S. HRG. 117–723

DISRUPTING DANGEROUS ALGORITHMS: ADDRESSING THE HARMS OF PERSUASIVE TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS, MEDIA, AND BROADBAND

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

DECEMBER 9, 2021

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
53–136 PDF WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota	ROGER WICKER, Mississippi, *Ranking*
RICHARD BLUMENTHAL, Connecticut	JOHN THUNE, South Dakota
BRIAN SCHATZ, Hawaii	ROY BLUNT, Missouri
EDWARD MARKEY, Massachusetts	TED CRUZ, Texas
GARY PETERS, Michigan	DEB FISCHER, Nebraska
TAMMY BALDWIN, Wisconsin	JERRY MORAN, Kansas
TAMMY DUCKWORTH, Illinois	DAN SULLIVAN, Alaska
JON TESTER, Montana	MARSHA BLACKBURN, Tennessee
KYRSTEN SINEMA, Arizona	TODD YOUNG, Indiana
JACKY ROSEN, Nevada	MIKE LEE, Utah
BEN RAY LUJÁN, New Mexico	RON JOHNSON, Wisconsin
JOHN HICKENLOOPER, Colorado	SHELLEY MOORE CAPITO, West Virginia
RAPHAEL WARNOCK, Georgia	RICK SCOTT, Florida
	CYNTHIA LUMMIS, Wyoming

MELISSA PORTER, *Deputy Staff Director*
GEORGE GREENWELL, *Policy Coordinator and Security Manager*
JOHN KEAST, *Republican Staff Director*
CRYSTAL TULLY, *Republican Deputy Staff Director*
STEVEN WALL, *General Counsel*

SUBCOMMITTEE ON COMMUNICATIONS, MEDIA, AND BROADBAND

BEN RAY LUJÁN, New Mexico, *Chair*	JOHN THUNE, South Dakota, *Ranking*
AMY KLOBUCHAR, Minnesota	ROY BLUNT, Missouri
RICHARD BLUMENTHAL, Connecticut	TED CRUZ, Texas
BRIAN SCHATZ, Hawaii	DEB FISCHER, Nebraska
EDWARD MARKEY, Massachusetts	JERRY MORAN, Kansas
GARY PETERS, Michigan	DAN SULLIVAN, Alaska
TAMMY BALDWIN, Wisconsin	MARSHA BLACKBURN, Tennessee
TAMMY DUCKWORTH, Illinois	TODD YOUNG, Indiana
JON TESTER, Montana	MIKE LEE, Utah
KYRSTEN SINEMA, Arizona	RON JOHNSON, Wisconsin
JACKY ROSEN, Nevada	SHELLEY MOORE CAPITO, West Virginia
JOHN HICKENLOOPER, Colorado	RICK SCOTT, Florida
RAPHAEL WARNOCK, Georgia	CYNTHIA LUMMIS, Wyoming

CONTENTS

WITNESSES

APPENDIX

DISRUPTING DANGEROUS ALGORITHMS: ADDRESSING THE HARMS OF PERSUASIVE TECHNOLOGY

THURSDAY, DECEMBER 9, 2021

U.S. SENATE,
SUBCOMMITTEE ON COMMUNICATIONS, MEDIA, AND BROADBAND,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:54 a.m., in room SR–253, Russell Senate Office Building, Hon. Ben Ray Luján, Chairman of the Subcommittee, presiding.

Present: Senators Luján [presiding], Cantwell, Klobuchar, Blumenthal, Schatz, Markey, Baldwin, Rosen, Thune, Fischer, Blackburn, Lee, and Scott.

OPENING STATEMENT OF HON. BEN RAY LUJÁN, U.S. SENATOR FROM NEW MEXICO

[Technical problems.]

Senator LUJÁN.—today is holding a hearing on disrupting dangerous algorithms, addressing the harms of persuasive technology, to examine the risks posed by algorithmic amplification. As we have heard from testimony in previous hearings this year, algorithms, automation, and artificial intelligence have deep consequences for the health of our democracy and civil discourse, equal access to critical information, and the mental and physical health of our children.

This hearing will focus on solutions that Congress and regulators can take to ensure these important innovations benefit all Americans and safeguard against potential harms. Today, more of our lives are lived online than ever before. Over the pandemic, the number of Americans using telehealth services more than tripled. More of us rely on the Internet for work, for school.

Online platforms like Facebook, Twitter, YouTube, TikTok, Snapchat, and Amazon connect us to news, economic opportunity, and our friends and family. Online platforms helped Americans stay connected and access basic services during the pandemic. However, this exchange has come with a cost. Founded on innovative and disruptive business models, these companies have come to rely on algorithms. Data scientists and engineers at these companies design these algorithms to predict the content that is most likely to provoke a response and in turn amplify that content to users. Rather than users choosing what they see online, these algo-

rithms make the decision for them to maximize growth and revenue.

Civic health and well-being of consumers come second. If there was ever any doubt that business models and consumer interests were in conflict, Frances Haugen's testimony put those notions to rest. Her work and the documents she uncovered showed repeated underinvestment from Facebook in civic integrity, and in the health of minority communities at home and non-English speaking populations globally.

She showed that Facebook had internal warnings that the platform was changing the global political conversation to be more extreme because of the content that it amplified. She showed that the algorithms favored emotions like anger and outrage due to deliberate decisions made at the highest levels of the leadership of these companies. We are here to chart a course forward.

The Internet was created in the United States. ARPANET, the First Amendment, Section 230, each of these contributed to U.S. leadership in tech and innovation. It is time for the United States to step up and again to protect these principles in the future while also accounting for the harms. We know there is a lot to do, but there is much that our constituents across the country agree on here. First, constituents want to have control over their personal information. Second, they want transparency for what tech platforms do with that information.

Third, they want oversight that can ensure these protections. And finally, they want accountability when platforms are negligent or actually harm Americans. It's all common sense. I don't know how we can't find common ground in each and every one of these areas, and it is clear based on the hearings that have come out of the Commerce leadership, this action is needed.

Now we know Americans want more control over their data. These automated algorithms rely on user data to target consumers at the exact moment they are most likely to cause a change in behavior. Laxed oversight of data brokers, opaque and complicated collection practices, and insufficient disclosure all contribute to the harms these persuasive algorithms have to our health and well-being. Second, we need to know what is going on within these companies.

Ms. Haugen described the internal sentiment of Facebook that, "if information is shared with the public, it will just be misunderstood." This is frankly insulting to the American people. We need more public transparency that allows for meaningful public oversight and discourse over the true impact these platforms have on our daily lives. Third, we need to strengthen our existing institutions.

The Federal Trade Commission, the States Attorneys General seek to protect consumers against harmful practices. With adequate resources, they can step up to this role. That is why I introduced the FTC Technologies Act to improve the Commission's ability to understand the dangers and protect consumers against harmful technologies. We must also strengthen local journalists and broadcasters to continue to act as checks to power and to live up to their roles as trusted voices in the communities that they serve.

Finally, we need accountability when tech platforms are negligent and actively cause harm. That is why I also introduced the Protecting Americans from Dangerous Algorithms Act with the support of Senator Whitehouse and Representatives Malinowski and Eshoo. Platforms that have consequences for actively amplifying content that deprives Americans of their civil rights or contributes to terrorist activity. We may have a lot to do, but we are also making progress. The reconciliation package before the Senate makes historic investment in privacy enforcement at the Federal Trade Commission.

The bill greatly improves the FTC's ability to go after bad actors by expanding its fining authority, and with a number of bipartisan bills to consider, Congress has the opportunity to make meaningful reforms. So I thank our witnesses for testifying today. Who is joining us remotely, Ms. Jessica González is the Co-Chief Executive Officer at Free Press Action. Ms. González has long been an advocate—advocating for the protection of minority communities and civil rights online, and I look forward to her perspective on that topic.

Ms. Rose Jackson is the Director of Democracy in Tech Initiative at the Digital Forensic Research Lab with the Atlantic Council. She will provide important context for the business models that incentivize these algorithms and the global context in which they operate. Dr. James Poulos is Executive Director of the American Mind at the Claremont Institute, and he will provide a broader context for algorithm and digital regulation.

Professor Dean Eckles is an Associate Professor of Marketing at the MIT Sloan School of Management and will provide testimony on the technical details on how these algorithms work and what measures, effective regulation should we consider. I want to thank Ranking Member Thune and his staff for their work to hold this hearing. And with that, I recognize—I will recognize the Ranking Member for remarks when he joins us. And I think we are going to go to our witnesses. And Ms. Jackson, we will hear from you first.

STATEMENT OF ROSE JACKSON, DIRECTOR, DEMOCRACY + TECH INITIATIVE, DIGITAL FORENSIC RESEARCH LAB, ATLANTIC COUNCIL

Ms. JACKSON. Thank you, and good morning, Chairman Luján, Ranking Member Thune, and all of the members of the Committee. Thank you for the opportunity to appear here before you today. My name, as you said, is Rose Jackson. I am the Director of the Democracy and Tech Initiative at the Atlantic Council's Digital Forensic Research Lab.

My work focuses on knitting together siloed conversations around tech governance, and that matters because the way that we fund tech, design it, govern it, fundamentally impacts democracy at home and abroad. Today's Internet is an outgrowth of incentives of global growth and financial gain. The Internet has connected the world and brought tremendous opportunity to billions. But the incentives that underpin it have also given rise to models that harm individuals and our democracy itself.

To successfully address these tensions, whether to mitigate the impact of algorithms, limit consolidation or anti-competitive behavior, protect human rights, or otherwise make the online world safer and fairer, we must recognize and address these incentives, as well as the complex and interconnected nature of the challenge. It is essential to acknowledge that the United States is not alone in this conversation. With our allies and our adversaries are actively trying to dictate the future of the global network, our allies are exploring sometimes conflicting solutions for how to reconcile new network challenges with deeply held democratic values. Meanwhile, authoritarian countries like Russia and China are taking an entirely different approach.

They are driving an alternative vision for the Internet that is incompatible with our constitutional democracy and universal human rights. If they can drive a wedge between the world's democracies, they can reinforce their control at home, while limiting civic space online for everyone. And because the Internet is systemic, the rights that Americans are insured offline cannot exist in the online world if we don't continue to bolster the human rights based model internationally.

Doing so requires us to answer our own tech policy gaps. And in that vein, Congress has an essential role in reestablishing U.S. leadership on these issues and incentivizing a safer and more accountable online experience for all Americans. Today, our digital world has grown to mediate nearly every aspect of our lives, and much of this ecosystem is made up of private companies, the majority of which are headquartered here in the United States.

That means this committee in particular, can play a decisive role. It is hard to scroll through the news today without seeing stories about the latest tech scandal. Many of these harms stem from the same root cause succinctly identified by Mark Zuckerberg when he appeared before this very committee 3 years ago. When he was asked about how Facebook sustains a business model in which users don't pay for services, Zuckerberg famously responded, Senator, we run ads. And it is the heart of the issue. It is not advertisements per se, but a particular business model of data extraction, user segmentation, targeted personalized, value maximized advertising.

This model, which has powered much of the explosive growth of the internet's most successful and profitable firms, including social media companies, has an entire industry set on a race to gather as much information about us as possible, tracking us wherever we go, maximizing our time on their platforms, and feeding us any number of diversions to keep us clicking away.

An extremely profitable intermediary market cleans, repackages, aggregates, and labels your data for anyone who wants to buy it, and that is either a shoe company or even a foreign intelligence agency. In the absence of meaningful privacy legislation, all of this is legal and very profitable.

Given that engagement metrics and advertising revenue are some of the primary indicators of stock valuations, one could argue that in the status quo, many companies have a fiduciary responsibility to pursue data collection and engagement at all costs. But

those costs are paid by people. And that can impact everything from someone's job prospects to their physical safety.

The erosion of privacy, the algorithmic amplification of harmful content, and the compromise of information integrity all pose serious risks to our democracy and global stability. We must bring together all actors, including legislators like yourselves, industry leaders, and civil society experts to solve our problems together.

And this means breaking down silos in Government and policy practices, improving our understanding of information ecosystems and the platforms that operate within it, strengthening our Government's ability to set and enforce the rules, and iterating our approaches as technology innovates.

I provided a more expansive set of recommendations in my written testimony, but I wish to leave you with five key recommendations. First, Congress should work urgently to pass comprehensive Federal data protection and privacy legislation. Second, in the meantime, it should create and resource a new bureau at the FCC to address online privacy, data security, and other online abuses, as has been recommended by many in this committee and referenced by the Chairman just now and written into the House version of the Build Back Better Act.

Third, Congress should also advance legislation to foster greater transparency and accountability around online harms, and address information asymmetries between companies and everyone else. Fourth, the Biden-Harris Administration should identify a lead at the White House to set a unified tech policy, bridging foreign and domestic priorities, and coordinating a more cohesive rights respecting approach across Government.

And finally, the Administration also should integrate and elevate tech policy and U.S. diplomatic engagement to ensure the United States is a strong partner for the free, open, secure, and interoperable digital world. I am encouraged by the work of this committee and honored to be asked to testify. I submit the remainder of my testimony for the record, and I look forward to your questions. Thank you.

[The prepared statement of Ms. Jackson follows:]

PREPARED STATEMENT OF ROSE JACKSON, DIRECTOR OF THE DEMOCRACY + TECH INITIATIVE, DIGITAL FORENSIC RESEARCH LAB, ATLANTIC COUNCIL

EXECUTIVE SUMMARY

Good morning, Chairman Luján, Ranking Member Thune, and all the members of the committee. Thank you for the opportunity to appear before you today. It is an honor to testify on this important topic.

My name is Rose Jackson, and I'm the Director of the Democracy + Tech Initiative at the Atlantic Council's Digital Forensic Research Lab. My work focuses on knitting together the often siloed conversations around tech governance through the lens of democracy and human rights. This is relevant to this committee because the way that tech is funded, designed, and governed fundamentally impacts democracy at home and abroad.

The internet, and today's dominant platforms, are an outgrowth of incentives–sometimes competing, and sometimes complementary–of global growth and financial gain. Together, we have built a wildly successful network that has connected the world and brought tremendous opportunity to billions. But these same incentives have also given rise to business models that exploit and extract value in ways that harm individuals and our democracy itself.

We all share a goal of maximizing the best parts of our connected world, while minimizing its harms. If we are to successfully address these tensions, whether to

mitigate the impact of algorithms, limit consolidation and anti-competitive behavior, protect human rights, or otherwise make the online world safer and fairer, we must start with an approach that recognizes and addresses these underlying incentives, and the complex and interconnected nature of the challenge.

It is essential to acknowledge that the United States is not alone in this conversation. Other countries–from our allies to our adversaries–are actively regulating, legislating, and dictating the future of the global network. Allies like Canada, the United Kingdom, and the European Union are all exploring different, and sometimes conflicting, approaches to these same problems and platforms, seeking solutions for how to reconcile new networked challenges with deeply held democratic values.

Meanwhile, authoritarian countries like China and Russia are taking an entirely different approach. They are proactively driving an alternative vision for the Internet that is incompatible with our constitutional democracy and universal rights. The authoritarian strategy benefits from a fragmented approach to the internet. If they can drive a wedge between the world's democracies, they can reinforce their control at home while limiting civic space online for everyone.

And because the Internet is systemic, the rights Americans are ensured offline can't exist in the online world if we don't continue to promote and bolster the human rights-based model internationally. Doing so requires us to answer our own tech policy gaps. If we don't, the world will decide these things for us.

Congress has an essential role to play in re-establishing U.S. leadership on these issues and incentivizing a safer and more accountable online experience for all Americans. The stakes couldn't be higher. Our failure to act threatens our national security, democracy, and global competitiveness.

Today, our digital world has grown to mediate nearly every aspect of our lives, from the conduct of business to the exercise of our basic rights. Much of this essential ecosystem is made up of global private companies, the majority of which were founded and remain headquartered here in the United States. That means that this committee in particular plays a decisive role in shaping the incentives and ensuring protections for the platforms, providers, creators, and individuals that make up the digital ecosystem.

It's hard to scroll through the news today without seeing stories about the latest tech scandal, whether whistleblower disclosures, hacking revelations, or the dystopian use of facial recognition tools. As the world grows disillusioned with an increasingly toxic digital experience,[1] we find many of these harms stem from the same root cause, succinctly identified by Mark Zuckerberg when he appeared before this committee three years ago. When asked about how Facebook sustains a business model in which users don't pay for its services, Zuckerberg famously responded, "Senator, we run ads."[2]

This is the heart of the issue. Not advertisements, per se, but a particular business model of data extraction, user segmentation, and targeted, personalized, value-maximized advertising.

This model, which has powered much of the explosive growth of the internet's most successful and profitable platforms, has set an entire industry on a race to gather as much information about us as possible, tracking us wherever we go, maximizing our time on their platforms, and feeding us any number of diversions to keep us clicking away.

And it's not just social media companies in on the game. An extremely profitable intermediary market, consisting of thousands of companies you've likely never heard of, cleans, repackages, aggregates, and labels your data for anyone who wants to buy it—whether a shoe company or a foreign intelligence agency.

In the absence of meaningful privacy legislation, all of this is legal and highly lucrative. Given that engagement metrics and advertising revenue are the primary indicators that determine many companies' investment and stock valuations, one could argue that, in the status quo, these companies have a fiduciary responsibility to pursue data collection and engagement at all costs.

But those costs are paid by people and can have serious ramifications on everything from someone's job prospects to physical safety. The erosion of privacy, algo-

---

[1] Brooke Auxier, "64 percent of Americans Say Social Media Have a Mostly Negative Effect on the Way Things Are Going in the U.S. Today," Pew Research Center, October 15, 2020. *https://www.pewresearch.org/fact-tank/2020/10/15/64-of-americans-say-social-media-have-a-mostly-negative-effect-on-the-way-things-are-going-in-the-u-s-today/*.

[2] *The Washington Post."*Transcript of Mark Zuckerberg's Senate Hearing," April 11, 2018, *https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/*.

rithmic amplification of harmful content, and the compromise of information integrity all pose serious risks to our democracy and global stability.

The issues are challenging, but the same ingenuity that built the Internet can be harnessed for the right solutions. We must bring together all actors, including legislators such as yourselves, industry leaders, and civil society experts, to solve our problems together. This means breaking down silos in government and policy practices; improving our understanding of our information ecosystem and the platforms within it; strengthening our government's ability to set and enforce the rules; and iterating our approaches as technology moves forward.

I have provided a more expansive set of recommendations in the written testimony which I have submitted for the record. But I wish to leave you with five immediate, actionable things that would make a real difference in addressing the issues we are gathered to discuss today.

1. For Congress: Pass comprehensive Federal data protection and privacy legislation.
2. For Congress: Create and resource a new bureau at the FTC to address online privacy, data security, and other online abuses, as provided for in the Chairwoman's Consumer Online Privacy Rights Act (COPRA) and the House version of the Build Back Better Act.
3. For Congress: Advance legislation to foster greater transparency and accountability around online harms, and address information asymmetries between companies and everyone else.
4. For the Administration: Identify a lead at the White House to set a unified tech policy, bridging foreign and domestic priorities, and coordinate a more cohesive rights-respecting approach across the government.
5. For the Administration: Integrate and elevate tech policy in U.S. diplomatic engagement to ensure the United States is a strong partner for the free, open, secure, and interoperable digital world.

The goal of these recommendations is not to remove all bad things from the Internet or expect human nature itself to change. But rather, to provide the mechanisms necessary in a democracy for the public, government, and civil society to play their roles, in establishing clear expectations and rules, developing shared information, and relying on avenues for recourse to address harms when they happen.

I am encouraged by the work of this committee and honored to be asked to testify. I submit the remainder of my testimony for the record and look forward to your questions.

GETTING TO THE ROOT OF THINGS

The Business Model

The Internet has become essential to modern life. We use it to conduct business. We use it to learn. We use it to stay connected with our family and friends. And we use it to access government services and exercise our basic democratic freedoms.

We often think of the Internet as an abstract idea, but its existence depends on a complex system of hardware and software. And today, most of those components from servers to websites, are built and run by private companies, each with their own business models. These models can take a range of forms, from your Internet service provider charging you a monthly fee to a marketplace taking a percentage from the sales price of those shoes you bought.

Of course, platform advertising is a business model, too. The particular personalized, targeted advertising business model that has powered much of the explosive growth of the Internet has set companies on a race to gather as much information about us as possible, including by maximizing our time on their platforms.

The Incentives

We produce an incredible amount of personal data points each day. The websites you visit and what you do on them. The details of your husband's grocery store run. The cell towers your phone pinged. What you typed in that search bar. When tracked and combined, it provides a shockingly accurate picture of a person's interests and behavior—a picture worth a lot of money to a lot of different potential buyers. According to a recent Aspen Institute report, in 2020 alone, the digital adver-

tising market accounted for approximately $356 billion, with Google taking nearly 29 percent of the market, Facebook 25 percent, and Amazon 10 percent.[3]

With personal data worth so much, and with so few rules limiting its collection and use, almost everyone has an incentive to track and make money off of what we do online. Platforms have an incentive to supercharge your use of their services, because the more you use them, the more they know about you. An extremely profitable intermediary market, consisting of thousands of companies you've likely never heard of, cleans, repackages, aggregates, and labels your data for anyone who wants to buy it—whether a shoe company or a foreign intelligence agency. All of this is legal and highly lucrative.

The platform design features and policies (such as recommendation algorithms or content moderation policies) are inevitably shaped by these monetary incentives. Given that engagement metrics and advertising revenue are the primary indicators that determine social media companies' investment and stock valuations, one could argue that, in the absence of any new legislation, these companies have a fiduciary responsibility to pursue engagement at all costs.

Those costs are not paid by technology platforms. They are paid by us, American citizens. And their toll is pervasive, from the types of jobs we find to the mortgage rates we're offered. They are often nearly invisible, as well. We aren't informed about what opportunities are withheld from us because of the decision of an algorithm. We can't know what our better future might have been. This shapes our ability to choose the path our lives travel and exposes us to real risks.

UNDERSTANDING THE HARMS

In a democratic society, the government has a duty to protect our rights and companies have a responsibility to respect our rights. However, that social contract is not reflected online in the United States today. While there are numerous harms stemming from our lack of tech sector regulation, in my testimony today, I'll focus on three broad categories: the erosion of privacy, algorithmic amplification of harmful content, and the compromise of information integrity.

Individual privacy is a bedrock American right. It is also foundational to democracy but currently in peril. As citizens, we expect to have the ability to express ourselves, assemble, and otherwise conduct our lives without surveillance. While we pay a great deal of attention to limiting the powers of the state in this regard, when it comes to commercially driven privacy protections online, the United States is on an island by itself.

Most countries have placed some restrictions on how an individual's data—whether personal details or behavior on and offline—can be used. But the lack of U.S. protections means the business of tracking Americans is quite lucrative. This financial upside incentivizes product approaches (*e.g.,* certain algorithms) and policy decisions (*e.g.,* what is and isn't allowed on a platform), designed to increase your engagement and generate more, and more valuable, data.

We are most often unwitting participants in this exchange. For example, a company may produce an app that millions of people like to use to make funny videos. But that app's primary business could be sourcing faces to train algorithms or to track your location to sell to a third party, all without you knowing.

Other platforms aren't just tracking you on their own apps, they follow you onto other sites, on your phone, or in some cases into the physical world. They combine the sum total of these data points to enable everyone from advertisers to political parties to better target you. But the network of data brokers I mentioned before means that this highly personalized information can be purchased by almost anyone for almost any purpose. This includes the U.S. and foreign governments.[4]

What's more, if a company fails to secure your data and a hacker steals it, there's little to nothing you can do. Like me, you've probably received a dozen or more e-mails about private information like your credit card data, social security number, and purchase history being leaked in a data breach. But given the state of our laws today, there are few, if any, consequences for the companies you entrust your data to. There's no Federal law to require them to protect your data, and the FTC can only really go after companies if they were deceptive about the security promises they made to you.

---

[3] Aspen Digital, "Commission on Information Disorder Final Report," Aspen Institute, November 2021, *https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute_Commission-on-Information-Disorder_Final-Report.pdf.*

[4] Justin Sherman, "Data Brokers Know Where You Are—and Want to Sell That Intel," *Wired,* August 8, 2021, accessed December 7, 2021, *https://www.wired.com/story/opinion-data-brokers-know-where-you-are-and-want-to-sell-that-intel/.*

Data I don't even know exists about me can be bought and sold without my knowledge, and then it can be used for everything from convincing me to buy new clothes to determining if my health insurance premiums should go up.

The privacy invasions here get worse when combined with algorithmic decision-making. Imagine that you have a fitness tracking app that shows that you recently stopped exercising as much. At the same time, you join your local bar's loyalty program that shows that you've started drinking more. Despite the fact that you may have just lost your Apple Watch or bought rounds of drinks for your team at work, a bank's algorithm might combine these data points and label you as a depressed alcoholic, leading you to be denied for a loan and hurting your credit score in the process.[5]

In more authoritarian contexts, the data we generate just by using the Internet to click on posts and "like" things can be used to identify activists and members of vulnerable communities. Corporate-held data is the fuel of the state surveillance machine, and it's relatively trivial for government actors around the world to track the movements of religious minorities, opposition parties, LGBTQ individuals, and human rights defenders. For every harm you can think of on the internet, the people most impacted are almost always the most vulnerable in society.

Another harm is the erosion of the shared set of facts that democracy depends on. Camille Francois, a Lecturer at Columbia's School of International and Public Affairs, has used the term "viral deception" to focus conversations about the fragility of the information ecosystem on the manipulative actors, deceptive behaviors, and harmful content that combine to undermine democracy and target individuals.[6]

While people often think of harms in this category as related to speech, solely focusing on content misses significant pieces of the puzzle. Microtargeting tools and recommendation engines are amplifying these dangerous messages and delivering them to those most susceptible.

