StackPath/Highwinds	4
Stanford Internet Observatory	1
StarNow	1
Stelivo	2,034
Stolichnaq	29
Streamable	90
Streamate	16
Stripe	1
Sykes	2
SynaptiCAD	31
Synchronoss Technologies	3,472
Tagged	5,504
Take-Two Interactive Software	3
TECH MEDIALAND KFT	1
The Walt Disney Company	1
Thorn	114
ThumbSnap	308
Thumbtack	1
TikTok	154,618
Tinder	3,642
Toontown Rewritten	12
Tropical Sun (Clips4Sale)	2
Tsu	18
Tumblr	4,511
Twitch	6,629

ESP	Number of Reports
Twitter	86,666
Uncharted Software	18
Various/FriendFinder/Tangotime	26
Veoh Networks	1
VeriSign	341
Verizon Online	50
Verizon Wireless	5
Vero Labs	177
Vimeo	360
Vistaprint	2
Visual Supply Company	34
Voice	1
Vokal (First Media)	130
Web.com/Network Solutions/ Register/NameBargain	3
Weebly	4
WhatsApp	1,372,696
Whisper	1
Wickr	15
Wikimedia Foundation	8
Wildlife Studios	84
WildWorks (AnimalJam)	8
Wink	108
Wixpress (Wix)	1
WordPress.com (Automattic)	310
x-up.ws	636
Yahoo!	5,485
Younow	1,001
Yubo	885
ZeroFox	1
Zoom Video Communications	548
Zvelo	1
Total:	29,157,083



2021 CyberTipline Reports by Electronic Service Providers (ESP)

NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children, including child sexual abuse material, child sex trafficking and online enticement. In 2021, the CyberTipline received more than 29.3 million reports. 29.1 million of these reports were from Electronic Service Providers that report instances of apparent child sexual abuse material that they become aware of on their systems.

Higher numbers of reports can be indicative of a variety of things including larger numbers of users on a platform or how robust an ESP's efforts are to identify and remove abusive content. NCMEC applauds ESPs that make identifying and reporting this content a priority and encourages all companies to increase their reporting to NCMEC. These reports are critical to helping remove children from harmful situations and to stopping further victimization.

The following is a breakdown of reports by electronic service providers.

ESP	Number of Reports
4chan	973
4shared	75
7web	1,908
Absolute Software Corporation	3
Adobe Systems Incorporated	1,066
Affinity Apps	869
Afilias USA	203
Airbnb	62
Airtime Media	95
Alpha Exploration Co (Clubhouse)	620
Amazon	99
Amazon Games	4
Amazon Photos	27,101
Amino Apps	75
animebw	16
Apple	160

2021 Reports by ESP 2

ESP	Number of Reports
Apricot Digitals	1
Arctic Wolf Networks, Inc.	3
Ariemgroup Limited	32
Ask.fm	117
Asurion Corporation	2
AT&T WorldNet Service	1
Badoo	475
Bark Technologies Inc	282
BigBang Media	225
Blizzard Entertainment (World of Warcraft)	4
Blue Vision	43
Box	2,599
Bubblup	13
Canva	1
Care.com	2
Chatango LLC	2
Checkstep	127
Classmates Online	1
Cloudflare	12,932
Comcast Cable Communications	8
Cyveillance	5
deviantART	6
Digital Ocean	200
Discord	29,606
Dreamstime.com	2
Dropbox	48,371
Easynews/Newshosting/Usenetserver	21
EasyOnlineSolutions/MojoHost/ North Tone/Hosthead	41
Ebay	19
Electronic Arts	7
Ello.co	4
Endurance International Group	103
Enom	56
Etsy	6
Facebook	22,118,952
Fenix International Limited	2,984

ESP	Number of Reports
Fotoloco	9
FreeDNS.Afraid.org	3
Gaggle	4,656
Get Together (IRL)	1
GF Networks	12
Giphy	229
GitHub	4
Globtech	4,078
GLU MOBILE	2
GoDaddy	32
GoFundMe	1
GoGuardian	21
Google	875,783
Grindr	10,671
Gumroad	2
Hacker Factor	386
Hewlett Packard Enterprise	5
Hinge.co	6
Hosting Services Inc/Midphase/ WestHost/Autica/VPS	33
HowlogicKFT	3
Imagebam/Flixya Entertainment/Videobam	54,742
Imgur	47,274
IMVU	10
Indeed	2
InfraWeb Solution Limited	7
INHOPE	130,723
Instagram	3,393,654
Internap Corporation (INAP)	15
Internet Archive	188
Interspace Technologies (Byte)	11
Intrado Interactive Services Corporation	184
JMS Internet	1
JNJ Mobile (MocoSpace)	33
Joyo Technology Pte	1
Kaleton Web S.R.O	1
KnownHost/PrivateSystems Networks	1