As researcher Renee DiResta has argued, speech and reach are not the same things.[7] We must consider the harms amplified, microtargeted, or otherwise orchestrated through particular platform features or products. And further think of them in a multi-platform and multi-mode ecosystem.

This includes everything from the ability to stoke public panic–as the Russian Internet Research Agency (IRA) did through coordinated messaging to convince a parish in Louisiana it was under imminent threat from a nonexistent chemical incident–to the deceptive advertising of harmful products, or the facilitation of outright illegal activities such as child trafficking or drug sales.[8] It also includes the broader breakdown of public trust and open dialogue required for a functioning democracy. Of course, the events in Myanmar–where the military and a group of extremist monks leveraged Facebook to unleash genocidal violence against the Rohingya people–reminds us of how severe the potential harms can be.[9]

To add to these dynamics, with the way real-time bidding for online ads works, many if not most advertisers don't even know what content their ads appear alongside, leading to sources of misinformation and radicalization directly profiting from this ecosystem as well. Indeed, a large part of the misinformation ecosystem would not exist without the ad ecosystem adding fuel to its fire. And this is independent of the social media platform systems, because even if a business, individual, or group is deplatformed, their websites can continue to make money from advertising, bolstered by the audience they built through social media.

As study after study has shown, because content that outrages leads people to keep watching and clicking, companies will keep showing harmful content to users

---

[5] Martin Tisne, "It's Time for a Bill of Data Rights," *MIT Technology Review,* December 14, 2018, accessed December 7, 2021, *https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights/*.

[6] Camille Francois, *Briefing for the United States House of Representatives Committee on Science Space and Technology,* Investigations and Oversight Subcommittee Hearing on Online Imposters and Disinformation, Graphika, September 26, 2019, *https://science.house.gov/imo/media/doc/Francois%20Testimony.pdf*.

[7] Renee DiResta, "Free Speech Is Not the Same as Free Reach," *Wired,* August 30, 2018, *https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/*.

[8] Camille Francois, *Briefing for the United States House of Representatives Committee on Science Space and Technology,* Investigations and Oversight Subcommittee Hearing on Online Imposters and Disinformation, Graphika, September 26, 2019, *https://science.house.gov/imo/media/doc/Francois%20Testimony.pdf*.

[9] Human Rights Council, "Report of the Independent International Fact-Finding Mission on Myanmar," September 2018, *https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf*.

regardless of the consequences for the users or our society.[10,11,12] That applies whether it be self-harm videos, sexualized images of children, calls for violence, or falsehoods about a politician.

These challenges are inherently linked. The invasion of our privacy at the hands of the internet's advertising-driven business model leads to the microtargeting and amplification of harmful content, which in turn compromises the integrity of information online, all raising important questions about what the appropriate rules of the road should be for companies operating in this space.

We have to avoid the trap of siloing our conversations to single harms, jurisdictions, or policy practices that end up missing the interrelated nature of business models, platform design, policy architecture, and user behavior.

BARRIERS TO A HEALTHIER ECOSYSTEM

While there are certainly no silver bullets to these interrelated issues, this section is about approaches that will lead to better policy outcomes across the space. Two challenges in particular have hampered effective responses.

Policy and Issue Silos

The first challenge is that, for the most part, we discuss the Internet and issues with it in defined policy silos. For instance, this Committee might examine everything from business regulation and trade to privacy and content moderation. The Judiciary Committees focus on antitrust and competition issues; the Foreign Relations Committees on geopolitical tech competition with countries like China; the Homeland Security Committees on cyber-and infrastructure security. And the Intel Committees focus on online drivers of radicalization or foreign influence operations. This dynamic is replicated in the executive branch. Each committee or agency focuses on the same platforms, ecosystems, and issues, but they are often doing so in isolation.

This hearing is focused on how to address online harms exacerbated or created by the technologies, policies, and designs of various platforms. The truth is that each one of the above policy issues is interconnected and essential in some form to address the harms we are focusing on in this hearing. Siloing our conversations to single harms, jurisdictions, or policy practices ends up missing the interrelated nature of business models, platform design, policy architecture, and user behavior.

Laying out the complexity of this ecosystem isn't meant to cause policy paralysis or inaction for fear of focusing on the wrong thing. It's meant to encourage a more holistic approach that unlocks broader coalitions and better solutions.

The Lack of Information and Explainability

The second challenge is our limited understanding of the information ecosystem and how it operates within societies. The open-source research community has been able to increasingly track networks seeking to manipulate platforms and populations. But it is undeniable that companies have more information on how harms are perpetrated on their platforms than anyone else. They do not, however, have cross-platform visibility and are often siloed internally, meaning they may not track or examine the ways different business lines incentivize harms in another area of the company. Further, their own terms of service sometimes outright prohibit the kinds of open research that can add valuable context to our understanding of the information ecosystem.[13]

Even with the best of intentions, platforms alone cannot solve these problems. But for civil society, researchers, journalists, and governments to play their role, there need to be better mechanisms for understanding how companies operate, what their technology is doing, and how people are using or misusing their tools in ways that drive harm for society and individuals.

---

[10] William J. Brady, Killian McLoughlin, Tuan N. Doan, and Molly J. Crockett, "How Social Learning Amplifies Moral Outrage Expression in Online Social Networks," *Science Advances* 7 (33): eabe5641, 2021, *https://doi.org/10.1126/sciadv.abe5641.*

[11] Kate Starbird, Ahmer Arif, and Tom Wilso,. "Disinformation as Collaborative Work," *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–26, 2019, *https://doi.org/10.1145/3359229.*

[12] Dag Wollebaek, Rune Karlsen, Kari Steen-Johnsen, and Bernard Enjolras, "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior," *Social Media + Society* 5 (2): 205630511982985, 2019, *https://doi.org/10.1177/2056305119829859.*

[13] Marshall Erwin, "Getting Serious about Political Ad Transparency with Ad Analysis for Facebook—Open Policy & Advocacy," Open Policy & Advocacy, October 18, 2018, *https://blog.mozilla.org/netpolicy/2018/10/18/getting-serious-about-political-ad-transparency-with-ad-analysis-for-facebook/.*

"Transparency" has become the watchword of the day, perhaps the single greatest point of agreement in the tech policy community. But few people can articulate exactly what transparency should mean. Is it the disclosure of unlimited data? The release of company-scoped transparency reports or impact assessments? Reporting on enforcement? Or something else entirely? Transparency is a means, not an end. So while working to advance improved information and data access, it's important to be clear what we want from that information, which may be case specific, but should always be focused on enabling accountability, the protection of individual rights and privacy, and prevention of harms.

For example, if a goal is explainability, we might then be focused on questions around how algorithms are intended to work, how they are trained, and how they influence the content people see. This is a more specific end than unscoped disclosure.

There are of course a number of other barriers to action, including the lack of empowered and resourced regulators. But I want to focus now on the broader context in which this hearing takes place.

THE GLOBAL CONTEXT

As a country we are behind on setting the rules needed to protect rights online. Our companies already comply with a myriad of foreign national and U.S. state laws on everything from privacy to content moderation. That patchwork of laws sometimes brings *de facto* improvements and protections to U.S. citizens, and other times undermines their basic human rights. As countries around the world grapple with how to address many of the same concerns we will discuss today, it's helpful to learn from their experimentation and consider U.S. action in the context of an urgent and existential global competition.

Europe has been setting the digital rules of the road for years, starting most notably with the General Data Protection Regulation (GDPR), which set the global standard leading everyone from Brazil to Kenya to legislate basic data protections for its citizens. The United States is an outlier on this issue, and that leaves Americans uniquely vulnerable. Most U.S. companies already comply with the GDPR and other data protection legislation, they just don't generally make those protections available to Americans.

Most recently though, Europe has jumped into a major, once-in-a-generation rewriting of the rules of the digital economy in the form of the Digital Services and Digital Markets Acts (DSA and DMA).[14,15] These two bills amount to the most significant rights-respecting effort at comprehensive tech regulation in history. Broadly, they cover everything from content moderation and the algorithms that shape our online experience to ads and commercial partnerships, as well as the data implications of mergers and acquisitions. For users, the outcomes will determine what they see online, how they can be tracked, and by whom. The bills will likely pass within the next year and set the global standard for determining which platforms meet criteria for regulation, content moderation norms, and requirements for transparency, reporting, and enforcement. With regard to algorithmic amplification specifically, the DSA would require covered platforms to make clear to users what targeting parameters are used to determine what they see through recommender systems, as well as provide an opt-out option for any personal data-based recommendations.[16]

Of course these bills are not perfect, and as they move through the European Parliament, a number of troubling provisions are under consideration that hew closely to those in other allied nations struggling to get it right. The United Kingdom and Canada are currently considering bills that would require companies to proactively

---

[14] Proposal for a Regulation of the European Parliament and Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.*

[15] Proposal for a Regulation of the European Parliament and Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020)0842, *https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0842/COM_COM(2020)0842_EN.pdf.*

[16] Proposal for a Regulation of the European Parliament and Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.*

monitor and remove ill-defined categories of "harmful" speech.[17,18] Australia has already passed a bill that requires this and mandates takedowns of such content within 24 hours of it being flagged. Australia takes things a step further and empowers a government authority to demand certain content be removed, without recourse for companies or users. Laws like these are proven to result in companies over-policing speech to avoid liability, while relying on algorithmic content moderation systems that do little to reduce real world harm.[19]

India, once a leader in democratic online governance, has recently implemented draconian rules that require platforms to take down content when requested by a government ministry, and to assign in-country staff dedicated to respond to these requests who are personally criminally liable if their companies refuse to do so.[20] This Indian law in particular is reminiscent of provisions recently leveraged in Russia threatening Google and Apple's in-country staff to compel the companies to remove an opposition party app from their platforms.[21]

These discrepancies in approach and embrace of undemocratic regulations bolster the efforts of China and other authoritarian countries proactively advancing an alternative vision for the internet. The consensus on a rights-based world order helped drive the adoption of the early principles stating that the Internet should be global, free, open, secure, and interoperable. Those principles helped spur the U.S. tech industry, and they still largely stand today. But they are being actively challenged by authoritarians who want a splinternet where they can be as repressive and controlling online as they are in the physical world, while leveraging the digital world to facilitate their centralized political control and sustained power.

The interests of authoritarians, from Russia to Iran, are well served by initiatives like China's Digital Silk Road, which is pouring billions of dollars into digital infrastructure. With nothing similar emerging from the world's democracies, many amongst the half of humanity currently unconnected to the Internet will take their first steps online into a state-owned, authoritarian-inclined digital landscape. At each step in their digital journey—from the fiber they connect through to the hardware and software they use to connect—their data will feed state-owned or backed enterprises that have shown few qualms supporting authoritarian agendas.

These countries are simultaneously leveraging the international system to advance their vision, seeking influence and control over the venues where norms and treaties around Internet policy are set. As we speak, countries are debating these issues in Krakow at the Internet Governance Forum, the main UN body for global, multi-stakeholder conversations on Internet policy. A Russian and an American are competing for the 2022 presidency of the International Telecommunication Union, a global treaty body which sets standards for global telecommunications, including the internet.[22] At the International Organization for Standardization, a Huawei senior director chairs the committee that sets global standards on AI and other technologies.[23] While authoritarian countries advance their preferences through the "rules-based order," democratic countries are falling behind.

Our companies will compete in this landscape and, as they have for years, respond to the regulations that are required of them. Each of these laws and actions are shaping our options. All of these foreign countries are deciding for us what the answer to these challenges will be.

---

[17] *Draft Online Safety Bill,* Presented to Parliament by the Minister of State for Digital and Culture by Command of Her Majesty, May 2021, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_SafetyBill_Bookmarked.pdf.*

[18] "The Government's Proposed Approach to Address Harmful Content Online," July 29, 2021, *https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.*

[19] Daphne Keller, "Empirical Evidence of Over-Removal by Internet Companies under Intermediary Liability Laws: An Updated List," Cyberlaw.stanford.edu, February 8, 2021, accessed December 8, 2021, *http://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.*

[20] Jochai Ben-Avie, "India Should Look to Europe as Its Model for Data Privacy," *Financial Times,* March 4, 2019, *https://www.ft.com/content/56ec37c8-39c0-11e9-9988-28303f70fcff.*

[21] "Google, Apple Remove Navalny App from Stores as Russian Elections Begin," Reuters, September 17, 2021, *https://www.reuters.com/world/europe/google-apple-remove-navalny-app-stores-russian-elections-begin-2021-09-17/.*

[22] Aaron Schaffer, "Analysis | U.S. And Russian Candidates Both Want to Lead the U.N.'s Telecom Arm," *The Washington Post,* October 12, 2021, accessed December 8, 2021, *https://www.washingtonpost.com/politics/2021/10/12/us-russian-candidates-both-want-lead-un-telecom-arm/.*

[23] Justus Baron and Olia Kanevskaia Whitaker, Global Competition for Leadership Positions in Standards Development Organizations, March 31, 2021, *http://dx.doi.org/10.2139/ssrn.3818143.*

And because the Internet is systemic, there isn't a world in which the rights Americans are ensured offline exist in the online world if we don't continue to promote and bolster the human rights-based model internationally. Doing so requires us to answer our own policy gaps on these issues.

To say it clearly, our lack of clear regulatory frameworks at home is a foreign policy weakness and a national security threat to our country.

RECOMMENDATIONS

The good news is that there are a number of things that this committee, other parts of Congress, the executive branch, industry, and the American public can do. Addressing these issues will require collective action–each of the following recommendations will be strengthened by a "multi-stakeholder approach;" that is, designing our policies to incentivize industry, empower civil society, center the American public and users, and strengthen the government's ability to set and enforce the rules. Regulation alone will not solve these problems, but the absence of it will make it hard for everyone else to play their roles.

We also must consider this policymaking in the global context and work closely with our allies to ensure we are not regulating at cross purposes. Perhaps more importantly though, U.S. leadership is necessary to help drive better global outcomes and ensure we have the ability to make these decisions for ourselves. U.S. foreign policy should prioritize rights-based tech governance, and, to do so, we need to center it in the highest levels of our diplomatic engagements. To that end, I am encouraged by Secretary of State Blinken's recent announcement creating a new bureau focused on tech diplomacy, reorganizing resources and expertise within the Department, and bringing in new people and skills to bolster the agency's capacity on these issues. Congress should ensure that this new bureau receives the resources and authorities it needs to fill this essential and unique role.[24]

Government Capacity to Set and Implement Tech Policy

But here there is an urgent need for the U.S. government to have a unified approach to tech policy, knitting together an overarching strategy for its foreign policy, trade priorities, and domestic imperatives, with the human-rights frame at its core. There are plenty of qualified officials spread throughout the government working on pieces of this broader issue set. *The Biden-Harris Administration* should name a Tech Policy lead, with a joint National Security Council, National Economic Council, Domestic Policy Council, and Office of Science and Technology Policy mandate, and formalize a working group to articulate clear areas of lead and support. This official should be tasked with reviewing the existing equities across the wide range of agencies and offices that touch these issues, work to develop a unified policy, and ensure the full force of U.S. power is moving in a common, rights-respecting direction.

For *Congress,* prioritizing action around protecting privacy, enabling transparency and accountability, and ensuring the U.S. government is appropriately staffed and resourced for our digital age would provide a meaningful foundation for many of the specific laws and rulemaking under consideration.

It's not just the State Department that needs the staff and mandate to drive better outcomes on technology. As the primary regulator of the tech industry, the FTC has increasing demands on it to oversee an industry that has grown exponentially. And yet, it has fewer total staff than it did in the 1970s and, in particular, woefully insufficient tech and data-specific staff to keep apace.[25,26]

The House version of the Build Back Better Act borrows from this committee's ideas and leadership and features significant resources to create and staff a new bureau at the FTC to address online privacy, data security, and other online abuses.[27]

---

[24] "Office of the Coordinator for Cyber Issues," United States Department of State, accessed December 8, 2021, *https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-coordinator-for-cyber-issues/*.

[25] *Group Letter in Support of FTC Privacy Funding,* September 21, 2021, *https://www.accessnow.org/cms/assets/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf.*

[26] The FTC is vastly underfunded and understaffed, particularly in comparison to the large, well-funded entities that it is tasked with regulating. Currently, the FTC only has 1,100 full-time employees (FTEs) to pursue both its competition and consumer protection missions. This number has been roughly flat over the past twelve years, and represents a substantial decrease from 1,746 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. In contrast, in 2020, Facebook alone had total revenues of nearly $86 billion and nearly 60,000 employees.

[27] Congress.gov. "Text—H.R. 5376—117th Congress (2021–2022): Build Back Better Act." November 19, 2021. *https://www.congress.gov/bill/117th-congress/house-bill/5376/text.*

Advancing those resources through the Senate would be a significant step forward on privacy and tech governance more broadly. Other efforts, like Chairman Luján's Technologists Act, could also help ensure the FTC has the capacity it needs to fill its essential role.[28] But the task of rulemaking and enforcement cannot sit with the FTC alone. The Federal Communications Commission (FCC), Consumer Financial Protection Bureau (CFPB), and others have significant roles to play. Congress should use the tools it has to help bolster staffing and expertise within those organizations, while also using comprehensive reform efforts to better define their responsibilities.

The same is true across the Federal government. Investments in the appropriate structure and staff to drive a cogent approach forward, whether in the Departments of Homeland Security, Defense, or Health and Human Services, will impact our ability to lead. Programs like Congress's own "Tech Congress" demonstrate the value of well-placed technologists in these roles. It also behooves Capitol Hill to find ways to break the legislative silos that exist around technology policy. Working across committee lines and jurisdictions needs to become the norm when approaching these questions.

To bring the point home, earlier this week, on December 7, the Senate Finance Subcommittee on Fiscal Responsibility and Economic Growth held a hearing on data brokers.[29] The witnesses all focused on the urgency of privacy legislation and the impact that the data broker market has on the issues under discussion at this hearing.

Congress could formalize or incentivize collaboration across the various Committees that share remit or responsibilities for tech policy and oversight. For instance, a caucus among Members or an informal forum for legislative staff to work together could serve an important purpose in generating ideas or deconflicting areas of lead and support among committees. This step would make it easier for experts to engage with Congress, as opposed to member by member or committee by committee.

Privacy

Substantively, the United States needs a comprehensive Federal data protection and privacy law. U.S. companies already comply with the GDPR in Europe and strong state laws in California and Illinois. Extending these protections to all Americans would help to shift the incentives currently driving many of the harms we discussed today and provide a base set of protections that make it easier to begin to address other tech governance challenges, from transparency to advertising. The bottom line is, every American should be able to control what data of theirs is collected, how it is used, and who has access to it.

In addition to pursuing this comprehensive approach, the committee should consider bolstering regulators' mandates for addressing data and privacy violations. For the FTC, section 5 is too limited as currently conceived. Further, with regulatory and enforcement jurisdiction on this issue spanning the FTC, FCC, CFPB, and DOJ, we need to better coordinate and ensure clearer understanding of how each body can approach its role on tech oversight in general. The only beneficiaries of a patchwork approach are special interest and the largest companies.

Transparency

It seems that almost everyone agrees that establishing *meaningful transparency and data-sharing standards* is a foundational requirement to address an array of digital issues. What such transparency should include, for which purposes, and what information is shared with which people are big questions we need to answer to ensure we don't legislate transparency for transparency's sake. With that said, Congress can and should take action to address the information asymmetry that exists between what companies know about their corner of the information ecosystem and what everyone else knows. This requires figuring out the mechanisms through which information can be securely and appropriately shared. Doing so can also help shape the questions we as a society are focused on in ensuring our technology reinforces our democracy.

To that end, I am encouraged by a slate of new legislative proposals in the U.S. Congress focused on this question, alongside major provisions in the European Union's DSA that mandate data sharing with regulatory authorities and qualified

---

[28] Congress.gov, "S.3187—117th Congress (2021–2022): Federal Trade Commission Technologists Act of 2021," November 4, 2021, *https://www.congress.gov/bill/117th-congress/senate-bill/3187*.

[29] "Promoting Competition, Growth, and Privacy Protection in the Technology Sector | the United States Senate Committee on Finance," December 8, 2021. www.finance.senate.gov, accessed December 8, 2021, *https://www.finance.senate.gov/hearings/promoting-competition-growth-and-privacy-protection-in-the-technology-sector*.

researchers, alongside potential risk-assessments and human rights impact reports.[30] Congress would be wise to build on the momentum created by this EU action and shape the direction both the EU and our own bodies take in incentivizing better information sharing and unlocking improved research.

It's worth noting that you would not be acting alone. In addition to the EU, the Organization for Economic Co-operation and Development and the United Nations are also advancing transparency-focused initiatives.[31,32] And I'm excited to announce a coalition my organization is jointly forming with the Global Network Initiative, the Institute for Strategic Dialogue, the Partnership for Countering Influence Operations, and the Center for Democracy and Technology, among others, that seeks to set common definitions, to better articulate the trade-offs, and to ensure each of the regulatory and policy efforts underway have a common grounding and language. There is much to work out in the details, but I am confident that this is an area where a great deal of progress can be made over the next year, and I hope our coalition's efforts, alongside these other initiatives, can inform the work of this committee and Congress more broadly.

With regard to social media algorithms specifically, proposals like those in the DSA, that provide some explainability and transparency to the user as to why they are seeing what they are seeing could be an important step in this larger conversation. However, doing so without giving the user the ability to change or remove those display algorithms would amount to transparency without control or accountability.

Which brings me to an important caution in the focus on transparency, which is that failure to tie it to accountability can result in chasing a bottomless pit of data, and what researcher Charley Johnson refers to as an endless transparency feedback loop, illuminating individual problems but not systemic drivers of those problems.[33]

Other Remedies

As we stay focused on remedies that address the underlying incentives driving online harms, it's worth calling out a number of proposals worthy of attention. The first is efforts to address the ad-based model driving many of these business incentives. The Honest Ads Act is a common sense option for migrating standards on political advertising that we already have on TV and radio to the digital sphere.[34] We should also consider proposals that require comprehensive disclosure of ads to researchers, such as the House Social Media DATA Act proposed by Representative Trahan.[35]

Efforts targeting virality as a unique characteristic of the problem could also have an impact—whether finding ways to introduce friction into sharing or prioritizing human review of content once it shows markers of potential viral spread.

If this list of recommendations sounds expansive, it's because it is. As I said at the beginning of this testimony, single interventions will not work in addressing the underlying incentives driving online harms. The menu of options available for action are all interconnected.

However, even if each of these things happened tomorrow, our digital world would still be fraught. The goal of these recommendations is not to remove all bad things from the Internet or expect human nature itself to change. But rather, to provide the mechanisms necessary in a democracy for the public, government, and civil society to play their roles, in establishing clear expectations and rules, developing shared information, and relying on avenues for recourse to address harms when they happen.

It's worth noting that the issues we're discussing do not sit with platforms and the technology they build alone. We won't solve all of society's ills through Internet governance. But we can work to ensure that the way platforms are funded, built,

---

[30] Proposal for a Regulation of the European Parliament and Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825, *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN*

[31] J. Llanos, Transparency reporting: Considerations for the review of the privacy guidelines," *OECD Digital Economy Papers,* No. 309, OECD Publishing, 2021, *https://doi.org/10.1787/e90c11b6-en.*

[32] The United Nations, "Our Common Agenda—Report of the Secretary-General," September 2021, *https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf.*

[33] Charley Johnson, "Some Unsatisfying Solutions for Facebook," Untangled, December 5, 2021. *https://untangled/p/-some-unsatisfying-solutions-for.*

[34] Congress.gov, "S.1356—116th Congress (2019–2020): Honest Ads Act," May 7, 2019, *https://www.congress.gov/bill/116th-congress/senate-bill/1356.*

[35] Congress.gov, "H.R. 3451—117th Congress (2021–2022): Social Media DATA Act," May 31, 2021, *https://www.congress.gov/bill/117th-congress/house-bill/3451.*

and governed at the very least does not exacerbate the harms we are discussing today.

I appreciate the Committee's leadership on these urgent issues and look forward to working together to address them.

Bibliography

Brooke Auxier, "64 percent of Americans Say Social Media Have a Mostly Negative Effect on the Way Things Are Going in the U.S. Today," Pew Research Center, October 15, 2020, *https://www.pewresearch.org/fact-tank/2020/10/15/64-of-americans-say-social-media-have-a-mostly-negative-effect-on-the-way-things-are-going-in-the-u-s-today/*.

Justus Baron and Olia Kanevskaia Whitaker, "Global Competition for Leadership Positions in Standards Development Organizations," March 31, 2021, *http://dx.doi.org/10.2139/ssrn.3818143*

Jochai Ben-Avie, "India Should Look to Europe as Its Model for Data Privacy," *Financial Times,* March 4, 2019, *https://www.ft.com/content/56ec37c8-39c0-11e9-9988-28303f70fcff*.

William J. Brady, Killian McLoughlin, Tuan N. Doan, and Molly J. Crockett, "How Social Learning Amplifies Moral Outrage Expression in Online Social Networks," *Science Advances* 7 (33): eabe5641, 2021, *https://doi.org/10.1126/sciadv.abe5641.*

Aspen Digital, "Commission on Information Disorder Final Report," Aspen Institute, November 2021, *https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute_Commission-on-Information-Disorder_Final-Report.pdf.*

Congress.gov, "Text—H.R. 5376—117th Congress (2021–2022): Build Back Better Act," November 19, 2021, *https://www.congress.gov/bill/117th-congress/house-bill/5376/text.*

Congress.gov, "S.3187—117th Congress (2021–2022): Federal Trade Commission Technologists Act of 2021," November 4, 2021, *https://www.congress.gov/bill/117th-congress/senate-bill/3187.*

Congress.gov, "S.1356—116th Congress (2019–2020): Honest Ads Act," May 7, 2019, *https://www.congress.gov/bill/116th-congress/senate-bill/1356.*

Congress.gov, "H.R. 3451—117th Congress (2021–2022): Social Media DATA Act," May 31, 2021, *https://www.congress.gov/bill/117th-congress/house-bill/3451.*

Renee DiResta, "Free Speech Is Not the Same as Free Reach," *Wired,* August 30, 2018, *https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/*.