ESP	Number of Reports
Lain.la	2
LBRY INC	2
LegitScript	1
LEGO System	37
Life on Air (Houseparty)	8,575
Linden Lab (SecondLife)	30
LinkedIn	110
Linode	28
Luftgescheft	5,270
Marbore Web Solutions Limited	4
Marinus Analytics (Traffic Jam)	9
Match Group	158
Medal.tv	26
MediaFire	3,506
MediaLab (Kik)	33,619
Medium	113
MeetMe	2,930
MeWe	1,444
MG Freesites	16
MG Freesites (Pornhub)	9,029
MG Freesites (Redtube)	21
MG Freesites (Tube8)	6
MG Freesites (Youporn)	31
Microsoft	78,603
Microsoft - Xbox	170
MMGuardian	54
Momentive	3
motherless	3,110
Movie Star Planet	5
Mozilla Corporation	2
Multi Media/Zmedianow/Chaturbate	532
Name.com	1
NameCheap	5
National Center on Sexual Exploitation	14
NEOSOLUT WEB SERVICES	3
Nexeon Technologies	8
NextDoor	2

ESP	Number of Reports
Niteflirt/Phrendly.com/Platphorm	22
NorfexHoldingsLimited	7
Northlock Holdings Limited	2
Notion Labs	1
Novi	1
OfferUp	1
Okcupid	178
Omegle	46,924
Orbiseen s.r.o	2
Outschool	1
OVH US	25
Padlet/Wallwisher/Cloudfront	235
Patook	2
Patreon	37
PayPal	970
People Media	1
Photobucket	10
PicsArt	316
Pinger	2
Pinterest	2,283
PocketStars	1
Pokemon	2
Porkbun	1
PORTICATO MEDIA	13
ProBoards	5
Public Interest Registry	183
Quora	25
RealNetworks	4
Redbubble	41
Reddit	10,059
Redgifs	87
Reflected Networks	124
RingCentral	1
Roblox	4,684
Scratch Foundation	20
Scruff App (Perry Street Software)	19
sendvid	703

ESP	Number of Reports
SimilarWorlds	94
Skout	1,203
Slack Technologies	1,263
SmugMug-Flickr	1,169
Smule	2
Snapchat	512,522
Sniffies	9
Softlayer	1
Sohosolutions	2
Sony Interactive Entertainment	2,071
Spotify USA	258
Squarespace	1
StackPath/Highwinds	4
Stanford Internet Observatory	1
StarNow	1
Stelivo	2,034
Stolichnaq	29
Streamable	90
Streamate	16
Stripe	1
Sykes	2
SynaptiCAD	31
Synchronoss Technologies	3,472
Tagged	5,504
Take-Two Interactive Software	3
TECH MEDIALAND KFT	1
The Walt Disney Company	1
Thorn	114
ThumbSnap	308
Thumbtack	1
TikTok	154,618
Tinder	3,642
Toontown Rewritten	12
Tropical Sun (Clips4Sale)	2
Tsu	18
Tumblr	4,511
Twitch	6,629

ESP	Number of Reports
Twitter	86,666
Uncharted Software	18
Various/FriendFinder/Tangotime	26
Veoh Networks	1
VeriSign	341
Verizon Online	50
Verizon Wireless	5
Vero Labs	177
Vimeo	360
Vistaprint	2
Visual Supply Company	34
Voice	1
Vokal (First Media)	130
Web.com/Network Solutions/ Register/NameBargain	3
Weebly	4
WhatsApp	1,372,696
Whisper	1
Wickr	15
Wikimedia Foundation	8
Wildlife Studios	84
WildWorks (AnimalJam)	8
Wink	108
Wixpress (Wix)	1
WordPress.com (Automattic)	310
x-up.ws	636
Yahoo!	5,485
Younow	1,001
Yubo	885
ZeroFox	1
Zoom Video Communications	548
Zvelo	1
Total:	29,157,083

Ms. Mutale Nkonde
Page 3

Attachment—Additional Questions for the Record

**Subcommittee on Consumer Protection and Commerce
Hearing on
“Holding Big Tech Accountable: Legislation to Protect Online Users”
March 1, 2022**

Ms. Mutale Nkonde, Founder and CEO, AI for the People, US

The Honorable Bobby Rush (D-IL)

1. Ms. Nkonde, digital redlining — through the use of technology, alternative data sets, and social media behaviors — systematically suppresses the presentation of certain online and mobile advertisements to certain populations. While it is generally reasonable that advertisers want to deliver ads to a targeted audience who have a greater likelihood of buying their products and services, this type of targeting is problematic when it comes to, among other things, financial services. Controlling the ad delivery process through the use of certain variables can have the effect of discriminating against protected classes, in a manner that constitutes an Unfair, Deceptive or Abusive Act or Practice (UDAAP) or otherwise violates fair lending laws.
 - a. What can be done to protect consumers seeking financial service products from online or mobile platforms using variables such as age and gender in their marketing algorithms in a manner that could result in individuals in protected classes being precluded from receiving advertisements for certain credit products?