Charles Duhigg, "How Companies Learn Your Secrets," *The New York Times,* February 16, 2012, *https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.*

Marshall Erwin, "Getting Serious about Political Ad Transparency with Ad Analysis for Facebook—Open Policy & Advocacy," Open Policy & Advocacy, October 18, 2018, *https://blog.mozilla.org/netpolicy/2018/10/18/getting-serious-about-political-ad-transparency-with-ad-analysis-for-facebook/*.

Camille Francois, *Briefing for the United States House of Representatives Committee on Science Space and Technology,* Investigations and Oversight Subcommittee Hearing on Online Imposters and Disinformation, Graphika, September 26, 2019, *https://science.house.gov/imo/media/doc/Francois%20Testimony.pdf.*

"Google, Apple Remove Navalny App from Stores as Russian Elections Begin," Reuters, September 17, 2021, *https://www.reuters.com/world/europe/google-apple-remove-navalny-app-stores-russian-elections-begin-2021-09-17/*.

"The Government's Proposed Approach to Address Harmful Content Online," July 29, 2021, *https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.*

Group Letter in Support of FTC Privacy Funding, September 21, 2021, *https://www.accessnow.org/cms/assets/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf.*

Human Rights Council, "Report of the Independent International Fact-Finding Mission on Myanmar," September 2018, *https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf.*

Charley Johnson, "Some Unsatisfying Solutions for Facebook," Untangled, December 5, 2021, *https://untangled.substack.com/p/-some-unsatisfying-solutions-for.*

Daphne Keller, "Empirical Evidence of Over-Removal by Internet Companies under Intermediary Liability Laws: An Updated List," Cyberlaw.stanford.edu, February 8, 2021,. accessed December 8, 2021, *http://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.*

J. Llanos, Transparency reporting: Considerations for the review of the privacy guidelines," *OECD Digital Economy Papers,* No. 309, OECD Publishing, 2021, *https://doi.org/10.1787/e90c11b6-en.*

"Office of the Coordinator for Cyber Issues," United States Department of State, accessed December 8, 2021, *https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-coordinator-for-cyber-issues/*.

"Promoting Competition, Growth, and Privacy Protection in the Technology Sector | the United States Senate Committee on Finance," December 8, 2021, accessed December 8, 2021, *www.finance.senate.gov.*

"Proposal for a Regulation of the European Parliament and Council on contestable and fair markets in the digital sector (Digital Markets Act)," COM(2020)0842, *https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0842/COM_COM(2020)0842_EN.pdf.*

"Proposal for a Regulation of the European Parliament and Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825," *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.*

Aaron Schaffer, "Analysis | U.S. And Russian Candidates Both Want to Lead the U.N.'s Telecom Arm," *The Washington Post,* October 12, 2021, accessed December 8, 2021, *https://*

www.washingtonpost.com/politics/2021/10/12/us-russian-candidates-both-want-lead-un-telecom-arm/.

Justin Sherman, "Data Brokers Know Where You Are—and Want to Sell That Intel," *Wired,* August 8, 2021, accessed December 7, 2021, *https://www.wired.com/story/opinion-data-brokers-know-where-you-are-and-want-to-sell-that-intel/*.

Kate Starbird, Ahmer Arif, and Tom Wilson, "Disinformation as Collaborative Work," *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–26, *https://doi.org/10.1145/3359229.*

Martin Tisne, "It's Time for a Bill of Data Rights," *MIT Technology Review,* December 14, 2018, accessed December 7, 2021, *https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights/*.

The Washington Post. 2018. "Transcript of Mark Zuckerberg's Senate Hearing," *The Washington Post.* April 11, 2018,. *https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/*.

The United Nations, "Closing Remarks 15th Annual Internet Governance Forum Internet Governance in the Age of Uncertainty," November 17, 2020, *https://www.un.org/en/desa/closing-remarks-15th-annual-internet-governance-forum-internet-governance-age-uncertainty.*

The United Nations, "Our Common Agenda—Report of the Secretary-General,". Published by the United Nations. September 2021,. *https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf.*

Dag Wollebaek, Rūne Karlsen, Kāri Steen-Johnsen, and Bernard Enjolras, "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior," *Social Media + Society* 5 (2): 205630511982985, 2019, *https://doi.org/10.1177/2056305119829859.*

Senator LUJÁN. Thank you, Ms. Jackson. Next, we will hear from Ms. González, the Co-CEO of Free Press. Jessica.

STATEMENT OF JESSICA J. GONZÁLEZ, CO-CHIEF EXECUTIVE OFFICER, FREE PRESS ACTION

Ms. GONZÁLEZ. Thank you, Chairman Luján, Ranking Member Thune, members of the Subcommittee. Thank you for inviting me to testify and please accept my condolences on the passing of your former colleague, Senator Dole.

Today's hearing calls us to address the harms of "persuasive technology." Of course, harmful and persuasive media is nothing new. As Free Press's media 2070 Project has documented, there is a long history of the U.S. media system spreading racist propaganda.

For instance, what is unique about the digital age is how online platforms collect troves of private data about us and then use it to target ads, recommendations, and other content based on our perceived interests and vulnerabilities. Sometimes this system produces innocuous or even beneficial outcomes.

But as whistleblowers, journalists, researchers, and activists have revealed, too often these systems cause grave harm, all while companies have little to no accountability to the American people. Indeed, they have failed outright at fulfilling even the most basic requests for transparency about how their systems work. They have rolled out expensive PR campaigns while continuing to profit handsomely from amplifying conspiracy theories and bigotry and enabling discrimination.

Tech firms are unwilling and unfit to effectively self-govern. They have amplified lies about COVID and vaccines, served up housing and employment ads in discriminatory ways, amplified voter suppression campaigns launched by foreign State actors, and discouraged participation in the U.S. census. They targeted abuse at people of color and have done a particularly poor job at solving these problems in languages other than English.

Facebook long has known the extent to which its products harm people of color, other minority groups, and our society. Its top executives have brazenly and routinely lied to or withheld the full

truth from civil rights leaders, researchers, the U.S. Congress, and the American people. This simply can't stand. This week, Free Press action and allies and the Disinfo Defense League released a policy platform designed to rein in these abuses.

Our main proposal for Congress is to adopt a comprehensive privacy and civil rights bill, which ideally would enshrine nine key concepts. Congress should limit text collection and use of our personal data, establish people's rights to control their own data, enhance data transparency, prevent discrimination by algorithms, increase platforms transparency about the known impacts of their business models, protect whistleblowers and external researchers, expand Federal Trade Commission oversight, encourage collaboration across agencies that hold specialized expertise, and set a Federal floor for consumer protection, not a ceiling. Fortunately, many of these elements are included in Senator Markey's Algorithmic Justice and Online Transparency Act, which prohibits algorithms that discriminate based on protected characteristics, and establishes safety and effectiveness standards.

And in the Consumer Online Privacy Rights Act, sponsored by Senators Cantwell, Schatz, Klobuchar, and Markey, which penalizes platforms that abuse personal data, allows people to see the information companies collect on them, and preserves a Federal private right of action. Free Press Action endorses both bills. But in addition to privacy and civil rights safeguards, we must invest in the media system we need to support a 21st century democracy.

Senator Cantwell's 2020 journalism report found local journalism is essential for healthy communities, competitive marketplaces, and a thriving democracy. I agree. Free Press Action and the Disinfo Defense League have proposed that Congress pass legislation to tax digital advertising and direct those monies to support high quality, noncommercial, and local journalism, including journalism by and serving people of color, non-English speakers, and other minority groups.

Let us make no mistake, tech companies are undermining public health, safety, civil and human rights, and our democracy, and they are doing so by extracting and exploiting our personal data. It is time for Congress and the FTC to act. Thank you, and I look forward to your questions.

[The prepared statement of Ms. González follows:]

PREPARED STATEMENT OF JESSICA J. GONZÁLEZ, CO-CHIEF EXECUTIVE OFFICER, FREE PRESS ACTION

Chairman Luján and Ranking Member Thune, Chairwoman Cantwell and Ranking Member Wicker, and other esteemed members of the Subcommittee: Thank you for inviting me to appear before you, and for seeking Free Press Action's views on how to rein in online platforms' harmful practices.

Today's hearing calls us to address the harms of "persuasive technology." Of course persuasive media is nothing new. For instance, as Free Press' Media 2070 project has documented, there is a long history of the U.S. media system being used to spread racist propaganda that legitimized and advanced the subjugation of Black people.[1] Yet the U.S. media system has been used for persuasion in the public inter-

[1] *See* Joseph Torres, *et al.,* "Media 2070: An Invitation to Dream Up Media Reparations," Free Press (Oct. 6, 2020), *https://mediareparations.org/wp-content/uploads/2020/10/media-2070.pdf.*

est as well, like for suicide prevention, tobacco warnings and other public-service announcements that support public health and safety.

What's unique about media persuasion in the digital age is how online platforms collect troves of private demographic and behavioral data about us all and then use it to target us with ads, recommendations, and other content based on our perceived interests and vulnerabilities. That data collection is pervasive, and may be invasive and extractive. Years of research, investigative journalism, activism and whistleblower revelations have illuminated that the companies collecting that data have little to no accountability to the American people. Indeed they have failed outright at fulfilling even the most basic requests for transparency about how their systems work and what they know about us. They haven't even attempted to redress the harms caused by their business models, which promote content to maximize engagement and profit handsomely from amplifying conspiracy theories and bigotry.[2]

Another novel aspect here is that, in part due to the sheer volume of clickbait pushed to users and the decimation of quality local journalism, people are consuming content not in ecosystems but largely in their own echo chambers. We each are seeing vastly different things—predicated on online platforms' abusive data practices. The divide between us all in what we see (and when we are largely unaware of what others see) means that we simply don't have the ability to fully ascertain who is being persuaded by what. Only platforms have the data about who sees what information and how much they engage with it. That gross imbalance is even more in focus now because platforms like Facebook have been shown to be aware of the negative impacts of their design and have failed to adapt it to prevent and mitigate harms.

Thus legislative and regulatory interventions ought to focus not on disrupting algorithms or shuttering persuasive technology *per se* but instead on mitigating its abuses and deterring the harms that companies employing it knowingly and negligently cause. This means prohibiting harmful data collection and use, including discriminatory algorithmic targeting, that runs afoul of civil and human rights, privacy rules, democratic norms, and public health and safety. Moreover, given how online platforms have polluted our information ecosystem, legislative approaches to invigorate local, independent journalism are ripe for examination.

Tech Companies Are Undermining Public Health, Safety, Civil and Human Rights and Our Democracy—And They're Doing So By Extracting and Exploiting Our Private Data

Nearly every day we learn about another tech company creating or exacerbating deep societal harms. Facebook's prioritization of profit at the expense of human rights and public safety—not to mention its now well-documented efforts to cover up its misdeeds—is too extensive to summarize here. The past few months of blockbuster revelations have confirmed, however, that Facebook is unwilling to self-govern effectively. And Facebook is not alone. Many other prominent and more obscure tech companies are similarly compromised by their own self-interests as they prioritize their profits over societal health.

To date, we know that tech companies have facilitated, profited from and sometimes even participated in activities that harm our democracy and voting rights, public health and safety, and other civil and human rights. To cite a few of the most prominent examples:

- Dangerous COVID–19 and vaccine conspiracy theories have proliferated over social media, exacerbating the public health crisis, impacting our hospitals and leading to far more death and serious illness than might otherwise have occurred. On Facebook, African Americans, Native Americans, Latinx people and other people of color were less likely to be shown credible public health information than White people.[3]
- Facebook served discriminatory ads to Facebook users in violation of the Fair Housing Act, prompting the U.S. Department of Housing and Urban Development to bring a lawsuit. Documents show that Facebook allowed advertising to target users based on location and other identity markers that could be proxies for protected categories, resulting in Black users seeing less or no ads for af-

[2] Jeremy B. Merrill and Will Oremus, "Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation," *The Washington Post* (Oct. 26, 2021), *https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/*.

[3] Corin Faife and Dara Kerr, "Official Information about COVID–19 Is Reaching Fewer Black People on Facebook," The Markup (Mar. 4, 2021), *https://themarkup.org/citizen-browser/2021/03/04/official-information-about-covid-19-is-reaching-fewer-black-people-on-facebook.*

fected housing. Research indicates that Facebook continued to run such ads on its platform more than a year after settling the initial complaint.[4]

- Twitter and Facebook have consistently failed to remove or flag as false content that discourages people from voting.[5] This content includes deception (lying about the time, place, and manner of voting); calls for boycott from individuals with alleged sponsorship ties to foreign state actors; and voter intimidation or threats, such as claims that people will show up to polling locations with guns.[6]
- Voter suppression campaigns over social media included surgical efforts to dissuade Black, Indigenous, and Latinx voters from turning out to the polls. False election and polling messages in non-English languages were much less likely to be taken down or flagged than similar messages in English.[7] Non-partisan organization Protect Democracy found that "[s]ocial media platforms were plagued by false content about various candidates for office, patently untrue information about electoral processes, systematic efforts to amplify bogus claims about voter fraud, and coercive political messaging tied to COVID–19 conspiracy theories. A great deal of this content targeted marginalized communities and, in particular, communities of color."[8]
- Internal Facebook research from 2019 brought to light by whistleblower Frances Haugen found that there was a concerted effort to discourage Latinx people from participating in the U.S. Census.[9] The company's research summarized posts "telling Hispanic[s] to not fill out the form; telling Hispanics not to participate in answering questions about citizenship; saying that people would be in danger of being deported if they participated; implying the government would 'get' immigrants who participated; and discouraging ethnic groups from participating."[10]
- Facebook has allowed alleged discriminatory employment ad targeting on the basis of gender and age.[11]
- Google's algorithms drive discriminatory search results, pushing users to image search results that under-represent women and women of color.[12] Research from 2018 showed its search terms related to Black girls mostly led to pornography, even when terms like "'porn,' 'pornography,' or 'sex' were not included in the search box."[13]
- In Free Press Action's statement for the record for this subcommittee's hearing "Shot of Truth: Communicating Trusted Vaccine Information," we documented

---

[4] Tracy Jan and Elizabeth Dwoskin, "HUD is reviewing Twitter's and Google's ad practices as part of housing discrimination probe," *The Washington Post* (Mar 28, 2019), *https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/;* Makena Kelly, "Facebook still runs discriminatory ads, new report finds," *The Verge* (Aug. 20, 2020), *https://www.theverge.com/2020/8/26/21403025/facebook-discriminatory-ads-housing-job-credit-hud.*

[5] *See, e.g.,* Young Mie Kim, "Voter Suppression Has Gone Digital," The Brennan Center for Justice (Nov. 20, 2018), *https://www.brennancenter.org/our-work/analysis-opinion/voter-suppression-has-gone-digital; see also* Ian Vandewalker, "Digital Disinformation and Vote Suppression," The Brennan Center for Justice (Sep. 2, 2020), *https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression.*

[6] *See* Kim, *supra* n.5.

[7] Samuel Woolley and Mark Kumleben, "At The Epicenter: Electoral Propaganda in Targeted Communities of Color," Protect Democracy (Nov. 2021), *https://protectdemocracy.org/project/understanding-disinformation-targeting-communities-of-color/#section-1* ("In Georgia, African Americans and Hispanic Americans were on the receiving end of sophisticated microtargeting efforts erroneously claiming that then-Senate candidate Raphael Warnock "celebrated" Fidel Castro. In Arizona, Hispanic American and Native American communities faced a cascade of untrue digital messaging over Twitter about the voting process. In Wisconsin, multiple communities of color from Madison to Milwaukee were targeted with lies about mail-in ballot fraud and ballot dumping." (internal citations omitted)).

[8] *Id.*

[9] Brian Contreras and Maloy Moore, "What Facebook knew about its Latino-aimed disinformation problem," *LA Times* (Nov. 16, 2021), *https://www.latimes.com/business/technology/story/2021-11-16/facebook-struggled-with-disinformation-targeted-at-latinos-leaked-documents-show.*

[10] *Id.* (internal quotation marks omitted).

[11] Noam Scheiber, "Facebook Accused of Allowing Bias Against Women in Job Ads," *New York Times* (Sep. 18, 2018), *https://www.nytimes.com/2018/09/18/business/economy/facebook-job-ads.html.*

[12] Xavier Harding, "Breaking Bias: Search Engine Discrimination? Sounds About White," Mozilla Foundation (Sep. 28, 2021), *https://foundation.mozilla.org/en/blog/breaking-bias-search-engine-discrimination-sounds-about-white/.*

[13] Dr. Safiya Noble, "Google Has a Striking Bias Against Black Girls," TIME (Mar. 26, 2018), *https://time.com/5209144/google-search-engine-algorithm-bias-racism/.*

how online platforms and broadcasters have both shirked their responsibility to the public and failed to mitigate harms for their roles in spreading dangerous disinformation that is designed to target Black, Latinx, AAPI, Indigenous, and other communities of color, as well as non-English speakers.[14]

As startling as these examples are, Free Press Action finds just as troubling the recent revelations that Facebook and other tech companies have long known exactly the extent to which their products were harming specific users and groups, and the lengths to which they have gone to cover up these harms rather than acknowledging and addressing them. We now know that Facebook refused to heed countless warnings from its own employees.[15] Facebook's top decision makers have brazenly and routinely lied to or withheld the full truth from me and other civil rights leaders, in meetings between company executives and leaders from the Stop Hate for Profit campaign, Change the Terms coalition, and Spanish-Language Disinformation coalition. Facebook has done the same to researchers, the U.S. Congress, and the American public. Facebook spent vast amounts of time and money running public relations campaigns to obfuscate the truth and pretend to fix its problems, instead of just investing to improve the integrity of its systems. And Facebook is far from the only bad actor here. In a meeting last year with Change the Terms coalition leaders, many YouTube executives showed an appallingly shallow grasp of civil and human rights.

Where Do We Go From Here?

Given the substantial challenges outlined above, how do we reset our information ecosystem to advance democracy, to prevent discrimination and abuse, and protect public health and safety? We need a comprehensive approach. Fortunately, there are solutions to the challenges we collectively face, and at least three of them have been introduced in legislation before this body already: The Fourth Amendment is Not for Sale Act (S. 1265), the Algorithmic Justice and Online Transparency Act (S. 1896), and the Consumer Online Privacy Rights Act (S. 3195).

Data Privacy and Civil Rights Legislation

Two days ago, in collaboration with three dozen other non-profit organizations—including Access Now, Common Cause, Demos, Cybersecurity for Democracy, and MediaJustice—that comprise the Disinformation Defense League, Free Press Action released a policy platform [16] designed to rein in technology companies' abuses. Our main proposal for Congress is to adopt a comprehensive privacy and civil rights bill,[17] which ideally would enshrine nine key concepts.

1. Congress should limit online platforms' and data brokers' collection and use of our personal data. Users should be able to control how apps use our data. We may want to share our data to receive services we sign up for, but apps should be prohib-

---

[14] *See* Carmen Scurato and Jessica J. González, Written Testimony for the Record, "Shot of Truth: Communicating Trusted Vaccine Information," U.S. Senate Committee on Commerce (Apr. 15, 2021), *https://www.freepress.net/sites/default/files/2021-04/free_press_action_written_testimony_shot_of_truth_hearing.pdf.*

[15] For example, the L.A. Times reported that the

leaked documents reveal substantial disagreement among staff about all sorts of issues plaguing the firm, with misinformation prominent among them.

The 2020 product risk assessment indicates one such area of dissent. After noting that Spanish-language misinformation detection remains "very low-performance," the report offers this recommendation: "Just keep trying to improve. Addition of resources will not help."

Not everyone was satisfied with that answer. "For misinfo this doesn't seem right . . . curious why we're saying addition of resources will not help?," one employee asked in a comment. "My understanding is we have 1 part time [software engineer] dedicated on [Instagram] detection right now."

A second comment added that targeted misinformation "is a big gap. . . . Flagging that we have zero resources available right now to support any work that may be needed here." (Redactions make it impossible to tell whether the same employee was behind both comments.)

In communications with the outside world, including lawmakers, the company has stressed the strength of its Spanish-language content moderation rather than the concerns raised by its own employees.

See Contreras & Moore, *supra* n.10.

[16] Disinfo Defense League, Policy Platform (Dec. 7, 2021), *https://www.disinfodefenseleague.org/policy-platform.* The Disinfo Defense League (DDL) is a distributed national network of organizers, researchers and disinformation experts disrupting online racialized disinformation infrastructure and campaigns that deliberately target Black, Latinx, Asian American/Pacific Islander and other communities of color. DDL was created by and for these communities.

[17] *See* Free Press Action and Lawyer's Committee for Civil Rights Under Law, "The Online Civil Rights and Privacy Act of 2019" (Mar. 14, 2019), *https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf.*

ited from collecting more information than they need from us and from surreptitiously tracking us across the web. For example, the information we hand over for one reason—like providing a phone number for security purposes—shouldn't be shared or sold to third-party companies.

2. Congress should establish individuals' rights to control our own data. Everyone should have rights to easily access, correct, delete or download their personal information and take it with them when they leave an online service. Making data portable by law would let people free themselves from a corporate walled garden and easily use other services. These rights should apply equally to users across languages.

3. Congress should enhance data transparency. We deserve to know what kinds of information companies and data brokers are collecting about us, and there need to be strict safeguards on what is off limits. Data brokers gather incredibly private details like individuals' sex, age, gender, geolocation, and health information; they can also collect internet-search histories that reveal even more sensitive information like a visit to a mental-health facility or house of worship. Companies need to disclose not just what information they collect, but where they get the information; who shares data with them, and with whom they share data; how they analyze data to profile us; how else they use our information; how they make decisions about what content, goods or services to offer us; and how they secure our data.

Congress should close loopholes in existing privacy law by banning law enforcement from purchasing this information from data brokers without a warrant,[18] and companies should conduct routine audits for bias, including opportunities for independent analysis of algorithmic bias, as well as privacy assessments to determine the risks of their data collection. And companies should be required to convey all of this information in two different ways: in an easy-to-understand format proactively notifying users, and in a detailed format for regulators, advocates and researchers for regular review.

4. Congress should prevent discrimination by algorithms. Everything we do online generates data, and every bit of that data can be tracked and used—no matter how innocuous it may appear in isolation—to create dangerous and invasive online profiles. Data feeds powerful algorithms to deliver personalized ads, recommendations and other services. There are some beneficial and harmless uses of these mechanisms, especially when robust transparency and user control are present. But Congress should ban algorithms that profile users and target content in ways that constitute unlawful discrimination in employment, housing, lending, and e-commerce on the basis of age, race, sex and other protected categories. Congress and relevant Federal agencies should investigate voting and other civil rights violations that flow from abusive data practices too.

5. Congress should increase platform transparency about known harmful impacts of their business models. Reporting over the past several years has demonstrated that—just as the tobacco companies knew that their products were killing people long before the public was made aware—social-media companies knew how their business models were harming people and communities long before the details came to light. Companies should be required to provide access to researchers and to immediately disclose the harm when they learn that a platform's algorithms are being used to discriminate against or otherwise harm people; and the companies should actively and in an ongoing manner mitigate those harms and be held accountable for any persisting harms.

6. Congress should protect whistleblowers and external researchers. We must protect whistleblowers who come forward to expose unethical, immoral, illegal and discriminatory behaviors, algorithms and practices inside of tech companies. Protecting whistleblowers from retaliation, labor law violations, baseless lawsuits, and targeted harassment is critical. We must also set out explicit protections for external researcher access to platform data to guard against what is now a documented pattern of targeted efforts by platforms to deny external researchers the opportunity to investigate platform practices.[19]

---

[18] Passing *The Fourth Amendment Is Not for Sale Act* would be an excellent start on preventing platforms and data brokers from selling people's personal information to law enforcement and intelligence agencies without a warrant or any other court oversight. This bipartisan bill led by Sens. Wyden and Paul was co-sponsored by eighteen Senators at introduction in April, including members of this subcommittee Sens. Lee, Markey, Baldwin, Schatz, Tester, Blumenthal, and Commerce Committee Chairwoman Cantwell.

[19] Platform efforts to cut external researcher access to their data have been well-documented. Documentation includes recent testimony by NYU's Cybersecurity for Democracy initiative before the Subcommittee on Investigations and Oversight, U.S. House Science, Space, and Technology Committee. *See* "Testimony of Laura Edelson, NYU Cybersecurity for Democracy," *Hearing on "The Disinformation Black Box: Researching Social Media Data,"* Sept. 28, 2021. ("Unfor-

7. Congress should expand Federal Trade Commission oversight. The FTC should have the power and resources to conduct rulemakings and effectively enforce against and prevent data abuses and other unfair or deceptive practices. Congress cannot anticipate and legislate against all future uses and abuses of data that companies may engage in, so lawmakers should enable the FTC to oversee and respond to future violations. For instance, users shouldn't have to waive our privacy, quality of service, or other rights by surrendering unnecessary data just to access a given service when there's no need for that extraneous data to deliver the promised service.

8. Congress should encourage collaboration across agencies that hold specialized expertise. Federal agencies such as the Consumer Financial Protection Bureau, Department of Education, Department of Labor, Department of Justice and Department of Veterans Affairs, among others, should study how personal information is used in their fields, identify disparities and risks for discrimination, and issue public reports to Congress on a regular basis with special focus on the discriminatory effects on communities of color and non-English speaking groups.

9. Congress should set a floor for consumer protection, not a ceiling. A Federal law must refrain from pre-empting the work that states are doing to build their own consumer-protection or privacy regimes. Many state consumer-protection laws are used to protect marginalized communities. A Federal data-privacy law that broadly preempts state laws and weakens these kinds of protections would jeopardize civil rights.

Fortunately, two solid legislative vehicles that address many of these core concepts have already been introduced. Free Press Action endorses S. 1896, Senator Markey's Algorithmic Justice and Online Transparency Act. We're particularly interested in this approach because it:

- Defines as places of public accommodation "any commercial entity that offers goods or services through the Internet to the general public," then prohibits algorithms that discriminate based on race, age, gender, disability status and other protected characteristics.
- Establishes safety and effectiveness standards for algorithms.
- Mandates that platforms provide simple explanations of algorithmic processes and the data they collect to power them.
- Requires that platforms submit detailed records about their algorithmic processes for review by the FTC to ensure compliance with key privacy practices.
- Compels platforms to publish transparency reports about their content moderation efforts.
- And creates an inter-agency task force to investigate algorithmic discrimination across sectors.

Free Press Action also endorses S. 3195, the Consumer Online Privacy Rights Act, introduced by Senator Cantwell and co-sponsored by Senators Schatz, Klobuchar and Markey. We're supportive of this approach because it:

- Penalizes platforms that abuse people's personal data.
- Restricts Internet companies and data brokers from processing or transferring data based on an individual's or group's "actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability" in ways that violate people's civil rights and access to economic opportunities.
- Allows people to see the personal information that companies have collected on them.
- Establishes a Federal private right of action.
- And sets a floor, not a ceiling, for consumer protection.

Reforms to Section 230, If Any, Should Be Narrow and Targeted

While Senators on both sides of the aisle have proposed changes to Section 230 as a way to reform platforms' harms both real and perceived, Free Press Action believes that any changes to this law should be narrow and targeted, ideally focused

---

tunately, researchers have been severely hampered not just by lack of such data, but also outright hostility from platforms toward our research. Indeed, this summer, Facebook cut off my team's access to their data. We used that very data to support *the finding* in our recent study that posts from misinformation sources on Facebook got six times more engagement than factual news during the 2020 elections, to identify multiple security and privacy vulnerabilities that we have reported to Facebook, and to audit Facebook's own, public-facing Ad Library for political ads."), *https://medium.com/cybersecurity-for-democracy/testimony-of-laura-edelson-nyu-cybersecurity-for-democracy-e0b7e046eb8.*

on clarifying the portions of the statute that courts have interpreted too broadly to preclude consideration of platform liability even for their own bad conduct.

The Senate bill that feels closest to hitting the mark in our view is S. 797, Senators Schatz and Thune's PACT Act. The transparency provisions in that bill are especially strong. Important too is the bill's language suggesting that platforms could be liable for the harms that their continued distribution of harmful material causes once they have actual knowledge of those harms, even if we preserve as we should these online intermediaries' initial protection against being treated as publishers for making user-generated content available to the public in the first instance.

As Free Press Action testified in a hearing before the U.S. House of Representatives last week, lawmakers should account for six precepts in any legislative discussions about Section 230:

1. Any Section 230 reforms should strike a balance by preserving low barriers to the distribution of benign and beneficial content, yet allowing platforms to be held accountable for their own bad acts, such as knowing distribution of content adjudicated to be unlawful or otherwise actionable, as well as other conduct, content, or defective design and distribution choices of the platform's own making.
2. Congress should reject any suggestion of a full repeal or effective evisceration of Section 230. A repeal would raise barriers to speech and chill expression by promoting excessive takedowns, possibly shuttering entire sites and services, and disproportionately shutting out people of color and other already-marginalized speakers.
3. Section 230 reforms should apply across the board, not just to "big tech" companies, because much harmful and abusive activity happens on smaller platforms too.
4. The best path for Section 230 reform, in our view, would be to clarify that the plain text of Section 230 does not immunize "interactive computer services" for their own actions beyond liability for "publishing" information others provide, or removing or restricting access to such information that the platform considers objectionable. Platforms' use of algorithms to distribute content when they have knowledge of its harms, or their monetization of engagement with that content, would be factors in determining ultimate knowledge and liability but would not automatically turn off 230s protections.
5. Even if Congress significantly altered Section 230, much of the speech the members are (legitimately) concerned about would still be protected by the First Amendment and otherwise unactionable on the basis of existing tort law.
6. That means Section 230 reform is not the only or even the most effective way to stem the tide of harm that online platforms are facilitating, and the types of privacy law enhancements and enforcement of existing laws described above, and efforts to rebuild our media system described below, are essential components for holding big tech accountable and combatting the harms that platforms pose to society.[20]

Building The Media System We Need To Protect Democracy In A 21st Century Society

Privacy and civil rights legislation is a critical part of mitigating the harms caused and perpetuated by social media platforms' failures. But we also must invest in alternatives to the current media system that create healthy pathways for online users to access information. Local news can be a powerful antidote to digital harms such as disinformation, further reinforcing the need to build up local, noncommercial media to correct course on these systemic and compounding crises. Research spanning the last decade underscores that local journalism is essential, a public good in fact, for a thriving democracy.[21] And as the presence of local journalism

---

[20] *See* Matthew F. Wood, Written Testimony for the Record, "Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity" (Dec. 1, 2021), *https://www.freepress.net/sites/default/files/2021-12/matthew_wood_written_testimony_holding_big_tech_accountable.pdf.*

[21] *See, e.g.,* PEN America, "Losing the News: The Decimation of Local Journalism and the Search for Solutions," (Nov. 20, 2019) ("According to one analysis, the act of reading a newspaper alone can effectively encourage 13 percent of non-voters to vote."); *see also* Meghan E. Rubado and Jay T. Jennings, "Political Consequences of the Endangered Local Watchdog: Newspaper Decline and Mayoral Elections in the United States," 56 *Urban Affairs Review* 1327 (2019), doi.org/10.1177/1078087419838058; Danny Hayes and Jennifer L. Lawless, "As Local News Goes, So Goes Citizen Engagement: Media, Knowledge, and Participation in U.S. House Elections," 77 *The Journal of Politics* 447 (2015), dx.doi.org/10.1086/679749.

withers in communities, research has shown an increase in corporate malfeasance and a decrease in civic engagement and voting. Meanwhile, Americans are desperate for local media. In the COVID–19 era, people in the U.S. have turned to local news and local TV more than ever. Twenty-three percent of Americans prefer local media over national,[22] and most American adults trust local media more than national outlets.[23]

Senator Cantwell's 2020 report, *Local Journalism: America's Most Trusted News Sources Threatened,* found that "local journalism is essential for healthy communities, competitive marketplaces, and a thriving democracy." I wholeheartedly concur. Yet, we find ourselves in a local journalism crisis. For instance, in the past fifteen years the newspaper industry has lost 55 percent of its reporting jobs, leaving us with a "reporting gap."[24]

Yet even in its heyday the corporate media structure never sufficiently met the information needs of all people in the United States. The industry has a long and sordid history of racism and exclusion. Indeed in 1969 the DOJ's Community Relations Service identified that "[f]ew American institutions have so completely excluded minority group members from influence and control as have the news media. This failure is reflected by general insensitivity and indifference and is verified by ownership, management, and employment statistics."[25] As Free Press' Media 2070 project has documented, the "white dominant press has used the power of racist narratives to subjugate, punish and control Black bodies and perpetuate white supremacy—both intentionally and unintentionally. Controlling narrative is about maintaining power. And that power has been wielded against Black and other Indigenous and colonized people to launch disinformation media campaigns from colonial times to the present."[26] Today many of these problems persist. This past summer, Reps. Jamaal Bowman, Yvette Clarke, Brenda Lawrence, and twenty-two other members of the House of Representatives wrote in a letter to FCC Chairwoman Jessica Rosenworcel that

> Today, people of color own and control just 6 percent of our Nation's full-power TV stations, 7 percent of commercial FM radio stations and 12 percent of commercial AM radio stations despite making up more than 40 percent of the U.S. population. As of 2017, Black Americans owned or controlled less than 1 percent of television stations. Although many journalists and artists of color have used their talent to ensure critical stories about their communities are being told, our Nation's big media companies nevertheless continue to stereotypically depict people of color as being a threat or a burden to society. Historic Federal policies are a primary reason why structural inequities exist in our Nation's media and telecommunication systems today. FCC policies, license decisions and inaction have had the result of effectively excluding people of color from media ownership opportunities. Our nation's first radio and TV licenses were awarded by the Federal Radio Commission and then its successor, the FCC, during an era of Jim Crow segregation. The previous administration's efforts to consolidate the media marketplace limited ownership opportunities for people of color and women.[27]

In sum, there are multifaceted causes for this reporting gap, and traditional media and now social media alike have been used to exclude, marginalize, and harm people of color in particular. But while these problems are not new to platforms nor wholly traceable to them, Free Press Action has proposed, and the Disinformation Defense League has endorsed, that Congress pass legislation to tax digital advertising and direct those monies to support high-quality noncommercial and local journalism. To fund local journalism, Congress could levy a small tax on the online-advertising revenues of large online platforms. For example, a 2 percent tax would

---

[22] Pew Research Center, "Local news is playing an important role for Americans during COVID–19 outbreak" (July 2, 2020), *https://www.pewresearch.org/fact-tank/2020/07/02/local-news-is-playing-an-important-role-for-americans-during-covid-19-outbreak/*.

[23] Pew Research Center, "For Local News, Americans Embrace Digital but Still Want Strong Community Connection" (March 26, 2019), *https://www.pewresearch.org/journalism/2019/03/26/for-local-news-americans-embrace-digital-but-still-want-strong-community-connection/*.

[24] *See* S. Derek Turner, "How Big is the Reporting Gap?," Free Press (June 2020), *https://www.freepress.net/sites/default/files/2020-06/free_press_reporting_gap_analysis_report.pdf*.

[25] *1969 Annual Report of the Community Relations Service,* Department of Justice, U.S. Government Printing Office, at 22 (1969).

[26] *See, e.g.,* Torres, *et al., supra* n.1, at 24.

[27] Letter from Rep. Jamaal Bowman *et al.* to Acting FCC Chair Jessica Rosenworcel (June 28, 2021), *https://bowman.house.gov/_cache/files/6/5/65b9a1a7-3553-4d5b-9d69-b8a92c0e628d/3290E56EAC603E81B4CFE58A5DAEBEF1.0628-congressional-letter-on-fcc-racial-equity-assessment-final.pdf*.

yield more than $2 billion annually for a national endowment to support local news and information, including journalism by and serving people of color, non-English speakers, and other minority groups.[28]

Thank you and I look forward to your questions.

Senator LUJÁN. Thank you, Ms. González. Next, we will hear from Dr. Poulos, the Executive Director of the American Mind, Claremont Institute.

STATEMENT OF JAMES POULOS, EXECUTIVE EDITOR OF THE AMERICAN MIND, CLAREMONT INSTITUTE

Mr. POULOS. Good morning, Chairman Luján and Ranking Member Thune, members of the Subcommittee. I am James Poulos, Executive Editor of the American Mind at the Claremont Institute, where my research focuses on preserving our shared way of life and form of Government in a digital age. It is an honor to speak today about how Congress can act. I will start by putting algorithmic harm in broader context and then make a few recommendations. The memes that algorithmic harm results from greedy CEOs hacking our minds fails to grasp the true nature of the digital crisis roiling America.

As with digital programs and data centers, today the main purpose of algorithms is not to make money or influence thoughts, but to control people in a direct and alien way hostile to our core beliefs and principles. The digital medium is unlike prior media such as print or television. Those technologies also reshaped minds and built fortunes. But Americans always felt at home with them. There was a comfort level, a compatibility with our life ways and a regime that is absent regarding digital tech, which most Americans feel unable to understand, much less to master.

As I show in my new book Human Forever, this morose incompetence is the product of a public, private partnership between unelected and unaccountable leaders across America's major institutions and our security and intelligence state.

Almost all digital tech ordinary Americans use is the product of innovations from military and spy agency research, spun off into consumer entertainment and corporate craft by tech companies key to our national strategic infrastructure. These leaders whom citizens and even elected officials are functionally unable to remove from power, have moved so much of our political and social life into their technological ecosystem that they now make and enforce fundamental decisions about what we can and must think, say, and do.

This lockstep reconfiguration of American life outside the reach of the democratic process has plunged us into a nascent social credit system. Social media's algorithmic harm is real, but social media is true to form a screen that obscures the depths below, where leaders like Eric Schmidt and Jeff Bezos are working to refound America as a control system built on innumerable swarms of programs and devices in a vast network of data centers. Through machine learning and AI, digitized governance automates the behavior of those swarms and through them, the behavior of you and me.

[28] Free Press's *Beyond Fixing Facebook paper* offers ideas on how Congress could institute an online-advertising tax to support local journalism.

The new system's logic is driven by seeing digital tech as better and stronger than humanity. As one ex-Google executive puts it, we humans "suck" in comparison to the new "god" our engineers are building. This view of our given humanity is a pathetic curse and not a precious gift is spreading because our leaders betrayed the expectations they created. Many believes when they told us the tech would bring global peace and harmony. The TV age ideal that whoever dreamed biggest, and best would rightly rule the world led to shock and panic when populists used digital tech to fight technocratic globalism.

Today, our techno ethical elite is religiously convinced they can invent a coding language so deterministic that they can take true control of the digital swarms, eliminating the need for politics as it has been known in the West since Aristotle. They expect, will soon merge fully, with our technology becoming as gods. To make us yearn to upload our consciousness to the cloud, these new cyborgs theocrats have begun by uploading our conscience. Many Americans now think the culture war demands a digital regime, reward the pure and obedient and crush the opposition, online and off.

This is why the COVID crisis has morphed so quickly into a pitched battle over who gets to act as judge, jury, and executioner when it comes to defining, preventing, and punishing harm. Now, representatives face a fateful choice, restore citizen controls of technology or surrender to the cyborg theocracy. Americans need Congress to intervene against the emergent social credit system.

Trust in digital competence on the Hill can be built with bipartisan steps protecting children from the worst online harms. And lawmakers can protect free association and expression by favoring policies like algorithmic choice over calls to legislatively overturn *Force v. Facebook,* which would entail cosmic Federal choices about the metaphysics of harm that amount to an establishment of a religion.

But unless ordinary Americans regain a hands on mastery of our most powerful digital tools, we will become compliant post-humans or ungovernable psychotics, sacrificing what is left of our civilization and our Nation to vengeful new gods. Congress can best blunt digital harm by passing what I and others compare to a Second Amendment for computing.

As I argued recently in the *New York Times,* legislation should enshrine Americans rights to buy and use high powered GPUs and to mine and hold bitcoin. This tech puts computation into human service, building apps and institutions where users create and exchange valuable, memorable works of culture.

To model this approach, I published my book, *Human, Forever,* onto the blockchain at the Bitcoin based platform Canonic.XYZ. Americans have the ability right now to restore their practical use of technology to defend and protect all they hold sacred from the social credit borg. By recognizing the free exercise of that ability as a fundamental right of the digital age, lawmakers can save America and Congress from technological oblivion. Thank you. I will be happy to take questions.

[The prepared statement of Mr. Poulos follows:]

PREPARED STATEMENT OF JAMES POULOS, EXECUTIVE EDITOR OF THE AMERICAN MIND, CLAREMONT INSTITUTE

Good morning Chairman Luján, Ranking Member Thune, Members of the Subcommittee. I'm grateful to join you. My name is James Poulos. I'm the Executive Editor of the American Mind at the Claremont Institute, where my research responsibilities focus on preserving our shared way of life and form of government in a digital age.

It's an honor to speak today about how Congress can act. I'll start my remarks by putting algorithmic harm in a broader context. Then I'll make a few recommendations.

The meme that algorithmic harm results from greedy CEOs hacking our minds fails to grasp the true nature of the digital crisis roiling America. The main purpose of algorithms, like digital programs and datacenters more broadly, is not to make money or influence thoughts, but to *control* people—in a direct and alien way hostile to our core beliefs and principles.[1]

The digital medium is unlike prior communications technologies such as the printing press or television. Those media also reshaped minds and built fortunes. But Americans always felt at home with them. There was a comfort level and compatibility with our lifeways and our regime that's absent regarding digital technology, which most Americans feel hopelessly unable to understand, much less master.

As I show in my new book *Human, Forever,* this morose incompetence is the product of a public-private partnership between unelected and unaccountable leaders across America's major institutions and our security and intelligence state. As economists such as David P. Goldman and Maria Mazzucato have reminded us, almost all the digital technology ordinary Americans use is the product of innovations attained through military and spy agency research and spun off into consumer entertainment and corporate cruft by the tech companies crucial to our national strategic infrastructure.

However well-intentioned, these leaders, whom citizens and even elected officials are functionally unable to remove from power, have moved so much of our political and social life into their technological ecosystem that they now make and enforce fundamental decisions about what we can and must think, say, and do.

This lockstep reconfiguration of American life outside the reach of the democratic process has plunged us into a nascent social credit system. Social media's algorithmic harm is real, but social media is, true to form, a *screen* that obscures the depths below—where leaders like Eric Schmidt are working to re-found America as a control system built on innumerable swarms of programs and devices in a network of vast datacenters. Through machine learning and artificial intelligence, digitized governance aims to automate the behavior of those swarms and, through them, the behavior of us human beings.[2]

The new system is driven by the logic of seeing technology as better and stronger than humanity. As Mo Gawdat, an ex-Google executive on publicity tour, recently told *The Times,* we humans "suck" in comparison to the new "god" our tech engineers are building. This view of our given humanity as a pathetic curse, not a pre-

---

[1] The objection could be raised that algorithms, in a certain strengthening sense, actually mainly exist so that digital devices and entities can communicate with one another. One reason digital technology is so alien to us is its indifference to our feelings and our existence alike, and our shared sense that digital tech which operated even in part based on its awareness of our presence and attitudes would be dangerous or difficult to establish trust with. Perceptive digital entities which did communicate openly with us might still "talk behind our backs" amongst themselves. In June 2019 testimony before the U.S. Senate Commerce Committee's Subcommittee on Communications, Technology, Information, and the Internet," Stephen Wolfram observed that "if we want to seriously use the power of computation—and AI—then inevitably there won't be a 'human-explainable' story about what's happening inside . . . if you can't check what's happening inside the AI, what about putting constraints on what the AI does? Well, to do that, you have to say what you want. What rule for balance between opposing kinds of views do you want? How much do you allow people to be unsettled by what they see? And so on." As Norbert Wiener helps us understand in *The Human Use of Human Beings: Cybernetics and Society,* even if algorithms and content-selecting AIs—or whole swarms of digital entities—communicate almost exclusively with one another in an ignorance of us they cannot describe, our commands are still the inputs, and however imperfectly they are executed, the outputs must inevitably have human significance intended to impact (*e.g.,* use) human beings.

[2] Innovation is palpably shifting, even within social media, away from writing algorithms and toward conducting swarms. Analyzing a leaked document from TikTok revealing the app's inner workings, UC-San Diego computer science professor Julian McAuley recently told Ben Smith of The New York Times that TikTok's advantage marries machine learning to "fantastic volumes of data, highly engaged users, and a setting where users are amenable to consuming algorithmically recommended content (think how few other settings have all of these characteristics!). Not some algorithmic magic."

cious gift, is spreading because our leaders betrayed the expectations they created. Many believed what they told us about how tech would bring global peace and harmony. The TV-age belief that whoever dreamed biggest and best would rule the world and deserved to led to shock and panic when populists used digital tech to fight technocratic globalism.

Today, our technoethical elite is religiously convinced they can discover a mathematical coding language so deterministic that they can take true control of the digital swarms, eliminating the need for politics as it has been known in the West since Aristotle.[3] Eventually, they believe, we will fully merge with our technology and become "as gods."

Rather than trying to upload our consciousness to the cloud, these new cyborg theocrats have begun by uploading our conscience. Many Americans now think the culture war must be fought and won through a digital regime that rewards the ethically pure and obedient and crushes the opposition online and off. This is why the covid crisis has morphed so quickly into a pitched battle over who gets to act as judge, jury, and executioner when it comes to defining, preventing, and punishing harm.

Now, the people's elected representatives face a fateful choice: restore citizen controls of technology or surrender to the cyborg theocracy. Americans need Congress to intervene against the emergent social credit system. Trust in digital competence on the Hill can be built with bipartisan steps protecting children from the worst online harms.[4] And lawmakers can protect Americans' free association and expression by favoring policies like algorithmic choice over calls to legislatively overturn *Force v. Facebook,* which would entail cosmic Federal choices about the metaphysics of harm that amount to the establishment of a religion.[5]

But unless ordinary Americans regain a hands-on mastery of our most powerful digital tools, we will become compliant posthumans or ungovernable psychotics, sacrificing what is left of our civilization and nation to vengeful new gods. Congress can save our humanity, our country, and our form of government from digital harm by passing what I and others compare to a Second Amendment for Compute. Legislation should enshrine Americans' rights to buy and use high-powered GPUS and to mine, hold, and use Bitcoin. This tech puts computation into human service build-

---

[3] The politics of determinacy extend well beyond the elite. Debates rage over whether digital technology is somehow "neutral" or can be made so by policy. It cannot be, in two senses. Pure neutrality cannot be achieved by or through algorithms, which, as instructions to produce a certain result, are always inherently "biased" by default. "Correcting" an algorithm means giving it a new and different bias. On the level of the medium, interoperability is the form of digital technology that shapes all digital entities. While the bias of digital tech in this sense is toward interoperability, the human bias is toward incommensurability. We may enjoy temporarily joining the crowd, the mass, or even the mob, the feeling passes and we return to abide in the unique and particular personhood of our self. Digital entities do not share this dynamic. Unlike us, they are biased toward the collective identity of the swarm, an identity incompatible with our human one. The quest for the Holy Grail of perfect determinacy depends on the faith that mathematics itself is neutral and unbiased in the sense of ultimately being perfectly legible and comprehensible—without secrets—to rational human minds. Quantum physics and millennia of Western theology agree that the truth is more complicated. Devotion to mathematics as the perfect language of true explanation is necessarily "biased against" mysteries, against the need for or permanence of mystery, and against the idea that the primal condition of reality involves phenomena inaccessible to human logic.

[4] Legislators should be prepared to discover that algorithms and human users often share joint responsibility for what emerges over time as accumulated harm. Writing about Instagram's algorithms in *The Atlantic,* Jonathan Haidt observes that "the toxicity comes from the very nature of a platform that girls use to post photographs of themselves and await the public judgments of others," specifically, we should recognize, other girls posting photographs. Social media is a hotbed of mimesis, the reflexive behavior of imitating one's real and imagined rivals that social theorists from Rousseau to Girard have recognized as fundamental to our human identity. The strongest and most prudent legislative intervention against the experience of having suffered harm from engaging in habits reinforced by algorithm would be to legally protect and defend Americans' fruitful use of digital technologies, such as Bitcoin, which do not inflict algorithmic or mimetic harm in the manner of social media platforms because they are not social media platforms.

[5] The House Energy and Commerce Committee, for instance, recently discussed the "Justice Against Malicious Algorithms Act," a bill that would amend Section 230 by allowing users to sue platform companies for inflicting "severe emotional injury," but which did not define emotional injury. The "Protecting Americans from Dangerous Algorithms" bill introduced last session would, as Cato Institute policy analyst Will Duffield noted last year at Techdirt, "have grave consequences for legitimate speech and organization . . . an omnipresent corrective authority"—spiritual and temporal together, like Hobbes' Leviathan—"would foreclose the sense of privileged access necessary to the development of a self."

ing apps and institutions where users create and exchange valuable, memorable works of culture.[6]

To model this approach I published my book, *Human, Forever,* onto the blockchain, at the Bitcoin-based platform Canonic.xyz. Americans have the ability right now to restore their practical use of technology to defend and protect all they hold sacred from the maw of the social credit borg.[7] By recognizing the free exercise of that ability as a fundamental right of the digital age, lawmakers can save Congress—and America—from technological oblivion.

Senator LUJÁN. Thank you very much. Dr. Eckles, our Associate Professor of Marketing at MIT Sloan School of Management. Dr. Eckles.

STATEMENT OF DR. DEAN ECKLES, ASSOCIATE PROFESSOR OF MARKETING, MIT SLOAN SCHOOL OF MANAGEMENT

Mr. ECKLES. Chairman Luján, and Ranking Member Thune, and members of the Subcommittee, thank you for asking me to appear here today to discuss these important topics. I typically don't work on public policy directly, but I have been studying social media for over a decade, currently at MIT. I also previously worked in industry, including as a scientist at Facebook. I have a wide view of current practice and fundamental challenges in the context of social media.

Social media have dramatically lowered the costs for anyone to share information and media with many people. It is so easy to propagate content that people often share things that on further consideration they would realize are misinformation. And various actors from legitimate marketers and political campaigns to spammers, scammers, and foreign disinformation efforts seek to maximize their reach and influence on these platforms. What role do algorithms have to play here? Yes, the algorithms show us content we are predicted to click on, to watch, and to propagate. But importantly, not just this.