Ms. Mutale Nkonde

Page 4

RESPONSE:

Dear Congressman Rush,

Thank you for this important question. Digital redlining remains a constant problem. Redlining refers to a policy pursued by the Federal Housing Authority (FHA) and government backed Homeowners' Loan Corporation (HOLC) from 1934 – 1971. They would use red ink on maps to warn mortgage lenders against approving loans to people living in neighborhoods with sizable Black populations¹. This isolated Black people within zip codes that suffered lower levels of investment and precluded Black families from building wealth through homeownership. Like its analogue equivalent digital or algorithmic redlining disadvantages Black Americans. However instead of its impact being limited to housing, because of the wide use of algorithmic decision-making technology across the economy², digital redline impacts Black consumers engaging with every part of the financial sector³.

Below I will draw on two examples, one in which the source code of a website has been found to disadvantage Black consumers. The second where a group of researchers have found algorithmic bias within mortgage determinations.

In both cases the algorithms under consideration are protected by intellectual property laws. Therefore, consumers do not have the right to find out how these systems reached these determinations. The American people are therefore looking to Congress to:

- Ensure algorithmic determinations do not violate Section VII of the 1964 Civil Rights Act
- Develop enforcement mechanisms to ensure bad actors are held accountable and
- Educate consumers when and how algorithmic systems are being used within consumer sector.

¹ Perry A M & Hershberger D (October 14, 2019) America's formerly redlined neighborhoods have changed, and so must solutions to rectify them, Brookings, find the article here <https://www.brookings.edu/research/americas-formerly-redlines-areas-changed-so-must-solutions/>

² McKinsey Global Institute (April 17, 2018) Notes from the AI frontier: Applications and value of deep learning, read the report here <https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-applications-and-value-of-deep-learning>

³ Perry A M & Hershberger D (October 14, 2019) America's formerly redlined neighborhoods have changed, and so must solutions to rectify them, Brookings, find the article here <https://www.brookings.edu/research/americas-formerly-redlines-areas-changed-so-must-solutions/>

Ms. Mutale Nkonde

Page 5

Digital Redlining and Dark Patterns.

One of the largest issues facing consumers seeking online financial services are the presence of dark patterns. Dark patterns are software programs that software can subtly trick users into engaging in behavior that's good for the company. For example, in 2019 journalists at ProPublica, found the tax preparation website TurboTax.com was steering users who made less than \$66,000 a year to their paid for products, despite having signed an agreement with the IRS to offer free tax preparation services to low income Americans.

The Pro Publica team found source code of the TurboTax website branded low-income consumers as "NONFFA." That stands for "Non-Free File Alliance." In other words, their technology was steering low-income consumers to paid for products, in doing so preventing them from accessing free tax filing services. This is in violation of the Unfair and Deceptive Practices Act and has a disparate impact on consumers from negatively racialized groups.

In 2018 the median household incomes of Black & Hispanic Americans, American Indians and Native and Alaskan people means people of color are more likely to qualify for free tax advice than white non-Hispanic Americans. Please see the table below:

Demographic	Median US Household income in 2018
Black American	\$41,361 ⁴
Hispanic American	\$51,404 ⁵
American Indian and Alaska Natives	\$49,906 ⁶

⁴ US Census Bureau: Income and Poverty in the United States in 2018

⁵ *ibid*

⁶ *Ibid*

Ms. Mutale Nkonde
Page 6

White Americans	\$70,642 ⁷
-----------------	-----------------------

Therefore, consumers from negatively racialized communities are most like to enter “free tax preparation services” into online search. Given that Google controls 85 percent of the global search market⁸, Black Americans are most likely to use Google search.

The Google business model is reliant on online advertising. In 2020 Alphabet Google’s parent company generated \$185 billion in revenue. \$145 billion (or 80 percent of that total) came from the Google Ads business⁹. Google Ads generates income by allowing businesses to target users using search terms. For example, someone searching for “free tax advice: may not just be directed to the TurboTax website, but other online financial services that discriminate against Black Americans in the same way.

Digital Redlining and Mortgage Determinations

Another example of algorithmic bias within financial services are in the online mortgage market. A team of researchers at Haas School of Business found online and traditional lenders gave Black and Hispanic borrowers higher interest rates than their white counterparts. The additional interest rate points to mortgage cost Black and Hispanic borrowers an estimated \$250 million to \$500 million each year¹⁰. Despite the fact these groups have lower median household incomes than white non-Hispanic Americans.