As sophisticated platforms, algorithmic ranking involves using many signals. This includes negative signals, signals that reveal we will regret engaging with the content and attitudinal signals like predictions of whether we would say the content is informative, important, or fun, if we were asked. These can serve as an

[6] Bitcoin is deeply resonant with American civilization. In no other country, especially leading country, has interest and activity in Bitcoin been so immediate, sustained, and powerful. Some countries, including China, have cracked down on Bitcoin or banned it outright. Given that digital technology's world dominance makes us reconsider venerable theological matters by causing us to question our identity and purpose, it seems important that the Bitcoin blockchain relies for the legitimacy of its architecture and operations on the deeply Protestant concept of Proof of Work. To activate the consensus that allows new blocks of information to be added on chain, Bitcoin miners must compete to solve a math problem. The achievement satisfying Proof of Work is not to have "cracked the code" but to have evinced the input of the most computational labor. Allegations that Bitcoin is therefore energy-intensive enough to represent an unjust *harm* to the natural environment fail on several fronts, including the relative energy consumed over a given period by China or the petrodollar, but especially on the ultimately theological basis of the idea of fair play through competitive labor that is a cornerstone of American civilization. Of course, many of those who insist we must leave theology behind in assessing the value of political or economic measures still retain, due to their own theological inheritance, an idea that fair play through the labor of competitive *reasoning* is a thoroughly secular standard of justice. Whether inflected in this more secular or the more theological key, the inner logic and structure of Bitcoin is at home in America, where the common sense is still that the unceasing labor of building and maintaining culture is the price of flourishing in freedom.

[7] Notably, the hardware associated with mining and building on Bitcoin gives users the ability to freely generate algorithmic markets, which guide people within a technological ecosystem based on voluntary agency and not, as in a social credit system, mandatory compliance.

important way of balancing against solely short run engagement signals.

Quantifying the impacts of algorithmic ranking is quite difficult. The platforms themselves often struggle, despite their data, their randomized trials, and their expertise, to quantify some of the effects of the decisions they must make. This isn't just because of technical complexity, but due to people's complex and often strategic responses to changes in algorithms.

First, everyday users adjust their behavior in response to algorithms. Say you are connected on social media to a relative who post a lot of political content that you disagree with. Due to algorithmic ranking, you don't see a lot of these posts. The platform accurately predicts you will not engage, and you wouldn't say they help you be informed. But you do see most of that person's posts about fishing.

Now, this might seem like a clear case of a filter bubble, whereby the algorithm is causing you to be exposed to less cross-cutting content than you would under a simple chronological ranking. But consider this, under chronological ranking, you might initially see so many undesirable political posts from this person that you choose to unfollow them.

So this could result in then seeing less crosscutting content and having fewer cross-partisan ties than you would under the algorithmic ranking. So was it really creating a filter bubble? What was really being amplified here? Second, more professional and strategic actors, marketers, politicians, publishers, et cetera, they have tuned what they post and when they post it to the status quo algorithm. If things change dramatically, they will adjust dramatically. Accounting for this is key to assessing what is truly being amplified by an algorithm.

Overall, we lack clear evidence about broader aggregate harms or benefits of algorithmic ranking. Nonetheless, far from there being clear benefits from simple rankings like chronological or overall popularity rankings, it can make some forms of undesirable strategic behavior easier and more successful.

I have seen some of this in my work on cross-platform coordinated campaigns to game Twitter trends during the 2019 Indian elections. So what can policymakers do? Some of what I said suggests that some of the easy pass here won't work. For example, simple definitions of algorithmic amplification can be turned out to be hugely misleading.

One basic thing policymakers can do, though, is to help scientists, journalists, and the public better understand these systems. First, they can protect the ability of external researchers to probe these systems, not unlike what staff here have done by creating accounts on Instagram and TikTok, but more systematically. While some court rulings have been encouraging, there has been substantial legal risk for researchers probing platforms to ask questions of broad interest. This can have chilling effects.

Second, policymakers can provide clear paths for platforms to retain and share data in privacy preserving ways with researchers. There remains a great deal of uncertainty about what methods for anonymization of data satisfy some international privacy regulations like GDPR, likely discouraging sharing data with researchers.

My understanding is that some platforms are not even retaining critical data for their own internal research, including on algorithmic impacts, because of such regulations. This suggests the value of care and clarity in crafting these regulations. I am encouraged by this committee's work in this area, and I look forward to your questions.

[The prepared statement of Mr. Eckles follows:]

PREPARED STATEMENT OF DR. DEAN ECKLES, ASSOCIATE PROFESSOR OF MARKETING, MIT SLOAN SCHOOL OF MANAGEMENT

ALGORITHMIC TRANSPARENCY AND ASSESSING EFFECTS OF ALGORITHMIC RANKING

Contemporary communication technologies have dramatically lowered monetary and practical costs of broadcasting information and media to many people—and of consuming others' broadcasts. They have created new ways for people to share their own thoughts, experiences, and creations, to consume and react to those shared by others, and—quite importantly—to rapidly propagate them. It is so easy to propagate content that people often share information that, on further consideration, they themselves would realize is misinformation.[1] Interactions on social media affect commerce, culture, politics, and public health,[2-6] thereby reasonably attracting scientific, public, and regulatory attention.

What role do algorithms play in all of this? Algorithms are unavoid-able here. Even sorting posts by friends in chronological order* or videos by overall popularity is algorithmic; and often it is unclear there is a single, simple baseline algorithm. What much of the public conversation about algorithms has in mind are particular kinds of more complex, potentially more opaque, algorithms—typically based on statistical machine learning—that are adaptive to, *e.g.,* features of the content and each person's history of consumption. In the context of social media, these algorithms typically first present items that are predicted to be something the consumer will take desirable actions on or would say is important, interesting, or fun.

Are these algorithms better or worse—for individual consumers and for society—than simpler alternatives that would, *e.g.,* present everything from the accounts someone follows in chronological order? Can we straightforwardly specify what a given algorithm "amplifies" in a way suitable for assigning moral or legal responsibility?

Here I briefly summarize some key points.

1. At established platforms, algorithmic ranking and recommendation involve using many signals and are typically not aimed at simply maximizing short-run engagement.
2. Quantifying the impacts of algorithmic ranking is quite difficult, even with access to proprietary data. This is not only because of the complexity of these technical systems, but due to people's complex and often strategic responses to changes in algorithms.
3. We lack clear evidence about broader benefits or harms of algorithmic ranking. Nonetheless, simple rankings and recommendations (*e.g.,* chronological, overall popularity) can make some forms of undesirable strategic behavior easier.
4. Policymakers can protect the ability of external researchers to probe these systems, and they can provide clear paths for platforms to retain and share data in privacy-preserving ways.

The rest of this statement is organized as follows. First, I characterize current practice in algorithmic ranking and recommendation of content in social media. Second, I elaborate on how we can learn—and what we already know—about effects of algorithms in social media. Third, I conclude by stating some policy implications.

Current practice

Before considering assessing their effects or crafting policy, it can be useful to understand the state-of-the-art in algorithmic ranking and recommendation in social media. This involves choosing from a large collection of items (*i.e.,* content, stories, posts, activity) that a user is eligible to see and determining which of those items are displayed in what order—and also how each item is displayed, as there are often

*For simplicity I use "chronological" to refer to a ranking that shows items ordered by recency—perhaps more precisely called reverse chronological.

multiple variations available. I start with a prototypical case, presenting a somewhat simplified solution, and then discuss a few relevant variations.

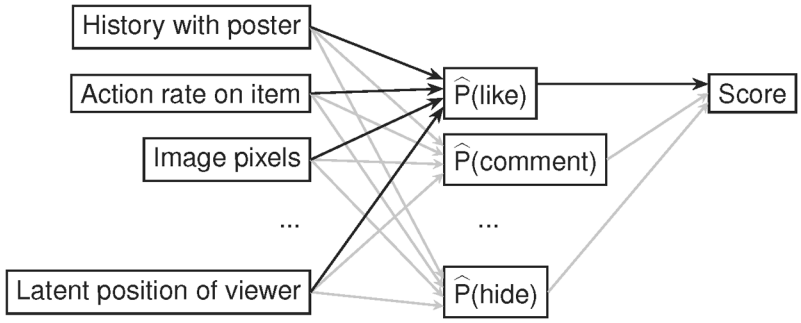
Consider the problem of choosing which of a large set of photos or videos shared by accounts a user follows to display and in what order. This is a version of the problem faced by Instagram and Snapchat in their feeds (that is, setting aside their other channels for now). People do not typically spend enough time using these services to see all—or even the majority—of what is shared by the accounts they follow.[7,8]

These platforms have multiple goals in mind when doing this ranking. They then attempt to quantify these goals in metrics, usually defined at the level of each user. These could include the fraction of days that users log in, the number of photos they post, their time spent using the service, what they would say in response to a survey question asking about the service, the revenue from them viewing or clicking on ads, etc. These may be combined into a single evaluation criterion,[9] or managers may decide to try to maximize one metric while ensuring that they do not have substantial negative effects on others.

It is difficult to directly optimize what items to show to maximize such metrics, since these metrics are defined at the level of users and there are many possible rankings of items.* So typically platforms simplify the problem by defining a small number of constituent scores for each item, defining a combined score that, *e.g.,* sums up these scores, and then ranking items by that combined score (Figure 1).[10,11]

These constituent scores are typically predictions of actions the viewing user might take on or related to the item. For example, there could be predictions of the probability the viewer will "like" the item.† Similar predictions can be made for many other item-level actions, such as commenting on it or viewing it for at least x seconds. Usually "negative" actions, such as unfollowing or unfriending the poster or hiding the item, are similarly predicted and given negative weights in the combined score.* Data scientists and managers try to identify new actions to predict that provide additional relevant signals (*e.g.,* sequences of actions indicative of "regretted" clicks).

Figure 1: Schematic representation of inputs to scores used to rank items in social media feed. Numerous characteristics of the item are used to predict the probability of the viewer taking various actions (e.g., "liking" the item) based on historical data. These predictions together determine a combined score; for example, the combined score might add up these predictions, each with a different weight.



The same approach is often used to predict other, less direct, actions. For example, the platform may produce predictions of whether the viewer will follow or friend someone involved in the item (*e.g.,* someone tagged in the photo). The general approach can also incorporate non-behavioral signals that are only available for a small sample of users, such as data from surveys. For example, if the platform has

* For a single user, there often are more possible rankings of available items than there are atoms in the universe: say there are 100 items available, then there are over 10^{156} possible orderings of those items.

† Ranking engineers at multiple firms can be overheard referring to "p-like".[12]

* That is, the combined score for an item will look something like score = w_{like} x $\hat{P}$(like) + w_{comment} x $\hat{P}$(comment) + . . . + w_{hide} x $\hat{P}$(hide), where the ws are the (positive or negative) weights given to the predictions of different actions. Recent reporting makes clear TikTok's ranking likewise follows this pattern,[12] though it apparently lacks both any negative signals or any signals from attitudinal (*e.g.,* survey) data.

contractors or everyday users rating content in their feeds,† they can predict those ratings; that is, the platform can produce predictions of whether, if asked, the viewer would say this item is important, informative, funny, or makes them feel connected.

How are the weights on these different constituent scores chosen? In some cases these weights may be selected through managerial judgement alone, but often sophisticated A/B tests‡ are used to compare how different choices of weights affect metrics.[10,14,15] For example, the weights might be selected to maximize a metric designed to (ambitiously) measure people's level of "meaningful social interaction", subject to a constraint on revenue. While it is most straightforward to assess effects on metrics for the viewing user, many of the immediate consequences of ranking apply to other people (*e.g.,* by showing this item to this viewer, the poster of that item may receive an additional comment).[16] Platforms often try to incorporate these consequences into their ranking as well.

Recall the constituent scores are the probabilities of various actions; how do platforms predict these actions? They use very large statistical machine learning (or, if one prefers, artificial intelligence) models trained on historical data about which items people were shown, what the characteristics of those items where, and what the viewing user did.* For example, the historical data would generally reveal that if the viewer frequently comments on items involving a particular person (*e.g.,* as the poster of the photo, as someone tagged in the photo), then they are more likely to do so for this new item. More recently, platforms have more thoroughly incorporated techniques from natural language processing and computer vision into these predictive models; the actual contents on the photo are used to predict what actions the viewer would take if shown it.† Furthermore, the history of a user's interactions and connections in the social network is sometimes used to learn some numeric representation of their preferences and dispositions, which can also be used in these predictions; these can be regarded as latent (*i.e.,* unobserved) positions of each user.

Thus, the algorithmic ranking of social media feeds typically depends on numerous inputs. Some of these inputs themselves are the results of prior statistical machine learning (*e.g.,* learned representations of the objects in photos). However, decision-makers within platforms are typically less focused on these inputs, but rather on understanding and effectively making tradeoffs between various metrics—defined not solely at the level of individual items to be ranked, but for individual users or for the entire service. They often make these tradeoffs by differently weighting predictions about how a viewer will act on or evaluate an item.

Further variations and complications

There are some variations on and complications of the above problem and solution.

1. When deciding what item to show in the second position, it can be useful to account for what the first item is; more generally, it can make sense to consider the full ranked set of items so as to reflect, *e.g.,* demand for variety of topics or sources. While it is typically computationally difficult to directly optimize rankings in this way, platforms often implement various heuristics to improve the final ranking. For example, they may have rules that prevent a ranking from being highly repetitive in having several items from the same poster, only videos, etc.*
2. There are sometimes multiple ways to display an item. For example, multiple photos posted by the same person could all be shown smaller and grouped together, or some or all could be displayed at a larger size and shown individ-

---

† Facebook, for example, created a paid "feed quality panel" to meticulously rate items in their feeds, and has combined this with data from users who respond to prompts to rate their feeds.[13] These ratings can be used both to evaluate a prospective ranking algorithm and in the algorithm itself via predictions, as described here.

‡ A/B tests (*i.e.,* randomized experiments, randomized controlled trials) involve randomly assigning users to different variations on a service. Here this would be assigning users to rankings using different weights on the predicted actions. As in medicine and economics, these randomized trials are considered the "gold standard" for evidence and decision-making.

* Usefully, this historical data typically involves users seeing stories in an order other than the status quo because they are in an A/B test or because the scores for items have had a small amount of random noise added to them.

† That Facebook uses such signals can be seen in that ad delivery is immediately imbalanced by gender depending on whether the ad image alone includes stereo-typically male- or female-relevant themes.[17]

* This is sometimes described as the "slate recommendation" problem, including in research from YouTube and others.[18] Facebook managers describe this as part of a "contextual pass" that, among other things, implements poster and content-type diversity rules.[11]

ually. Some or all existing comments on an item could be displayed by default.[16] Thus, similar algorithms are also often used to make these decisions.

3. What comprises the inventory of items to be ranked is not always obvious, and it is often not limited to other accounts broadcasting new content (*e.g.,* posting a photo), but can include other activity (*e.g.,* a friend being tagged in a public photo, a friend commenting on a photo by another friend). Typically, many of these items score poorly or are removed according to rules to avoid repetitiveness (*e.g.,* several items about friends commenting on the same photo), but some may score well.
4. Even in the same platform there are numerous channels for algorithmic ranking and recommendation. Public discourse often has in mind a single feed (*e.g.,* Facebook News Feed, TikTok's series of videos), but these same items might be delivered to users via multiple feeds[†] and via e-mail or mobile push notifications, with these likewise subject to optimization.[19] Established platforms are often ranking and recommending many types of items in many different formats. For example, many platforms suggest accounts to follow or friend based on numerous signals and with the aim of getting new users to make, *e.g.,* engaging and varied connections.[20] Many platforms also have personalized search functionality in many places, including some that might seem mundane or invisible (*e.g.,* autocompletion of friends' names when tagging them in photos).

Algorithmic transparency and impact: Evidence and challenges

There is substantial interest in characterizing "algorithmic amplification"—what content is given greater reach than it would have with some baseline algorithm—and the broader impact of algorithms. The title of this hearing refers to "dangerous algorithms" and posits associated harms. I find it quite plausible that, in particular cases, algorithmic ranking in social media is the proximal cause of specific harms; likewise, in particular cases, algorithmic ranking is the proximal cause of specific benefits and the absence specific harms. But how would we know whether aggregate effects of algorithmic ranking and recommendation in social media are positive or negative? To be clear, I do not think there is a social-scientific consensus here in favor of some simple baseline ranking (*e.g.,* chronological) over the status quo.

Ideally, we would like to have rigorous, quantitative evidence about the effects of algorithmic ranking. While there presently is not a large body of evidence, one hope is that algorithmic transparency and other efforts would enable expanding this evidence. Here I review ways we can learn about algorithmic ranking and recommendation, in the pro-cess summarizing what limited evidence[*] we do have and highlighting some of the challenges in using simplistic comparisons of algorithms.[22]

I see three common ways we can learn about the effects of algorithms: (a) querying the algorithm with different inputs, (b) comparing outputs (*i.e.,* rankings) of different algorithms on the same inputs (*i.e.,* content inventory), and (c) conducting randomized trials assigning users (whether content producers or consumers) to different algorithms.

First, and most minimally, we may be able to *see how the algorithm ranks different items;* we can provide a variety of items (perhaps systematically varying some of their characteristics) and see the output. To some degree, this is commonly done by marketers (whether in commercial, public interest, or political campaigns) probing social media platforms in attempts to optimize their own reach by trying numerous variations on the content and timing of what they post. This is also an approach that has been used successfully to identify, *e.g.,* disparate error rates in commercial computer vision systems.[23†] One challenge here is that one needs relevant samples of items—and perhaps the ability to generate systematic variations on them—to run through the algorithm. In the context of computer vision, there are available corpuses of images and creating a new sample of images is possible since they can be provided to the algorithm in standard formats. However, in the context of social media, external researchers may have little access to a distribution of items and

---

[†] For some time starting in 2011, Facebook had both its News Feed and a second, chronological feed (Ticker) that updated in real-time; both were visible simultaneously when using Facebook on a computer.

[*] Further afield, there are detailed studies of predictive systems making biased and harmful decisions in, *e.g.,* health care,[21] a setting where both quite different regulatory considerations apply and some of the challenges described above as less severe.

[†] A variation on this approach would also use access to the algorithms' code itself. This might seem like a substantial advantage, but often the complete algorithm is complex enough—having potentially billions of parameters—that this may neither facilitate human understanding (even by the engineers building them) or readily enable external researchers or auditors to run a variation on the algorithm.

many different signals are used in the ranking (*i.e.,* the left column of Figure 1), many of which have only some proprietary format.

Second, we may be able to *compare how different algorithms rank the same inventory* for the same user. Academic researchers have, for example, set up Twitter accounts that emulated some archetypal real users and compared how news content is displayed in the "Home" (algorithmically ranked) versus "Latest Tweets" (approximately chronological) view; one study with eight artificial accounts found that the algorithmic ranking resulted in less exposure to external links as a whole, including links to news.[24*]

While these kinds of comparisons are an important tool, they typically do not tell us about "algorithmic amplification" writ large. These comparisons tell us about how items would be ranked if—for a moment and for one account only—the algorithm was changed; they do not typically tell us about what would happen if the algorithm were changed for a longer period of time and for many people or everyone.

Consider an example. Say you are connected on social media (*e.g.,* are friends on Facebook, follow them on Twitter) to a relative with political views very different than your own and who posts a lot of political content. Due to algorithmic ranking and recommendation you might not see a lot of those posts, as the platform accurately predicts you will not engage with them nor would you say, if asked, that they helped you be informed or feel connected; rather you see a few of those posts, but you do see most of their posts about family and fishing. This might seem like a clear case of a "filter bubble" whereby the algorithm is causing you to be exposed to less cross-cutting content than you would under a simple chronological ranking.[†] However, the truth can be a bit more complex than that. Under chronological ranking you might initially see so many undesirable political posts from this person that you choose to unfollow or unfriend them. This could result in eventually seeing less cross-cutting content than you would under the algorithmic ranking.[‡]

More generally we can note that some of the effects of algorithmic ranking and recommendation of content occur by causing people to change their behavior including the formation, maintenance, and dissolution of their social network ties.[32] It can also affect the timing and duration of use of social media. Both of these then determine the longer-run consequences for what items they see. This process is illustrated in Figure 2.

Third, platforms can conduct *randomized trials comparing different ranking algorithms.* This is a key tool by which they optimize these algorithms with respect to their goals, and it is also used to gain further understanding of these complex systems.[33-35]

Randomized trials show that ranking choices can indeed matter. In the lead up to the 2012 U.S. presidential election, a routine ranking experiment at Facebook randomly assigned over 1 million Americans to an algorithm that boosted the ranking of "hard news" from established news outlets; a preliminary analysis concluded that this increased political knowledge, altered policy preferences, and increased voter turnout compared with the status quo ranking.[36] Note, however, that the baseline here is not chronological ranking; in fact, the novel algorithm only moderately differed from the status quo, as it only affected a small fraction of items.[37§] Thus, while this study provides evidence that, in a broad sense, *ranking matters,* it says less about how something approximately like the social media status quo compares with, *e.g.,* a chronological ranking.

Figure 2: A simplified feedback loop in algorithmic ranking in social media. The content available to a user (i.e., their inventory*) depends on what accounts they follow. Even in the case of chronological ranking, what they see depends on their behavior (via, e.g., timing of use). Users change their behavior when the content they are shown changes (e.g., unfollowing other accounts, spending more or less time on platform).*

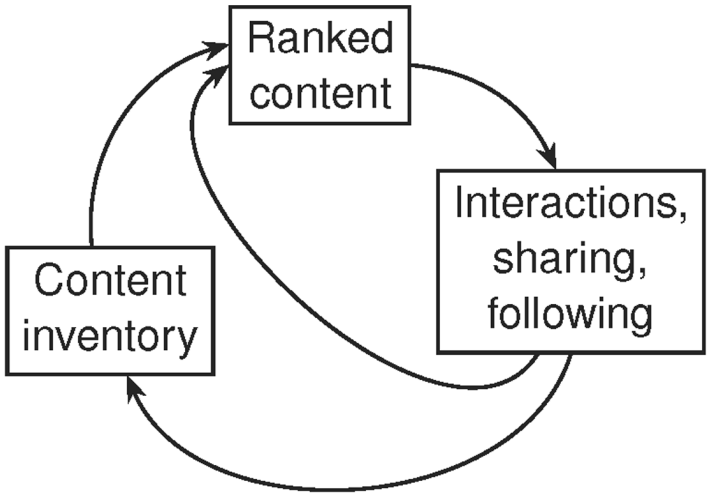
---

[*] These studies are often limited—by platform policies and enforcement—in the number of artificial accounts they can use to probe these algorithms.

[†] While studies by researchers at Facebook[25] document a reduction in cross-cutting political content from the set available from friends to that displayed in the feed, these researchers cautioned[26] that this was not immediately informative about what would happen in a counterfactual world with a chronological feed.

[‡] Perhaps in contrast to conventional wisdom, whether such reduced exposure to cross-cutting content is harmful for society is not always so clear,[26-28] further highlighting that the conclusions here are not so obvious. I am far from alone in arguing that some common claims associated with the "filter bubble" idea lack evidence.[29-31]

[§] With respect to some of the challenges described above and below, this is actually an advantage of this study, as we might expect less dramatic adjustments by users and publishers in response to such a change.



There are a small number of published studies directly comparing algorithmic ranking with simple heuristic ranking by chronology or overall popularity. These are largely in settings (*e.g.,* music and podcast recommendations) removed from much of the public discussion about social media.* However, recently leaked documents from Facebook include a preliminary analysis of a test in which some users were randomly assigned to chronological ranking.[39,40] While we lack important details about this test, and a single such A/B test is not definitive, this reveals how, in the absence of ranking, metrics measuring exposure to likely "bad" content (*e.g.,* spam, items people propogate and then delete) increased dramatically—as did these users' time spent on Facebook and the revenue attributed to them.† Users in chronological ranking also did not seem to like what they were seeing, as they hid many more items. As noted by the author of the internal report,[40] as with the comparisons described above, it is possible some of these effects are only short-run and they might reverse over the longer run as users remove friends, leave groups, or lower their expectations for Facebook and visit less.

A recent article reports on a similar, longer-running experiment at Twitter, in which some users were randomly assigned to chronological ranking.[41] These authors summarize their results as indicating that politicians in general receive "algorithmic amplification" in that they get more reach among users in the status quo ranking compared with chronological ranking; across several countries, right-leaning parties are said to receive more amplification. While this long-running experiment avoids some of the challenges described above (*e.g.,* these users have had time to adjust who they follow), it is still not obviously informative about what would happen in the counterfactual world where everyone has chronological ranking.*

To see an important remaining challenge here, consider how politicians or their social media managers would respond if all Twitter users have chronological ranking. Presently, they have tuned their Twitter activity to the status quo, but if suddenly everything was chronological, they would change their behavior.† Accounting

* For example, Spotify conducted a test of their podcast recommendations in which some users received recommendations personalized based on their listening, while others received recommendations personalized based only on their demographics.[38] The more personalized group listened to somewhat more podcasts, but on average listened to a lower variety of categories of podcasts.

† This highlights that the status quo ranking was clearly not optimized to simply maximize short-run time spent or revenue.

* The Twitter researchers refer to these challenges briefly, citing some of my work[42] and noting that the experiment does not "provide unbiased estimates of causal quantities of interest".[41]

† Sophisticated social media managers would be optimizing this quantitatively, but even individual users (including politicians) would receive feedback via the amount of likes and retweets their different posts get or may view basic aggregate reach statistics provided by Twitter.

for this kind of response from users—and especially from strategic, professional users of a platform—is key to assessing what is truly being amplified by an algorithm. Highly-transparent rankings and recommendations can be easier for various actors to "game".[‡] I would not be surprised if key results from these experiments might disappear or reverse when accounting for these responses.

Platforms clearly regard these feedback loops, spillovers across users, and adaptive, strategic behaviors as important, with several industry and industry–academic teams working on methods to better quantify these effects.[35,38,44] Thus, assessing what a ranking algorithm is amplifying is not a trivial task that platforms have simply neglected. And we may be substantially mislead by assessments of algorithmic amplification that simply compare two rankings of the same content or even compare consumption by users randomized to different algorithms.

Qualitative evidence

In the absence of evidence from quantitative studies, we might look to more qualitative evidence. Commentators frequently point to cases where algorithmic recommendation of, *e.g.,* content or groups is an antecedent of some harm. But it is unclear how much of these outcomes to attribute to specific features of social media, and algorithmic ranking in particular. One useful comparison is that clearly inflammatory content and misinformation can very much go viral in the absence of such ranking, with similarly terrible immediately consequences. For example, viral rumors spread on the group messaging service WhatsApp[§]—which lacks algorithmic ranking—have been the proximal cause of lynching and other violence in India.[46] This hardly proves that algorithmic ranking does not matter, but it certainly highlights the difficulty of credibly attributing harms to algorithmic ranking based on these kinds of observations alone.

This absence of general, credible evidence about effects of algorithmic ranking and recommendation partially reflects the limited ability of external researchers, journalists, and others to probe these systems. Thus, we may expect that efforts to promote algorithmic transparency and to enable producing reports on algorithmic impact using internal, proprietary data could facilitate the creation of better evidence. But this absence also reflects some fundamental challenges, some of which I have elaborated on here, to learning about effects of interventions in these complex environments—even with access to all of the proprietary data.

Policy implications

It is beyond the scope of my testimony and my expertise to make comprehensive policy recommendations. Instead I just highlight a few implications of the preceding discussion.

- Policy-making should not presume that requiring or promoting the use of largely unfiltered chronological feeds in social media will be beneficial. There could be benefits from resulting transparency (*e.g.,* requiring platforms to offer choice may make it easier for external researchers to learn about the algorithms), and perhaps to individual consumers. But there may be other substantial costs, including substantial increases in spam and misinformation without corresponding direct improvements for consumers.
- Minimal versions of algorithmic transparency—such as requiring disclosure of ranking algorithms—may not be sufficiently informative to yield many benefits. Depending on the values of policy-makers, this might suggest these efforts are not worthwhile, or that a broader and more substantial version of transparency, involving disclosure of substantially more data, is needed.
- Algorithmic ranking and recommendation are ubiquitous, often appearing in many distinct channels on the same platform. Policymakers may want to consider whether a particular regulation should apply to all of these channels, especially if compliance requires substantial effort and user-facing controls for each channel (*e.g.,* a prominent icon) and if some channels are already close substitutes for each other.
- Algorithmic ranking and recommendation are not limited to the decision of whether to display and item and in what order, as items can be aggregated or displayed more or less prominently. Expanding this repertoire of user interfaces can be an important site of innovation. Transparency mandates that neglect

[‡] Rankings by recent overall popularity are also often subject to strategic behavior as well. For example, we observed groups coordinate their Twitter activity to make dozens of political hashtags appear on Twitter's trending topics list during the 2019 Indian general election.[43]

[§] In our study of images shared in politics-related WhatsApp groups in India, images identified as misinformation by journalists made up around 13 percent of all image shares.[45]

this may (a) fail to be informative about important decisions by platforms and/or (b) impede innovation in new ways of presenting information and media.

- There are existing (*e.g.,* TikTok, YouTube) and potential social media platforms where there is no obvious "default" ranking. Policies that would enshrine comparisons to a particular baseline when defining "algorithmic amplification" may lead to absurd conclusions for many platforms.
- Naive definitions of "algorithmic amplification" can be misleading because they do not account for the reactions of consumers and (often quite strategic) producers, which can be dramatic. Alongside other problems, this may complicate efforts to use such definitions to establish moral or legal responsibility.[47]
- External researchers (whether academics, journalists,[48] or government officials) depend on the ability to probe these systems. Various data-collection methods often opposed by platforms (including scraping public content, participants consenting to automated contribution of their data,[49,50] confirming participants have stopped using a service,[51,52] and sophisticated audit studies[24,53-55]) remain central to their work. If policy-makers want rigorous external research—whether on foreign interference in U.S. elections[56] or on effects of algorithms—to be possible, they can protect the right to employ these methods, rather than, *e.g.,* the Computer Fraud and Abuse Act discouraging such work.[57]
- Some of the best evidence I have drawn on comes from A/B tests (*i.e.,* randomized trials) conducted by platforms. These are regarded as a "gold standard" for learning about cause-and-effect relationships, and they are a key tool for understanding effects of changes to algorithmic ranking, as well as many other key decisions. Policies and rhetoric discouraging their use could leave scientists and the public less informed—as well as make it harder for the platforms themselves to make good decisions.[58]
- Arrangements whereby platforms share data with external researchers while protecting people's privacy can be beneficial for science and the public. However, there remains substantial uncertainty about what methods for privacy protection satisfy some international privacy regulations,[59] perhaps discouraging more of such sharing. In some cases, privacy regulations have apparently discouraged platforms from even retaining detailed data that would be useful for assessing algorithmic impact.[56]

About me

I am a researcher and educator working at the intersection of communication technologies and topics of broad societal interest, including political participation, public health, and commerce. In addition to doing empirical research, I work on methodology for learning about cause and effect relationships (*i.e.,* causal inference), particularly when people are affected by others' behaviors, as in much of social life, but especially in social media.

I am faculty at the Massachusetts Institute of Technology (MIT), where I am currently the Mitsubishi Career Development Professor, an associate professor in the Marketing group of the Sloan School of Management, and affiliated faculty at the Institute for Data, Systems & Society in the Schwarzman College of Computing, including its Center for Statistics and Data Science. I teach analytics in our professional degree programs and research methodology to PhD students in multiple programs. My academic research has been published in peer-reviewed journals and proceedings spanning several fields. I studied at Stanford University, resulting in five degree including my PhD.

While currently an academic, I have broad knowledge of the Internet industry and state-of-the-art practices there. I was previously a scientist and consultant at Facebook, where I worked on feed, messaging, advertising, survey methods, and tools for randomized experiments. Before that I worked at Nokia and Yahoo, where I likewise worked in research, studying and designing social media. I co-organize an annual conference that involves substantial participation by data scientists and managers from the Internet industry, and I frequently have industry experts as guest speakers in my classes at MIT.

Acknowledgements

I am grateful to comments from several people, including Jennifer Allen, Daniel Björkegren, Tom Cunningham, Andrey Fradkin, Marta Franco, David Rand, and Johan Ugander. Thanks to Alex Kantrowitz for allowing me to review a key document[40] used in his reporting.[39] Responsibility for this document is mine alone.

Disclosures

Here I note some relevant potentially competing interests. My full set of potentially competing interests are listed on my website. I am a consultant to Twitter. My research has been funded by Amazon, Boston Globe Media, Facebook, IBM, the U.S. Air Force (via a subcontract from Lincoln Laboratory), and The World Bank. A conference I co-organize has been sponsored by Amazon, Facebook, and Netflix. I conduct some of my research via both data use agreements with unnamed firms (*e.g.,* retailers, Internet companies, and fitness companies) and by advising research by collaborators, often students, who are employees or consultants of other firms (*e.g.,* Facebook). I have significant financial interests in Amazon, GoFundMe, Google, and Salesforce.

References

1. Pennycook, G., Epstein, Z., Mosleh, M., Arechar, A. A., Eckles, D., & Rand, D. G. (2021). Shifting attention to accuracy can reduce misinformation online. *Nature, 592*(7855), 590– 595.
2. Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature, 489*(7415), 295–298. doi:10.1038/nature11421
3. Jones, J. J., Bond, R. M., Bakshy, E., Eckles, D., & Fowler, J. H. (2017). Social influence and political mobilization: Further evidence from a randomized experiment in the 2012 U.S. Presidential Election. *PLOS ONE, 12*(4), e0173851.
4. Aral, S. & Nicolaides, C. (2017). Exercise contagion in a global social network. *Nature Communications, 8*(1), 1–8.
5. Holtz, D., Zhao, M., Benzell, S. G., Cao, C. Y., Rahimian, M. A., Yang, J., . . . Sowrirajan, T. *et al.,* (2020). Interdependence and the cost of uncoordinated responses to COVID–19. *Proceedings of the National Academy of Sciences, 117* (33), 19837–19843.
6. Aral, S. (2021). *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health—and How We Must Adapt.* Currency.
7. Bernstein, M. S., Bakshy, E., Burke, M., & Karrer, B. (2013). Quantifying the invisible audience in social networks. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 21–30).
8. Mosseri, A. (2021). Shedding more light on how Instagram works. *Instagram.* Retrieved from *https://about.instagram.com/blog/announcements/shedding-more-light-on-how-instagram-works*
9. Kohavi, R., Tang, D., & Xu, Y. (2020). *Trustworthy online controlled experiments: A practical guide to A/B testing.* Cambridge University Press.
10. Backstrom, L. (2016). Serving a billion personalized news feeds. In *Proceedings of the ninth ACM International Conference on Web Search and Data Mining* (pp. 469–469). Retrieved from *https://www.youtube.com/watch?v=Xpx5RYNTQvg*
11. Lada, A., Wang, M., & Yan, T. (2021). How does news feed predict what you want to see? *Facebook Newsroom.* Retrieved from *https://about.fb.com/news/2021/01/how-does-news-feed-predict-what-you-want-to-see/*
12. Smith, B. (2021). How TikTok reads your mind. Retrieved from *https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html*
13. Oremus, W. (2016). Who controls your Facebook feed. *Slate.* Retrieved from *http://www.slate.com/articles/technology/cover_story/2016/01/how_facebook_s_news_feed_algorithm_works.html*
14. Letham, B., Karrer, B., Ottoni, G., & Bakshy, E. (2019). Constrained Bayesian optimization with noisy experiments. *Bayesian Analysis, 14*(2), 495–519.
15. Obeng, A. & Bakshy, E. (2020). Preference learning for real-world multi-objective decision making. In *ICML 2020 Workshop on Real World Experiment Design and Active Learning.*
16. Eckles, D., Kizilcec, R. F., & Bakshy, E. (2016). Estimating peer effects in networks with peer encouragement designs. *Proceedings of the National Academy of Sciences, 113*(27), 7316–7322.
17. Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through optimization: How Facebook's ad delivery can lead to biased outcomes. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1–30.
18. Wilhelm, M., Ramanathan, A., Bonomo, A., Jain, S., Chi, E. H., & Gillenwater, J. (2018). Practical diversified recommendations on youtube with determinantal point processes. In *Proceedings of the 27th ACM International Conference on Information and Knowledge Management* (pp. 2165–2173).
19. Zhao, B., Narita, K., Orten, B., & Egan, J. (2018). Notification volume control and optimization system at Pinterest. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (pp. 1012–1020).
20. Su, J., Kamath, K., Sharma, A., Ugander, J., & Goel, S. (2020). An experimental study of structural diversity in social networks. In *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 14, pp. 661–670).
21. Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science, 366*(6464), 447–453.
22. Rahwan, I., Cebrian, M., Obradovich, N., Bongard, J., Bonnefon, J.-F., Breazeal, C., . . . Jackson, M. O. *et al.,* (2019). Machine behaviour. *Nature, 568*(7753), 477–486.
23. Buolamwini, J. & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (pp. 77–91). PMLR.
24. Bandy, J. & Diakopoulos, N. (2021). Curating quality? How Twitter's timeline algorithm treats different types of news. *Social Media + Society, 7* (3), 20563051211041648.

25. Bakshy, E., Messing, S., & Adamic, L. A. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science, 348*(6239), 1130–1132.
26. Bakshy, E. & Messing, S. (2015). *Exposure to ideologically diverse news and opinion, future research.* Retrieved from *https://solomonmg.github.io/post/exposure-to-ideologically-diverse-response/*
27. Bail, C. A., Argyle, L. P., Brown, T. W., Bumpus, J. P., Chen, H., Hunzaker, M. F., . . . Volfovsky, A. (2018). Exposure to opposing views on social media can increase political polarization. *Proceedings of the National Academy of Sciences, 115*(37), 9216–9221.
28. Levy, R. (2021). Social media, news consumption, and polarization: Evidence from a field experiment. *American Economic Review, 111*(3), 831–70.
29. Guess, A., Nyhan, B., Lyons, B., & Reifler, J. (2018). *Avoiding the echo chamber about echo chambers.* Knight Foundation.
30. Hosanagar, K. & Miller, A. P. (2020). Who do we blame for the filter bubble? On the roles of math, data, and people in algorithmic social systems. In K. Werbach (Ed.), *After the Digital Tornado: Networks, Algorithms, Humanity* (pp. 103–121). Cambridge University Press.
31. Bail, C. (2021). *Breaking the Social Media Prism.* Princeton University Press.
32. Berman, R. & Katona, Z. (2020). Curation algorithms and filter bubbles in social networks. *Marketing Science, 39*(2), 296–316.
33. Bakshy, E., Eckles, D., & Bernstein, M. S. (2014). Designing and deploying online field experiments. In *Proceedings of the 23rd international conference on World Wide Web* (pp. 283–292).
34. Peysakhovich, A. & Eckles, D. (2018). Learning causal effects from many randomized experiments using regularized instrumental variables. In *Proceedings of the 2018 World Wide Web Conference* (pp. 699–707).
35. Gupta, S., Kohavi, R., Tang, D., Xu, Y., Andersen, R., Bakshy, E., . . . Coey, D. *et al.,* (2019). Top challenges from the first practical online controlled experiments summit. *ACM SIGKDD Explorations Newsletter, 21*(1), 20–35.
36. Messing, S. (2013). *Friends that matter: How social transmission of elite discourse shapes political knowledge, attitudes, and behavior.* Doctoral dissertation, Chapter 7. Stanford University.
37. Allen, J., Howland, B., Mobius, M., Rothschild, D., & Watts, D. J. (2020). Evaluating the fake news problem at the scale of the information ecosystem. *Science Advances, 6*(14), eaay3539.
38. Holtz, D., Lobel, R., Liskovich, I., & Aral, S. (2020). Reducing interference bias in online marketplace pricing experiments. *arXiv preprint arXiv:2004.12489.*
39. Kantrowitz, A. (2021). Facebook removed the News Feed algorithm in an experiment. Then it gave up. *Big Technology.* Retrieved from *https://bigtechnology.substack.com/p/facebook-removed-the-news-feed-algorithm*
40. Anonymous. (2018). *What happens if we delete ranked News Feed?* Facebook. Part of "The Facebook Files".
41. Huszár, F., Ktena, S. I., O'Brien, C., Belli, L., Schlaikjer, A., & Hardt, M. (2021). Algorithmic amplification of politics on Twitter. *arXiv preprint arXiv:2110.11010.*
42. Eckles, D., Karrer, B., & Ugander, J. (2017). Design and analysis of experiments in networks: Reducing bias from interference. *Journal of Causal Inference, 5*(1).
43. Jakesch, M., Garimella, K., Eckles, D., & Naaman, M. (2021). Trend alert: A cross-platform organization manipulated Twitter trends in the Indian general election. *Proceedings of the ACM on Human–Computer Interaction, 5*(CSCW2). doi:10.1145/3479523
44. Karrer, B., Shi, L., Bhole, M., Goldman, M., Palmer, T., Gelman, C., . . . Sun, F. (2021). Network experimentation at scale. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining* (pp. 3106–3116).
45. Garimella, K. & Eckles, D. (2020). Images and misinformation in political groups: Evidence from Whatsapp in India. *Harvard Kennedy School Misinformation Review.*
46. Dwoskin, E. & Gowen, A. (2018). On WhatsApp, fake news is fast—and can be fatal. *Washington Post.* Retrieved from *https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast-and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html*
47. Keller, D. (2021). Amplification and its discontents: Why regulating the reach of online content is hard. *Journal of Free Speech Law, 1,* 227–268.
48. Matt, F., Stern, J., Barry, R., West, J., & Wells, G. (2021). How TikTok's algorithm figures out your deepest desires. *Wall Street Journal.* Retrieved from *https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigation-how-tiktok-algorithm-figures-out-your-deepest-desires/6C0C2040-FF25-4827-8528-2BD6612E3796*
49. NYU researchers were studying disinformation on Facebook. the company cut them off. (2021). *NPR.* Retrieved from *https://www.npr.org/2021/08/04/1024791053/facebook-boots-nyu-disinformation-researchers-off-its-platform-and-critics-cry-f*
50. Brinberg, M., Ram, N., Yang, X., Cho, M.-J., Sundar, S. S., Robinson, T. N., & Reeves, B. (2021). The idiosyncrasies of everyday digital lives: Using the human screenome project to study user behavior on smartphones. *Computers in Human Behavior, 114,* 106570.
51. Brynjolfsson, E., Collis, A., & Eggers, F. (2019). Using massive online choice experiments to measure changes in well-being. *Proceedings of the National Academy of Sciences, 116*(15), 7250–7255.
52. Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2020). The welfare effects of social media. *American Economic Review, 110*(3), 629–76.
53. Edelman, B., Luca, M., & Svirsky, D. (2017). Racial discrimination in the sharing economy: Evidence from a field experiment. *American Economic Journal: Applied Economics, 9*(2), 1–22.
54. Metaxa, D., Park, J. S., Robertson, R. E., Karahalios, K., Wilson, C., Hancock, J., Sandvig, C. *et al.,* (2021). Auditing algorithms: Understanding algorithmic systems from the outside in. *Foundations and Trends in Human–Computer Interaction, 14*(4), 272–344.

55. Chen, W., Pacheco, D., Yang, K.-C., & Menczer, F. (2021). Neutral bots probe political bias on social media. *Nature Communications, 12*(1), 1–10.
56. Aral, S. & Eckles, D. (2019). Protecting elections from social media manipulation. *Science, 365*(6456), 858–861.
57. Sandvig v. Sessions. (2018). District Court, District of Columbia.
58. Meyer, M. N. (2015). Two cheers for corporate experimentation: The A/B illusion and the virtues of data-driven innovation. *Colorado Technology Law Journal, 13*, 273.
59. Altman, M., Cohen, A., Nissim, K., & Wood, A. (2021). What a hybrid legal-technical analysis teaches us about privacy regulation: The case of singling out. *Boston University Journal of Science and Technology Law, 27,* 1.

Senator LUJÁN. Thank you, Dr. Eckles. I will recognize myself for questions. And starting a discussion as critical and complex as this one, it is important to start from common ground. And with that, I would like to start with the point where I believe there is broad agreement. Personal data used by online recommendation and targeting systems has come to include everything from personally identifiable information and preferences to individual behavior patterns.

This data draws on the incredible ability for recommendation and engagement algorithms to target consumers at the optimal time with the optimal content to provoke a reaction. Unrestricted access sharing and consolidation of data allows users to be targeted in ways they do not agreed to. Many times they are not even aware that it is happening.

As I said in my opening statement, giving consumers control over their own data is a shared priority. The vast majority of Americans believe Congress should act on comprehensive privacy legislation. Earlier this year, Morning Consult found that 86 percent of Democrats and 81 percent of Republicans want privacy to be an important priority for Congress.

I know Chair Cantwell recognizes this, and I am grateful for her leadership on privacy reform and advocacy for increased resourcing the Federal Trade Commission so it can effectively do its job. Now, Ms. González, how is data privacy a critical component for protecting consumers from the harms of algorithmic amplification?

Ms. GONZÁLEZ. Thank you for the question, Senator Luján. You know, part of the way that harms happen online is because we are being targeted because in ways that companies know that we might be persuaded because of the data they are tracking. So take, for instance, targeted fraud against elders. This is not a new problem. It is a problem we have dealt with as a society for a long time.

But online, a person, an older adult may be targeted based on their perceived fears or interests. And so there is a heightened duty, I think, to protect consumers when they are being targeted for abuse, fraud, and other types of harm in these ways, based on the personal characteristics that they may or may not know they are even giving up when they searched the Internet or go on an app.

Senator LUJÁN. And Ms. Jackson, online platforms take measures to ensure their platforms aren't actively promoting civil rights violations, terrorist recruitment, and other extremism. Unfortunately, too often these systems fail, and platforms instead do the opposite and actually contribute to extreme harms through their algorithmic recommendations. That is why I am proud again to have introduced the Protecting Americans from Dangerous Algorithms Act. Online platforms have real accountability when their algo-

rithms are at fault for making recommendations that contribute to terrorism. So, Ms. Jackson, what principles are necessary to increase platform accountability when they amplify extremism online?

Ms. JACKSON. Thank you, Senator, and thank you for your leadership on this issue. I think what is important and I would commend the companion bill that you recently introduced for taking a similar approach is to focus on not content itself, but on the mechanisms of the platforms, and in particular how they spread across an ecosystem platform to platform.

And so the more that we are looking at questions of the data itself and the incentives behind it, the algorithms that may interact with other incentives on a platform, the business incentives that are a completely different aspect of a platform, the better shape that we are in. And I think that gets back to all of the focus that I think each of the panelists have had on issues of transparency, privacy, protection, and having a better understanding of our ecosystem at large.

[Technical problems.]

Senator LUJÁN.—algorithmic ranking is complex and not just aimed at maximizing short run engagement. Oversight of the harms of algorithmic ranking is a challenge because these systems are complex, and users often respond strategically to try to game these systems. Three, we are still gathering evidence on the harms and benefits of algorithmic amplification. And four, Congress can act to protect external researchers and enable independent oversight and auditing of these systems in privacy preserving ways.

Now, I agree that this is a challenge, but we have to rise to this moment. What can platforms do to reduce the effectiveness of these cross-platform manipulation campaigns?

Ms. GONZÁLEZ. Senator, I am not sure if that question was for me because the audio cut out on my end. Please excuse me.

Senator LUJÁN. That was for Dr. Eckles. Thank you.

Mr. ECKLES. So in some of my own work, we have been able to track some of these cross-platform campaigns because of collecting data on multiple platforms, on WhatsApp and on Twitter. Individual platforms often have blind spots there, and if they start to coordinate more, that can raise questions of anti-competitive behavior or them acting as content cartels, as some legal scholars have suggested.

And so I think getting clear guidance from regulators, whether from Congress or from the FTC, about what sorts of coordination between platforms and data sharing they want to encourage could be helpful. It could allow more of that coordination across platforms. Though in some ways I found it striking just how easy some of these algorithms seem to be to game. And those are some of the ones that are most transparent. What we observed in our research was the trending topics on Twitter being gamed, which is pretty much just a popularity ranking.

And so these groups were able to coordinate looking at the current ranking and work to move their topics up the ranking, in part because everything was so simple and so transparent. And so in a lot of ways, I would like to see the platforms both exchanging more information, but also making some of these algorithms more com-

plex in some ways to account for what they detect when there is this coordination happening. Sometimes this coordination doesn't rise to the level of manipulation, it is in a gray area between genuine political participation and astroturfing.

Senator LUJÁN. Thank you, Dr. Eckles. I will now recognize the Ranking Member, Mr. Thune. Both, Mr. Thune, if you want to take your 5 minutes for an opening statement and then also for questions as well. In addition to that, sir.

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Mr. Chairman. And I won't take that for five minutes and I appreciate your indulgence. Some of us were over at the Capitol at a rotunda funeral there. I do want to ask that my full statement be included as a matter of the record and say how much I appreciate you convening today's hearing to continue the conversation on how these massively wealthy and powerful big tech platforms are using persuasive technology and how they are profoundly altering our future. There is also a growing bipartisan consensus that we need to shed greater light on the secretive content that the moderation processes that social media companies use.

And it is time, in my view, to make big tech more transparent, more accountable, and I look forward to working with you and our colleagues on this committee to get legislation like the Filter Bubble Transparency Act and the PACT Act across the finish line.

So I want to thank each of the witnesses for their participation in this important hearing, particularly as the Committee works to enact meaningful legislation to hold big tech accountable. And I again will submit my entire statement for the record.

[The prepared statement of Senator Thune follows:]

PREPARED STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

Thank you, Chairman Luján.

In 2019, six months before the onset of the COVID–19 pandemic, I served as chairman of this subcommittee, and convened a hearing on the use of algorithms and persuasive technology on Internet platforms.

During that hearing, I noted that former Google Executive Chairman, Eric Schmidt, once said modern technology platforms "are even more powerful than most people realize, and our future will be profoundly altered by their adoption and successfulness in societies everywhere."

Now we are near the end of 2021, and it seems like 2019—only two years ago—was a different age.

Since that time, the pandemic has accelerated the use of technology platforms, and algorithms have become even more ubiquitous in every aspect of the technology we use each day, largely without us even realizing it.

Indeed, while the pandemic has damaged many sectors of the economy, 2021 has been a year for Big Tech's record books, even more so than was 2020.

Already in June of this year, the Financial Times observed that Apple, Microsoft, Google, Amazon, and Facebook were adding a combined $51 billion dollars of equity value *a week*.

The current stock market value of these five companies, at over $9 *trillion* dollars, is more than the value of the next 27 most valuable companies put together.

As Eric Schmidt predicted, these technology companies have grown exponentially more wealthy and powerful, especially over the course of the pandemic.

So Mr. Chairman, I appreciate you convening today's hearing to continue the conversation on how these massively wealthy and powerful big tech platforms are using persuasive technology, and how they are profoundly altering our future.

There is no question that Internet platforms, and especially social media platforms, have transformed the way we communicate and interact with friends, family, and the public.

So much of the content we see on social media is entertaining, educational, and can be beneficial to the public.

However, I, along with several of my colleagues, and the public, have become more and more concerned about the influence and power of big tech within our society and the potentially damaging effect these platforms can have on individuals.

We've heard testimony earlier this year about social media's damaging effects on consumers.

Hearing after hearing demonstrated that users are not aware of how their data is being used by big tech to affect their behavior and influence certain outcomes.

We know that a major problem with social media platforms, as well as search engines, is their use of secret algorithms—artificial intelligence developed by Silicon Valley software engineers that's designed to shape and manipulate users' experiences.

The powerful AI behind these platforms serve as prediction engines, creating a unique universe of information for each user, a phenomenon that's often referred to as the "filter bubble."

The filter bubble contributes to political polarization and social isolation.

Perhaps the most important thing to understand is that most users don't make a conscious decision to enter the filter bubble.

This can be particularly troubling for younger users.