Researchers found one of the reasons the mortgage algorithm being examined by the Berkley team discriminated against Black borrowers was because the developers used the “rate of comparison shopping” within its decision tree. This presents two ways this algorithmic system discriminates against Black people.

⁷ Ibid

⁸ Statista.com Worldwide desktop market share of leading search engines from January 2010 to January 2022 , find the data here <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>

⁹ Graham M and Elias J (May 18, 2021) How Google’s \$150 billion advertising business works, find the article here <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html>

¹⁰ Counts L (November 13, 2018) Minority homebuyers face widespread statistical lending discrimination, study finds, Berkeley Haas blog, find the article here <https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/>

Ms. Mutale Nkonde
Page 7

The first is the nature of targeted advertising. I have pointed out Google's Ads allows businesses to target consumers using specific search terms. In 2021 another Berkley research team found 80 percent of residential areas in metropolitan areas are segregated by race¹¹. Therefore, within the algorithmic era, zip code is an indicator of race.

- Many websites ask our permission to deny or allow them to track your location, when users check "yes" they are allowing businesses like Google pinpoint your geo location.
- If they are logging on from a zip code with high Black population, this allows advertisers to infer your race by combing your zip code with the other data they may have about it.
- During COVID lockdowns is likely you were logging on from home.
- Zip codes are mapped to census tract data giving computer scientists information on the median age, gender, household income, education, and health levels of the people within this location.

Then when we consider how the federal government racialized the housing market through redlining policies, zip code becomes proxy for race.

The same is true on the company side, Google Ads allows mortgage lenders to segment their audience by zip code. In 2019 the Department of Housing and Development (HUD) sued Facebook for allowing advertisers to use check boxes that prevent Black Americans from seeing housing ads¹². It is therefore not a stretch to assume this happens within the mortgage lending sector. This type of online discrimination creates digital financial services deserts, akin to food deserts created in these areas through lack of access to fresh food. Either way Black consumers may not be given the same opportunity to see the same number of online mortgage ads as their white counterparts. It would therefore be harder for Black Americans to reach the comparison-shopping threshold set by the algorithmic mortgage lending tool examined by the Berkley team.

¹¹ NBC (August 16, 2021) U.S. neighborhoods are more segregated than a generation ago, perpetuating racial inequity, find the article here <https://www.nbcnews.com/think/opinion/u-s-neighborhoods-are-more-segregated-generation-ago-perpetuating-racial-inequality-1276372>

¹² Tobin A (March 28, 2019) HUD Sues Facebook Over Housing Discrimination and Says the Company's Algorithms Have Made the Problem Worse, ProPublica, read the article here <https://www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms>

Ms. Mutale Nkonde
Page 8

The other way the “comparison-shopping determination” discriminates against Black Americans is that it assumes Americans are given equal access to mortgage loans.¹³ However this is not true:

- In 2019 a team at the Mark Up team used the data available through the Home Mortgage Disclosure Act to find out how mortgage determinations were made.
- They found Black mortgage applicants in Chicago were 150 percent more likely to be denied a mortgage than their white counterparts, and Black Americans were 80 percent more likely to be denied a mortgage loan than their white counterparts nationwide.
- One of the reasons they cited this was Freddie Mac and Fannie Mae's use of the “Classic FICO” credit scoring algorithm, used to determine whether an applicant meets the minimum threshold to be considered for a conventional loan

The FICO algorithm was developed from data from the 1990s and is more than 15 years old. It is considered detrimental to people of color because it rewards traditional credit, to which White Americans have more access¹⁴.

In a situation where Black consumers are more likely to be denied for credit than their white counterparts, they may choose not to opt to comparison shop because each time a mortgage lender makes a credit inquiry it reduces their FICO score¹⁵. Which in turn would reduce the likelihood of this borrower being granted a conventional mortgage. The team developing the mortgage determination algorithm did not consider how the history of racial discrimination within the United States shapes how Black financial behavior. Instead, they used this “comparison shopping” as an indicator for risk worthiness. Despite the fact it did not provide any insight to whether borrowers will pay back the loan.

This is an example of how subjective inputs lead to the development of algorithms that discriminate against not just Black Americans, but people from the protected classes.

¹³ Martinez E and Kirchner L (August 25, 2021) [Denied](https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms) The Secret Bias Hidden in Mortgage-Approval Algorithms, The Mark Up, read the article here <https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms>

¹⁴ Ibid

¹⁵ White J (September 13, 2019) How Many Points Does an Inquiry Drop Your Credit Score? Experian blog, read it here <https://www.experian.com/blogs/ask-experian/how-many-points-does-an-inquiry-drop-your-credit-score/>