For example, a recent Wall Street Journal investigation described in detail how TikTok's algorithm serves up highly inappropriate videos to minors.

As a general matter, the economic incentives are aligned for big tech to keep the filter bubble in place, without users' awareness, because platforms only make money by keeping eyeballs on their platforms as long as possible.

Without congressional intervention, platforms have very little incentive to be more transparent about the existence of the filter bubble.

The days are over when you logged into your favorite social media platform and consumed content that had been posted chronologically since your previous log-in.

Now platforms like Facebook, Instagram, and TikTok—and other social media platforms, as well as search engines—use algorithms to shape your newsfeed and suggest additional, seemingly never-ending content, emphasizing posts the platforms think you'll be interested in and deemphasizing the ones they want you to scroll past.

And looking to the future, at the cutting edge of the use of algorithms, machine learning, and artificial intelligence on Internet platforms, is the idea of the "embodied internet," or "metaverse," which Mark Zuckerberg described as "the next evolution of social connection" when he changed the name of his company to Meta this past October.

The aspect of algorithms amplifying or suppressing content leads to increasing dissatisfaction and suspicion about bias being built in to the algorithms.

Big tech platforms are certainly free to deploy algorithms that select content based on what will keep each user engaged.

But the platforms should not be free to keep their users unaware of the fact that an algorithm is controlling which content each consumer sees on the platform.

With some rare exceptions, people aren't given a choice to easily opt out of a black-box algorithm that secretly selects the content they see.

We're learning more and more about what the problem is, and I have offered several proposals aimed at giving the public more transparency into these systems, and more control and accountability for consumers.

I've introduced the bipartisan Filter Bubble Transparency Act, which would give consumers the privacy, choice, and transparency that has been absent on these platforms for too long.

Specifically, large-scale Internet platforms would be required to notify users that their platform uses secret algorithms to select the content they see, what's often described as the "filter bubble."

In addition, users would be given the choice to switch to a different version of the platform that is filter bubble-free.

At the very least, users should have the option to engage on these platforms without being manipulated by secret algorithms.

There's also a growing bipartisan consensus that we need to shed greater light on the secretive content moderation processes social media companies use.

That's why I've introduced the bipartisan PACT Act, which, among other things, would require Internet platforms to make biannual transparency reports outlining material they've removed from their sites or chosen to deemphasize available to the

public—and not just in intentionally complicated, hard-to-understand legalese. Sites would also be required to provide consumers with more due process and explanation when content is removed or otherwise moderated.

It's time to make big tech more transparent and accountable, and I look forward to working with my colleagues to get these proposals across the finish line.

Today, each of our witnesses has deep expertise regarding algorithms and artificial intelligence more broadly, as well as in the more narrow context of engagement, prediction, behavior modification, and persuasion, and brings valuable perspective about where we are today and what we can expect in the future on these matters.

Your participation in this important hearing is appreciated, particularly as this Committee works to enact meaningful legislation to hold big tech accountable.

Thank you, Mr. Chairman.

Senator THUNE. Mr. Eckels, there is a growing concern that large technology platforms may one day know every individual even better than we know ourselves. In your written remarks, you discussed the vast amount of data Internet platforms have on users and that these platforms are able to predict certain outcomes for every individual based on this data.

Could you talk further about how Internet platforms use algorithms to make predictions about each user and how they influence the behavior of every individual, and perhaps how that might concern you?

Mr. ECKLES. Thank you, Senator Thune. I would say, while some of these tech giants have a lot of data about many of us, we are a little ways off from having that kind of a mastery. Sometimes it seems like the people most convinced of that mastery are the tech critics and marketing snake oil salesman like the people at Cambridge Analytica who were suggesting that they really could control people and they could predict them so well. So I think we have a bit of time in that sense. What I have been sometimes concerned about in the past is when this ability to predict people's behavior, how they will respond to messages, reaches across many domains.

Maybe I have interacted with one firm where I bought some products. Can they also use that same data to know how to persuade me in politics? Could they sell that for that purpose? Could they use that same data to help me stick with my fitness goals, so there could be some benefits there as well? But in a lot of cases, when that data jumps from one domain to another, I think that is a potentially concerning area. And when you have single firms that reach into so many parts of our lives, we think they might be able to start doing that kind of cross domain prediction.

So that is one of the aspects that I find concerning is that it may be hard for consumers to understand that this data about some purchases I made could also be used in conjunction with some other data about other people to predict my behavior in a totally different setting and to target totally different types of messages, maybe political messages, to me.

So that is one aspect that I find concerning because there is this opacity, and it is a little hard for consumers to understand the consequences of this one disclosure for this very other setting.

Senator THUNE. Mr. Poulos, what is your reaction to Mr. Eckles' testimony highlighting the vast amount of data these companies have on individual users? And do you believe that large tech companies use persuasive technology, meaning the technology is designed to change people's attitudes and behaviors?

Mr. POULOS. Thank you, Senator. Short answer is, yes. Longer answer is it is inherent in the nature of this technology. This is a communications technology and other communications technologies, probably all of them in history, have been used and were inherently designed to influence people and to cause changes in their behavior, printing press, radio, television. These things are a part and parcel of, you know, whether you want to call it mind control or something more benign, this is how it works with human beings.

We communicate with each other and those who have the most control over communications infrastructure and technology wield that control to move hearts and minds to sculpt behavior. So I think it is inherent to digital technology. I think that we need to be aware that what is really going on here is the amassing of personal information inside data bases so that large groups of people can be conditioned in certain ways to accept and prefer certain ways of life, certain ways of Government.

That is just kind of baked into the technology, and that is why it is so important that we make sure that ordinary Americans have the ability to use technologies to build institutions that serve their humanity and protect their country and their culture.

Senator THUNE. I want to come back to that, but let me ask Mr. Eckels, you mentioned in your testimony that quantifying the impacts of algorithm ranking is quite difficult due to the complexity of both technical aspects of algorithms and due to people's complex responses to changes with algorithms. If this is the case, what should policymakers require or expect of Internet platforms with respect to algorithm explanation or transparency?

Mr. ECKLES. Thank you, Senator. I think the answer is going to be different in different settings. So in some settings, some of the most important area sensitive settings like diagnoses in health care are not nearly as subject to such rapid strategic responses. And so while I don't study the health care system, I think this is something that the Federal and State Governments are actively involved in already, and so it would be natural for them to regulate quite closely the adoption of algorithms in those settings.

When it comes to communication technologies and social media, it is not clear exactly what type of transparency we need. In fact, these algorithms often can be broken up into multiple different pieces, as I have detailed in my testimony.

And that can be one tool for how Congress and other policymakers can get some transparency. So I don't know if Congress should mandate explanations and transparency, but I hope that my testimony provides kind of a blueprint for what questions should be asked of these firms. So they should be able to tell you and the public how much weight they put on predictions of clicks, predictions of reshares and retweeting, versus how much weight they put on predictions of survey responses about whether people say this is really important to me, or how much weight they put on potentially negative signals that tell them that people regret their engagement, that maybe they spent too long on the platform, or that they wish they hadn't reshared that piece of misinformation.

And so by being able to tell policymakers and the public about those weights, I think that provides one opportunity. I mean, as I

was preparing my written testimony, I was really struck with some of the reporting in the *New York Times* about TikTok.

And it turns out their algorithm matches exactly what I had written without really any knowledge of that, except that it seems to lack many of those signals. They seem to not be, at least according to this reporting, collecting data about people's more considered opinions of whether this was a worthwhile video to have seen or any signals that I saw this and then later, I felt misinformed or misled.

And so probing that and pushing platforms to actually be more sophisticated in their algorithms, I think could be beneficial.

Senator THUNE. So a qualitative as opposed to quantitative. Just very quickly, and I know my time expired, Mr. Chairman, but I—since I didn't use my 5 minute opening statement, I want to just ask one question, and Mr. Poulos, coming back to what you said about these are communication mediums and, in other words, designed to influence people. I want to come back to this question. You said that decision should be made about these being used in a way that is positive or good for humanity.

And I guess my question is and the thing I think concerns a lot of us is who decides what is good for humanity? Who is behind the curtain making these decisions? And then I want to ask you this question because you discussed the notion that we are in the nascent stage of a social credit system with regard to the use of AI and algorithms on Internet platforms.

And I am curious what your thoughts are about what approaches Congress should be considering to prevent a social credit system. So you can answer that question, but maybe answer the bigger question about who decides what is good for humanity?

Mr. POULOS. Sure. That is a very good question, Senator. You know, ultimately this is a Government by, for, and of the people. And I think we have to keep that in mind as we grapple with the question of how to ensure that our form of Government is not replaced by a social credit system.

The reality is that every major power in the world right now, every civilization state, as some call them, is racing to establish sovereign authority over the digital technology within its territory. And because of the way that these super powerful digital entities raise ultimate questions about our place in the universe, about what it is to be human, why we should bother? We seem to have created things that are that are bigger and smarter and have superpowers that we lack.

So, many countries are responding to that kind of feeling of disenchantment or fear by turning to their deepest cultural resources, which are, in many cases, theological resources. You see China with the Great Firewall and, you know, trying to focus on making algorithms and programs Daoist. Russia's response to the digital revolution was to build a very large military cathedral just outside of Russia. And in countries in the West, like France and others, they are actively looking for ways to make sure that digital technology really captures and expresses and even enforces their particular cultural leanings. You see India pursuing some of these things and Israel and others.

In the U.S., we have a First Amendment, and we have a prohibition on the establishment of religion. So we really have a special challenge because we can't sort of take that theological, theocratic option and say, "look, the Government is going to decide, you know, what the proper system of ethics is, what counts as harm, you know, whether something like transhumanism is something that, people shouldn't be exposed to or whether it is something that actually exposes them to, you know, what they need to know in order to flourish." The Federal Government needs to make sure that it doesn't nationalize social media in an effort to turn it into a tutelary system that programs Americans the way that they want Americans to be programmed.

So, you know, I think the best option is to make sure that Americans can buy and use digital technologies, high powered GPUs, bitcoin so that they can freely build new institutions, cultural and market institutions, in a digital environment where they can freely protect their human identity and make sure that we preserve our form of Government and argue openly about fundamental political questions.

Senator THUNE. Thank you. Mr. Chairman, thank you.

Senator LUJÁN. Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much and thank you for doing this hearing. Really important, Mr. Chair. Thank you to our witnesses. Algorithms touch every aspect of our lives. We know that. And it is not typically very pretty. And what we know is that Americans are getting increasingly addicted to platforms, especially young people taking up significant parts of their days. And part of that is because of how they are targeted.

Yesterday, we had a hearing with the head of Instagram, and I pressed him about the fact that the *New York Times* reported that his major increase in the marketing budget, $67 million in 2018 to $390 million this year was focused on wooing teens, mostly allocated to that. And as some of our colleagues have discussed, we need Federal privacy legislation, but we also need more transparency on algorithms, and we need to do something about this.

Senator Coons and Portman and I introduced a bill today to require that the companies make—allow access to outside researchers. Some of this has been shut down, as you know, by Facebook, now Meta. But I think it is important for my colleagues to know that there is more going on here than meets the eye. Amazon is creating knockoff products made by small businesses and then using its algorithm to show its own version of the product they ripped off first. That has happened, *Wall Street Journal* reporting. Or number two, Apple is doing this when you search for maps or music or podcasts, the first result is often an app that Apple makes, even though they control the platform. And algorithms provide—pervade our entire existence online.

And one of the most shocking things that I think came out of the whistleblower documents was the fact that, it didn't surprise me, given my own experience online, maybe when I put something out there that Senator Thune and I worked on a bill together, it might

not be as an attractive to the algorithms of Facebook as some other forms of speech, no matter how interesting I try to make it sound.

And then I find out that in fact, the angry emoji gets five times attraction as a simple like. So if our constituents in Minnesota and South Dakota want to put a simple like, they may never see that post on Facebook because it is the angry ones with the angry emojis that are going to start getting traction.

So Ms. Jackson, in your testimony, you talked about how these companies designed their algorithms to promote engagement. And it is, of course, to boost advertising. I think we have to think about that. They want to get it out there so people get addicted, so they get more advertising revenue. Can you tell us more about how companies designed algorithms to increase the time users spend on their platform and how that affects users?

Ms. JACKSON. Thank you, Senator, and I am looking forward to reading the bill in detail that you just mentioned referencing—introducing today. It is an important step in ensuring that we do have more visibility into how these platforms operate in our ecosystem at large. I think to your question, I want to call back real quick to something we have been talking about in the context of these algorithms. I think over indexing or emphasizing the ability of tech companies to know us and the kind of perfection, the idea of perfection of these algorithms, can cause harm as well.

Because as you alluded to, we are not just talking about algorithms on social media, we are talking about algorithms used, whether it is to help Amazon promote its own products, or frankly, to help insurance companies make decisions about what your premiums should be, what your sentencing might be in a criminal justice context. Those are all very different contexts. But if we believe that those algorithms are in fact infallible, that they have the most accurate representation, we might be tempted to allow those algorithms to be integrated into our decisionmaking, Government decisionmaking, determining the rights that we might have.

And I would call back to examples of, you know, maybe I joined a member program at my local bar, and it says I have been buying more drinks and I lost my Apple Watch and so says that I haven't been exercising too much, and so my insurance company has decided that I am a depressed alcoholic, and I am then denied for a loan.

And that may sound fantastical, but right now there is nothing that would make that illegal. And so I think coming back to putting these in context, algorithms themselves are not a magical solution in one direction or other. They are not a magical harm. But it is important that we have accountability, that we have limits on data collection that power them, and awareness of the ways in which they are used in our lives.

Senator KLOBUCHAR. OK. So one other piece of this, the other bill that I should also mention, that has kind of, I think one commentator called it the Ocean's Eleven of co-sponsors, that I have with Senator Grassley and Graham and Warner and Booker, and including two on this committee, Senator Blumenthal and Senator Lummis, and what that bill is about is about getting after this exclusivity, the self-preferencing, the discriminatory behavior that just no one that looks at it can really think it is okay. It is just

that our laws haven't caught up to a major, major part of our economy.

And my view has always been that competition is good for innovation. We have heard a lot of claims that somehow doing something is going to undermine the tech companies, but in fact, they are doing just fine. And what we want to make sure is we continue to foster competition. Could you talk about how this innovation can ultimately by monopolies and dominant platforms get stunted? And do you share concerns on this—along these lines? You started up—you started a startup, right?

Ms. JACKSON. Yes. I don't actually talk about that a lot. I founded a small tech company to try and help Americans become more civically engaged. And you know, I was—I didn't really have a choice, honestly, in using Facebook and Google advertising tools. It is kind of—in the startup community, just it is the only option. We kind of joke about it as the startup tax, that a large portion of your budget, no matter what you do, is going to go toward cloud providers of Amazon or Google and advertising and Facebook and Google, regardless of whether you want to——

Senator KLOBUCHAR. They are each dominant on their own sector is what it is.

Ms. JACKSON. Absolutely.

Senator KLOBUCHAR. OK. And so——

Ms. JACKSON. Sorry. Yes. I mean, I think there are serious consequences for what that means for competition at home, but it also means that the ability to feed, everyone has to feed into a system that is collecting more and more data that is driving these incentives that we are talking about.

And so no matter what angle, we want to address these online harms, whether we are looking at competition issues or privacy issues or content issues and extremism, they are all interconnected because it is a system that feeds itself. And so again, I applaud members of the Committee focusing on privacy and transparency.

Senator KLOBUCHAR. And would you agree that at some point we have to stop talking and have a little less talk and a lot more action?

Ms. JACKSON. I am a big fan of action, Senator.

Senator KLOBUCHAR. OK, thank you.

Senator LUJÁN. Senator Fischer.

STATEMENT OF HON. DEB FISCHER, U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Thank you, Mr. Chairman, and thank you to all our witnesses for being here today for this very timely discussion. Many of you described in detail how Internet platforms increasingly quantify and tailor our online experiences in granular ways. On one hand, you get more personalized user experiences and platforms are more responsive to what makes you tick. But this also allows companies to take persuasion too far. Companies are constantly competing for our attention. This increases the motivation for more intrusive technologies, including the web design around those technologies. It forces us to assess the impact of online persuasion on user choice and privacy.

Yesterday, I was proud to reintroduce the DETOUR Act with my colleagues, Senators Warner, Thune, and Klobuchar. The Act would prohibit large online platforms from purposely using deceptive user interfaces, also known as dark patterns.

Many of us can recognize the dark patterns we have personally experienced where we are trapped into clicking, clicking, clicking, clicking and trapped into buying or signing up for something that you don't really want because the user interface intentionally confuses the options that are presented. Our legislation would take an important step, I believe, to restore the hidden options and improve user autonomy.

Dr. Eckles, I appreciated your technical perspective about how persuasive technologies are developed as we seek to craft related policies. Do you think that we have enough debate and guidance on the ethics in designing technology that influences our behavior within the tech industry or in academia?

Mr. ECKLES. Thank you, Senator. I would like to see more discussion of these ethical issues in the tech sector and in the public as well, and especially not just from ex-tech insiders who now are repenting but really drawing on kind of the rich expertise that we have from ethicists and policymakers in the way that bioethicists have provided some guidance in the context of thinking about clinical trials, et cetera.

So I do think we want more guidance there. One of the things that I think of with the Detour Act, at least in the last version I was familiar with was, that from my perspective, it is very important to allow and encourage these platforms to continue to do A/B tests, continue to do randomized trials. That is much of the evidence that I have drawn on whether published work by those platforms or leaked is A/B test that they have conducted.

And so I would hope that while we can shut down some of these dark patterns maybe that has to do with subscription services, etcetera, etcetera, that we also still allow these platforms to keep making systematic comparisons of different options and hopefully sharing more of those results with the public.

Senator FISCHER. Do you think that the designers and developers right now are approaching taking into any kind of consideration the ethical consequences here?

Mr. ECKLES. Thank you, Senator. I think at firms that are established and have found themselves with a bit of a breathing room and a large staff with technical expertise, they are. I mean, in some ways that is part of what we have seen in the Facebook files leaks is a huge amount of disagreement and debate about some of these issues. But a lot of times that happens only after some engineer quickly built something, it got big, and then now there is a whole bunch of data scientists and researchers cleaning up the mess.

Senator FISCHER. So how do you get the ethical considerations at the front end of development? How do you incentivize or encourage, I would rather go that route, to have designers really, really work, not just with Government, but with business and academia to be able to get that done? How do you do it?

Mr. ECKLES. Thanks, Senator. I think one way is to make the public and all these potential designers really aware of the long-term negative consequences of some of these choices, right.

Facebook's reputation is still deeply hurting from some of the move fast and break things decisions that they made years and years ago. So that is a consequence that they are living with that brand. And so thinking about that as an entrepreneur is important. From my perspective, I also think about that, in the context of education, that we have burgeoning enrollment in computer science programs.

Ethics and these considerations and social sciences have to be part of that curriculum in some way. And so I know in some of my own teaching and analytics I try to bring that in. But it is also useful to draw on additional expertise. We are trying to hire a philosopher of technology ethics at the moment at MIT in order to help this be part of the curriculum.

Senator FISCHER. I think it is important that we bridge the technical consideration with the policies that we seek to implement, and I appreciated your points about the value of A/B testing, which remains important if we are going to have improved user experiences and distinct from the dark patterns that we are trying to address. So I thank you for that, sir. Thank you, Mr. Chair.

Senator LUJÁN. Thank you, Senator Fischer. Senator Schatz.

STATEMENT OF HON. BRIAN SCHATZ,
U.S. SENATOR FROM HAWAII

Senator SCHATZ. Thank you, Mr. Chairman, Ranking Member, thank you, and to all of the testifiers for your thoughtful remarks. I just want to respond a little bit to Senator Fischer's question because Dr. Eckles, with all due respect, I don't think that this is going to end up being effective if it is voluntary because you can't have individual coders to sort of waking up in the morning and saying, what are the ethical implications of this? Because they are engineers, they are supervised, they are told to deliver a product, they deliver that product.

The only way to provide an effective counterweight to the fiduciary obligation to maximize clicks, which is essentially as Senator Klobuchar said, the maximization of revenue is to establish in Federal law an affirmative obligation not to harm the consumers whose data is being collected. I am all for notice and consent, but we all know that we click, I agree, as a matter of course without reading anything, and it is not fair to individual consumers to ask them to opt out of the world, essentially, in order to retain their privacy rights.

So the only, in my view, the only way to do this is to establish, you may collect data from individuals as you are, but you have an affirmative obligation to not use that data against people, which doesn't mean you can't do behavioral advertising, it just means you can't harm people. Most companies are comfortable with that.

The ones that are not comfortable with that either have Government relations and lawyers who are just nervous about what that would mean, or they are actually worried that they are in the business of harming people. So just wanted to offer that for Senator Fischer. I have not yet had a Republican co-sponsor of our legislation, but I would invite you to take a look at it. For Mr. González, you know, Chair Khan is known as a sort of antitrust crusader, and I know that she is moving on FTC action against some of these dominant Internet companies from a competition policy standpoint.

But I am wondering about the Section 5 authority to find unfair and deceptive practices, and even the FTC's authority under the Equal Credit Opportunity Act and the Fair Credit Reporting Act. Does the FTC have authorities that it is not yet using? In other words, have we already delegated some of this policymaking to the FTC and should it exercise additional authorities?

Ms. GONZÁLEZ. Yes, Senator, I do think it already has some authority to act here and it should exercise that. I think the work that Chair Khan is doing on the antitrust front is incredibly important.

I also think an inquiry about how companies are violating our privacy and using our data to harm us is incredibly important and should move forward under the Unfairness Doctrine, which the FTC already has authority to move forward on. The other two statutes that you referred to on credit reporting, certainly, I think the FTC should enforce that statute.

Those statutes may not be broad enough to get at the harms that we are seeing online where our personal data is extracted, used to target us in harmful ways. And so that is why I believe the FTC ought to initiate a proceeding focused on privacy and civil rights as well.

Senator SCHATZ. Yes, just in response to the last comment you made about, you know, it may not be—we may not have a broad enough statute, point taken. But I will also observe that, you know, been on the Commerce Committee for now a number of years, and our complaints about tech and big tech are so broad and so numerous as to overwhelm our policymaking ability.

Besides the filibuster and our normal partisan disagreements, we sort of can't separate out what are we just irritated by, what do we think is real harm, how do we balance the needs of American users of technology with the kind of fear that we could set a precedent for, say, Kyrgyzstan to impose authoritarianism through their own controls. So I think that the important thing for us as a committee and as a Congress is to chip away at this, is to say, well, what Section 230 reforms makes sense, right, and what antitrust actions makes sense, and what protections for researchers make sense?

Because I do think that, especially during the last Administration, this sort of invocation was almost an incantation against big tech became so expansive as to become meaningless and very difficult for policymakers to sort out and even more difficult for politicians to sort out. Because if you say, well, it is not so simple, you look like you are schlepping for these big tech companies when in fact, this stuff is complicated, and we have seen sort of comprehensive legislation fail and fail and fail.

And I subscribe to my predecessor, Danny Inouye's point of view, which was his 40 percent rule, which is try to get 40 percent of whatever you are asking for, and by the third year, you have already got more than you have ever asked for. I always chop that in half and say I got 20 percent because I am certainly not Danny Inouye. Thank you.

Senator LUJÁN. Thanks, Senator. Senator Blackburn.

STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE

Senator BLACKBURN. Oh, Mr. Chairman, thank you so much for this hearing. And as our witnesses have heard, this is a very timely hearing. We have had quite a focus on technology issues. And I know Senator Klobuchar mentioned to you the hearing that we had yesterday where we had the Instagram CEO before us. And Senator Blumenthal and I are continuing to work on these issues around privacy and data security, making certain that the virtual space is going to be safe for all users and especially for our children.

Mr. Eckles, let me come to you, and thank you for your well-written testimony. I want to pull from that. You mentioned in your testimony, and I am quoting you, "there is no large body of evidence on the effects of the algorithmic ranking." You also noted that "for a single user, there are often are more possible rankings of available items than there are atoms in the universe. So even though the same data may be entered in the algorithm, a huge variation in outcomes could occur." Alright, so here is my question.

Given all this, is it even possible to attain algorithmic transparency and get to where we are trying to go with the effects of these algorithms? Or would the data outputs be too large to even begin to make heads or tails of them?

Mr. ECKLES. Thank you, Senator. I think there are hard problems here, but I don't want to make it sound like all versions of algorithmic transparency are impossible. And I think breaking it up into smaller problems can help. Actually, even for data scientists and ranking engineers of these companies, they have to do a lot of work to understand their own algorithms in a lot of cases.

And that is in part because they are doing things like looking at the contents of a photo, figuring out what is in the photo, and knowing whether you might actually be interested in that content, right. So that becomes a very complex process. But luckily, some of that can be broken down into kind of more comprehensible pieces, because at the end of the day, there is a prediction about whether you are going to click on that content, whether if we asked you in a survey, you would say it was important.

And those are each given weights in these algorithms. Those weights, if disclosed, can give you a good picture of what is actually being valued. The *New York Times* reporting on TikTok wrote out the equation, supposedly, for TikTok's weights on those predictions. So that kind of level of transparency could take us somewhere that isn't necessarily the entire algorithm, which in fact has billions of parameters. There are billions of numbers used to determine these algorithms.

Senator BLACKBURN. OK, let me interject right there. Let's talk about TikTok. We know the TikTok likes to hook young users, and we know that TikTok is collecting this information. And basically, what they are doing with their Chinese Communist Party shared ownership, I guess you would say, is they are basically creating dossiers on Americans. And then they have the ability to funnel that information back to the Chinese Government. Should policymakers give more thought to the way that algorithms and the way that companies collect the data, the way they hold this data, the

length of time they hold that data, and then look at that as a national security risk?

Mr. ECKLES. Thank you, Senator. I think as Americans, we have had the luxury of having so many of the tech giants here in the U.S., and the result of American innovation. And so as that changes, as we depart from that that raises a bunch of questions and a lot of ways other countries have been grappling with for a while.

And so my sense is that there certainly could be additional scrutiny there when data is moving overseas to authoritarian regimes that perhaps don't have the kinds of privacy protections that we at least like to imagine for Americans here.

But policymakers maybe have to think about this from a foreign relations perspective as well, because a lot of these other countries are imposing regulations that require data from American companies to be there locally, require employees who are locally in that country to potentially be on the hook criminally if those companies don't comply with sometimes really un-American regulations locally. So I don't know how to navigate that, but it sounds like an important project for all of you.

Senator BLACKBURN. OK, Mr. Poulos.

Mr. POULOS. Hi, Senator.

Senator BLACKBURN. Yes. Mr. Poulos, do you have any comment?

Mr. POULOS. I think what I would say——

Senator BLACKBURN. Mr. Poulos, I am sorry. Yes.

Mr. POULOS. Sure, yes. I mean, I think what I would say is that algorithms can't be neutral, and we shouldn't expect that we can engineer them to be neutral. It is in the nature of them to move behavior and opinion and that what the social media companies have done that I think in a sense is most productive of harm is that they have convince people that what happens on screen is more important than what happens off.

And the reality in a digital age is that what happens in the database is more important than what happens outside the data base. And so when you have companies that are convincing users that their life online is more important than their life off, there is a disconnect there between that impression and the reality that those users are actually being onboarded into a really comprehensive data system where they have no agency as citizens. And that disconnect is one that is very difficult to legislate away.

So I think the important thing to do is, you know, yes, we can nibble away at and ameliorate certain kinds of algorithmic harm. But really, what we want to do is make sure that Americans can recognize that they can build new institutions that preserve their way of life and preserve their agency as citizens and as members of a community through digital technology, that really social media isn't the extent of digital technology.

And I think what we are seeing with Facebook trying to change into Meta and other similar moves, that social media companies are aware to a degree that perhaps their form of technology is just technologically limited. And so this is a fast shifting space. And while, you know, as one of the other Senators indicated, it is easy to point out what is frustrating, irritating about the space. Ulti-

mately, you know, trying to make social media a creature of the Federal Government is not going to get us where we need to go.

Senator BLACKBURN. Thank you. Mr. Chairman, thank you for the time.

Senator LUJÁN. Thank you very much. Senator Markey.

STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman. At the same time, social media companies can't escape the same rules that everyone else has to play by. So, you know, I think many in the industry think that just because they have to play by the same rules, means they are a creature of the Government. No, they are not a creature of the Government, they are a creature of the American people. That is who they are supposed to be serving, the American people, and they can't escape those responsibilities.

And so I thank you, Ms. González, for mentioning my bill because what my bill says is that there has to be a prohibition on algorithmic processes on online platforms that discriminate on the basis of race, age, gender, ability, and other protected characteristics. These young white men, privileged men who write these algorithms, and that is who does it, they are writing algorithms that discriminate against people. And there are laws against it in the real world, and they have to be laws against it online as well, because that is where the world no operates.

If you are looking to get a job, if you are looking to get housing, and you are black or you are brown or you are LGBTQ or disabled, these young white men can write algorithms that help companies to avoid all of the laws that apply in the real world, and we know that. So, Ms. González, talk about that, will you, a little bit and how this whole world of algorithms is just another cover for discrimination that were banned in the real world?

Ms. GONZÁLEZ. Thank you for the question, Senator Markey. Yes, one of the reasons that Free Press Action is very enthused about the legislation you put forward is because we know that discrimination exists. We have a long standing civil rights law that bans discrimination in housing and employment and in many other scenarios. And what we need is to clarify that those protections apply in the digital world as well. It is actually not rocket science.

This is a long standing set of societal norms and laws, and they ought to be enforced in the digital world as well. I think what is even more pressing about how discrimination happens online by algorithms is that it is happening based off another abuse of our civil and human rights, which is an invasion of our privacy. So I think this is a critically important part of the problem that we need to address immediately. And I am so grateful that both your bill and COPRA address this.

Senator MARKEY. Yes, so that is where we are. We have young white men who create algorithms, you know, algorithms that run from here to Osaka and back in a nanosecond that wind up being in a black box that no one can understand that then discriminates against black people, brown people, LGBTQ people, and many others in our society. And we just have to have transparency, but we

need a safety and effectiveness standard to protect against discrimination online. Do you agree with that, Ms. Jackson?

Ms. JACKSON. Thank you, Senator, it is an important question. I would reframe——

Senator MARKEY. But do you agree?

Ms. JACKSON. I agree that we absolutely need protections. And I believe that the most vulnerable in society are often the most harmed by online issues that we are discussing. But that is why I get back to the kind of systemic aspect of this——

Senator MARKEY. But in this area. I am just talking about this area. In this area, it is systemic, but in terms of this harm, you do agree that it is egregious what goes on and how algorithms are used to discriminate? You do agree with that?

Ms. JACKSON. I agree. I would return to something I said before, which is over indexing on the power of algorithms intentions. Some of the greatest harm we have is when people put algorithms into the world without thinking about it and a lot of the discrimination, I agree with you, that comes out of that is actually the unthinking nature of the design of technology.

Senator MARKEY. But it can also be thinking.

Ms. JACKSON. Absolutely.

Senator MARKEY. You can actually design algorithms.

Ms. JACKSON. Absolutely.

Senator MARKEY. So it can be young white men who are thinking in terms of how they discriminate against black and brown, LGBT, and disabled. But it can also just be an algorithm to set up in order to accomplish the goal that the redlining that is accomplished by a company in real life is also furthered by what they do online, the digital redlining. And its thinking or unthinking, but nonetheless, the impact is dramatic in terms of how it has a negative impact on families. So should we ban it? OK, let me go—let me go to you, Ms. González, should we ban that discrimination online?

Ms. GONZÁLEZ. Yes, of course, anything that is banned in real life in terms of discrimination ought to be banned online. Now the tricky question here is whether the platform itself is engaging in discrimination or whether they are dealing with third party content that is discriminatory in nature. And so that is an important distinction. But I think the way that you set this out in your bill really gets to the heart of what platforms are doing and holding them accountable for their own actions, which is what we ought to be doing.

Senator MARKEY. And thank you for that. So, yes, these hearings are all very helpful. They discriminate and they target children, OK, but they also discriminate against those who are most vulnerable in our society in addition to children.

So that is why it is so important for us to legislate because we would never allow this to happen in real life. We would never allow people to engage in these kinds of discriminatory practices against minorities or exploitation of children. And same rules for the real world have to exist in this unreal world that has been created principally by young white men who get very rich in drafting these algorithms. And that whole, area has to—in our society. Thank you, Mr. Chairman.

Senator LUJÁN. Thank you, Senator Markey. Senator Lee.

STATEMENT OF HON. MIKE LEE,
U.S. SENATOR FROM UTAH

Senator LEE. Thank you very much, Mr. Chairman. We often talk about Government regulation or requirements that would address these legitimate problems with big tech. One issue that I continue to grapple with—that it really is a challenge, I think we ought to think about it as we consider legislation in the tech space—involves the potential for deeper entrenchment of market incumbents.

Dr. Eckles, I would like to start with you. Government regulation can be expensive in terms of compliance costs, correct? It costs a lot. Not everybody can do it. But those who are already there, those who have already arrived, who can afford a team of compliance specialists and accountants and lawyers have some advantage to the point where entry can be difficult to impossible it. Do you agree that regulation can have this kind of an effect?

Mr. ECKLES. Thank you, Senator. Yes, I think we have actually seen some of that in the context of GDPR, the European Privacy Regulation, where there is evidence that that increased consolidation as many firms stopped doing business with all but the biggest players who could ensure compliance.

Senator LEE. So is there a way to thread that needle? How do we undertake that balance?

Mr. ECKLES. That is a great question, Senator, because I think actually as bad as some of the big tech giants are, often it is the smaller players who are doing some of the most Wild West things with our data. So it is not that they should somehow be exempted from all of these considerations.

I would say one of the challenges with what we saw with GDPR was just how much ambiguity there was. So I would really hope that lawmakers would really be quite clear and precise in the laws or at least the policymaking that happens administratively.

Senator LEE. Statutory ambiguity tends to lead to regulatory complexity. Regulatory complexity itself further entrenches incumbents. It is a subsidy of sorts, a subsidy on the wealthy and well entrenched. I have got grave concerns about how tech companies can use their algorithms to harm users. Sometimes it is through censorship. Sometimes it is through recommending inappropriate content to children.

We actually see a lot of both of those things. But we shouldn't underestimate how Government solutions can often end up potentially making that situation worse. With that being said, transparency can be a good first step as a means to inform consumers. So in your view, what does transparency look like in the algorithm space and how can we balance that with the need to protect intellectual property?

Mr. ECKLES. Thanks, Senator. I think there is a lot of opportunities for transparency that wouldn't necessarily disclose a lot of the core intellectual property because so much of that is often in the context of making a specific prediction for a person, that this person is going to like this content, that they are going to watch this video for at least 30 seconds, right. But then what do you do with that prediction? How much do you weigh that in your decision-

making? That is more of a managerial decision, and that can be disclosed.

So you can say something broad about what are the inputs to this prediction, and you can disclose what is done with that prediction, even if the prediction itself is made by some deep neural network with billions of parameters involved. So I think that is one angle for transparency. The other one is that these companies are constantly doing randomized controlled trials to compare different algorithms internally, to weigh a lot of different metrics, some that are just engagement metrics, but some that are metrics of potential harm.

They could disclose more of the results from those. Actually I have relied in my testimony on the leaked Facebook files that covered one such A/B test that was conducted by Facebook comparing their status quo feed with a reverse chronological feed, which ended up making them more money. In fact, showing they weren't optimizing just for money making, but also had a bunch of other harms. Those kinds of comparisons are really useful, and so I would like to see a lot more openness about those in algorithmic impact and transparency reports.

Senator LEE. So the light could be an effective illuminator and disinfectant. I would like to conclude with one thought, algorithms and the use of machine learning technology are undoubtedly a necessary piece of technology to deal with, to deal specifically with the continued use of the Internet and the increased activity that we see on the internet. We also know this technology can be used for nefarious ends, and we certainly want to stop those activities.

I think we need to approach this challenge with humility, understanding that the Federal Government's intervention into these complex issues could and probably would do a lot of things to make the situation worse. Government regulation could end up hamstring companies' ability to innovate and evolve with emerging technology used by bad actors and empowering such bad actors to easily circumvent the technological standards adopted by Government, which would almost inevitably become outdated the moment they were enacted.

There are certainly worthy challenges, challenges that I think Congress has to consider and try to deal with in whatever way we can responsibly. But I can't emphasize enough to my colleagues that we should urge caution and we shouldn't be thinking that Government solutions don't have great potential to set us back even further in pursuing policy updates in our Internet laws. Thank you.

Senator LUJÁN. Thank you, Senator Lee. Senator Baldwin.

STATEMENT OF HON. TAMMY BALDWIN,
U.S. SENATOR FROM WISCONSIN

Senator BALDWIN. Thank you, Mr. Chairman. And thank you to our witnesses today. As you have heard, yesterday the Commerce Subcommittee on Consumer Protection held a hearing yesterday on protecting youth online, and our witness was the CEO of Instagram. I asked him about steps that the company was taking to combat harmful and problematic content relating to eating dis-

orders on their platform and urged him to invest more resources into human reviewers to help tackle that problem.

But as internal research from Meta shared with us by the whistleblower Frances Haugen has shown, it is Instagram's algorithms that can cause users to be drawn deeper into exposure to such harmful content. Ms. González, do you believe that we can truly get to the bottom of this particular problem relating to eating disorders or other problematic content like hate speech or vaccine disinformation or misinformation by simply pushing better moderation by platforms? Or do we really need to address how algorithms amplify and magnify and target that problematic content to users?

Ms. GONZÁLEZ. Thank you for the question, Senator Baldwin. You know, I think this is really tricky because of course, Congress needs to abide by the First Amendment, and so there is a limit to how deeply you can get into content.

However, what is really clear to me is that Congress has the ability and the responsibility to help the American people and help parents like me understand more about these problems by compelling transparency from the companies so we understand what is happening and how our children's personal and private data and their behavior is being tracked online and then used to target them with these kinds of messages, whether that is, you know, information about eating disorders or like in the case of my children, they are both big into gaming and watching other gamers talk about how they play the game.

And I have noticed even with them, they are very young, they get pushed on a path where suddenly they were watching just really mean content. And so I think it is critically important to compel transparency and to set some limits about how all of our private data can be used, but especially our children's private data.

Senator BALDWIN. Thank you. In 2016, in that Presidential election, my home State of Wisconsin was one of the top targets for Russian influence efforts through targeted advertising on Facebook. Since then, we have seen numerous efforts by foreign and now domestic actors to use Facebook and other social media platforms to spread divisive content and misinformation. We have heard time and time again from these companies that they are taking steps to stop their services from being used to undermine elections.

But I am concerned that we will keep facing this problem when we are also facing an erosion of public trust in our elections. Ms. Jackson, to what degree do you think Facebook's algorithms contribute to the spread and amplification of misinformation like that received by voters in Wisconsin in 2016? And do you think Facebook or other platforms have taken sufficient steps to address how they can be vectors for divisive and misleading content that can undermine our democracy?

Ms. JACKSON. Thank you, Senator. It is one of the most important questions we can focus on. And I think what it comes down to is the ability of actors, whether that is the Russian state, a terrorist organization, or well-intended but misinformed neighbor to manipulate or be manipulated by a platform without their knowledge is a threat to our democracy. And there are a few things going on there that we should focus on. One is, you know, my organiza-

tion was involved in something called the Election Integrity Partnership.

We worked with Stanford and the University of Washington closely with DHS, CISA, and frankly, the platforms on a narrowly targeted issue, 2020 in response to 2016, to figure out how we could better track what was going on. And we found decent success in that partnership, but we noted that the platforms themselves had very different content moderation policies, as well as extremely different transparency standards for how they communicated those policies outward. So one starting point is ensuring that there are in fact content moderation standards, and second, that those are public.

The second, though, is I don't think that self-regulation alone is sufficient, and it gets to the point that when the misinformation and disinformation that you were talking about in Wisconsin, that didn't just happen on Facebook, that is cross-platform. They used YouTube. They go into groups. They talk—they organize the actual events. And so what are we to say that, you know, is Facebook solely responsible or capable of addressing this problem, we would be missing a large piece of the puzzle. And returning again to the importance of data protection, privacy requirements, meaning that I would know, for instance, if the Russian State was attempting to buy ads, I was limiting the ability of the Russian State to target me on the basis of my predilections.

All of those things will provide better safety and a safer and more productive environment across the board digitally, will also prevent our adversaries from manipulating us and harming our democracy. So it is fundamentally important, and I can say it 12 more times, privacy, privacy, privacy.

Senator BALDWIN. Thank you.

Senator LUJÁN. Thank you, Senator. Senator Scott.

STATEMENT OF HON. RICK SCOTT,
U.S. SENATOR FROM FLORIDA

Senator SCOTT. Thank you, Chair. I think we can all agree the way big tech companies gather and manipulate and sell Americans' personal data, all without consequence, is alarming. These are the same companies that censor free speech, pick and choose which viewpoints are allowed on their platform, remove a United States President, but allow murderous foreign dictators on their platforms. For example, recent reporting has shown that Instagram's algorithms has recommended content to teens related to illegal drugs. Anybody with children or grandchildren that should be alarming.

We have to find a way to hold these companies accountable for failing to protect the rights and privacy of all Americans. I have introduced the DATA Act, which would require large online platforms with over 30 million daily users to obtain user expressed consent to collect their data and preference to use an algorithm and provide Americans the ability for a private right of action if they believe that their privacy is violated.

So my first question is for Mr. Poulos. I understand that these algorithms are designed to pull users back into the platform, pushing and prodding until the user engages again. It is not hard to see

how that could cause someone to develop an attachment to these platforms and feel they can't escape. Do you believe that this is how these platforms are functioning? If so, what does that mean for users, especially young people and young girls?

Mr. POULOS. Thank you, Senator. Human beings are imitative creatures above all. We are disputatious. We are jealous. We are envious. We are prideful. We are, in short, problematic. And social media gives human beings the ability to accelerate relationships and exchanges that involve, you know, all of the sins and foibles of human nature in a way that does, at its worst, create a kind of feedback loop.

And I think, you know, it is undeniable that when you look at the way that mental illness is increasing in America, especially among young people, the way that frankly just bizarre and even barbaric forms of self-modification are spreading, I mean there are now even groups on social media where young people are ceasing to identify as individuals altogether and now identify themselves as members of a swarm. In some ways, I think this is clearly an effort to imitate our digital entities themselves in an effort to fit in in this new world. So we need to recognize that the digital revolution is a sweeping and deep and profound, and it is not going away.

But that doesn't mean that we should either surrender ourselves to the rule of these entities or err in the opposite direction, which is to take an approach that thinks that the Federal Government can simply take control of the whole system and use it to really just take a side on the culture war and decide that Americans have to either get with the program or be systematically silenced or punished. And that is the power of a social credit system. You know, for all the flaws that social media has, speaking as a parent, you know, you can go on there and you can see all manner of memes and amateur commentary from young people who clearly understand what China is doing. There are plenty of memes out there about how you know John Cena's social credit score has gone to negative infinity because he said the wrong thing about China.

Ordinary Americans can't quite explain what is going on behind the scenes, but I think that they are aware that they are being forced in a direction that is incompatible with our way of life. And so as we look toward algorithms, as we look toward the social media ecosystem, what we need to do is find the areas where there is broad based, popular, and, within Government, support for specifying exactly what harm is. I think there is a lot of disagreement right now, regardless of identity. You know, you just look at polling that shows that, you know, Hispanics are split on whether Donald Trump should be elected President again.

You know, gay men—I mean, regardless of identity, there are deep seated cultural differences among Americans, and so there is not going to be an easy way to say, well, this is problematic, it should be suppressed. This is extremist, it should be suppressed. There isn't enough agreement. And so we have got to focus on really the most severe harms. Start there, build trust as a Government that the people are actually going to be able to preserve their human identity and their community identities online.

Senator SCOTT. Mr. Poulos, other than to make money, is there any reason for big tech to have these algorithms? Is there any user focused reason that these are important or are helpful to a user?

Mr. POULOS. Thank you, Senator. Yes, I mean, I would emphasize again that Stephen Wolfram was testifying on the Hill recently, and basically the point that he made was you can't have digital technology that interfaces of human beings without having in some way sort of algorithms that have a purpose and that direct people in one way or another based on what the technology is able to identify is their own preferences or leanings. And there is value at that. And consumers, who have clearly expressed a preference for being delivered ads that they are inclined to be interested in, rather than things that they are not inclined to be interested in.

I know that there is an appreciation for, you know, why can't we go back to the days when it was just a chronological feed of our friends posts? Well, you know, sometimes that ends up being a better user experience and sometimes it doesn't. So, you know, they are commonsensical reasons why the sort of algorithms have emerged in the way that they have. And I think that one source of frustration is sometimes we get in the habit of taking an outcome based measure of judgment, where "oh, it looks like something is happening to people that we associate with some kind of injustice, and so therefore, whatever was going on in the black box has to automatically be bad, and we need to punish—open the lid and just punish whatever is in there because we are focused on outcomes."

And I don't think that is right way to do it. I mean, you know, with all due respect to Senator Markey, I think his claim that, you know, young white men rule the Internet would fall flat among the many, you know, H–1B visa holders who are explicitly brought into this country and privileges as applicants so that they can build the technological infrastructure of online life.

Senator SCOTT. Thank you. Thank you, Chairman.

Senator LUJÁN. Thank you, Senator Scott. The Chair of the Full Committee, Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

The CHAIR. Thank you, Senator Luján. I want to thank you and Senator Thune for having this very important subcommittee hearing, and again a lot of my colleagues for good attendance, good questions, and good discussion by the witnesses, so thank you. Dr. Eckles, I think I want to start, though, you mentioned a little bit of this in your testimony, but algorithms are just software, right? I mean, we are talking about software here.

I feel sometimes like any technological advancement gets a little bit, you know, the Internet got critiqued, you know, for the things that it enabled, and drones get critiqued for the things they enable, but the underlying technology in general is something that we support. Me, I am most excited about every particle in a storm now can be an algorithm, and if you put the government dollars behind supercomputing, then you will have a really good weather forecasting system. So there are great applications.

The discussion we are having here today is how people misuse or what are the problems with those algorithms. And I think one of the things, you know, my colleague, Senator Thune and Schatz have been discussing this issue of 230. But when we first looked at content moderation, I don't think we really even thought that it was going to be automated. I don't think we were in that mode of this automation. And now we are—it is automated, and the algorithms have varied choices in them. In fact, they are editorializing. Is that not correct? They are making choices and editorializing about content?

Mr. ECKLES. Thanks, Senator. I don't know if I necessarily would describe it as editorializing, but I think fundamentally it is unavoidable that a lot of this has to be automated, right? If we want it to be cheap for so many of us to be able to share things with other people, we are not paying enough to have somebody on retainer to review all of our content, right.

Our clicks on ads are not making these companies enough money for there to be a person on a retainer to review all my content personally. So some of that automation is unavoidable. And I think it makes sense to have some scrutiny on where those lines are for what stays up and what gets taken down.

The CHAIR. But would you call that choice?

Mr. ECKLES. Yes, I think I think that is a choice, and I think there—one of the directions that I have seen this promising is having more choices there, so that it is not just leave up the content or take it down, but there is a larger repertoire of choices by the platform. So they can say, look, we, you know, this photo could be disturbing. We don't want to show it by default. But if you wanted to see it, you know your friend posted this content. Or ranking things, part of what they do through algorithms is to say, you know, this content is there, you can seek it out, we don't necessarily need to take it down, but we don't have to put it in front of you.

So actually, I think that a lot of algorithmic ranking and recommendation and some of the choices about what to show, how big, what to open up right in your face already, those are more subtle and really beneficial ways for them to make those choices. So it doesn't have to be about we banned this person entirely from the platform. Take down all their content.

The CHAIR. Well I think the question you have been discussing here for some time, or at least the gist of it I am getting is that again, when we looked at the 230 issue, an exemption, it was about you, you know, protecting people just for being publishers. But now with algorithms, you can be very precise, and you can have practices, as were discussed by either Ms. Jackson in her testimony or Ms. González, that are endangering either people's privacy or discriminatory, as some of my colleagues, or even promulgating hate.

So the question then becomes, what do you want to do about those individuals—because they have become far more than just a publisher. They really have increased their activities. And so I wanted to ask this question because Mr. Poulos, you brought up real harm. We had this discussion yesterday with Instagram about what happens when there is real harm. I guess actually, this is for all the witnesses, because your testimonies are talking about what

to do about these if there is real harm. I think Ms. González and Ms. Jackson are saying that we should have legislation and that has been loud and clear. But I wanted to hear whether you thought Mr. Poulos that real harm should be more than binding arbitration with Facebook or Instagram.

Mr. POULOS. Thanks, Senator. In the abstract, you know, I think I mean, I am one of these people who thinks that binding arbitration is usually not the right way to resolve legal disputes. So I am inclined to say that, you know, if Congress wants to ensure that there is a more active legal process, that is in their remit to do so. You know, my concern is more along the lines of trying to split hairs and pick and choose as a deliberative body over what gets to count as harm is going to be difficult on the internet. And it is——

The CHAIR. But you think real harm, as some of the witnesses that we have had here for or my colleagues yesterday and their hearing, I know it is interesting our two committees, subcommittees, but you know, my other two colleagues who have been doing a fine job, Senator Blumenthal and Senator Blackburn, have been showing the harm to kids. So in that case, would you agree that some of those cases are real harm?

Mr. POULOS. Thanks, Senator. I mean, rather than there being a sort of epistemological, unsolvable question about whether people are suffering, I think what you would probably find in most cases is that once these things go to court, it would be difficult, either too difficult on the one hand to meet legal standards of connecting those dots.

Or on the other hand, it would push judges and juries too hard in the direction that, you know, oftentimes happens in our litigious society, where a plaintiff just shows up and says, you know something bad happened to me, now give me $20 million. You can have sort of, you know, you kind of perversions of the legal system, I think, in either direction. You know, that said, you know, arbitration is not the be all and end all, either.

The CHAIR. OK, Ms. Jackson, Ms. González, do you want to comment on that? The need to show—to do more on real harm.

Ms. GONZÁLEZ. Senator, yes, I would agree we need to do more on real harm. You know, in the context of 230, one of the things that we have been thinking about at Free Press Action is how the intent of that statute has been overread by the courts. And so clarity around platform accountability when they themselves, the platform itself, either by design or negligently is causing harm, ought to be reviewable by courts. So that is kind of where we stand on the Section 230 issue.

And then of course, we have long standing laws, civil rights, privacy, etc., norms and principles that ought to apply online as well. The harms here are really concrete. I don't think it is out of the regular order of the Congress or, you know, especially an expert agency like the Federal Trade Commission to look at the facts before them and to promulgate rules that apply across the industry and to take enforcement action when companies violate those rules.

The CHAIR. Thank you. I do see my time is over, but Ms. Jackson, did you want to add something really quickly?

Ms. JACKSON. Yes, just to double down there. There is criminal content online that we are talking about, and so over focusing on

whether or not there are harms or distract from the fact that real people are being hurt and everyone else in the world is making decisions about this about us.

And so I think it is really important, we can have debates about which legislation, or which approaches or what we do, but the United States not acting is ceding one of the most consequential decisions of our time to literally every other country, including China, and having that be the law of the land eventually for our own citizens. And so just really encouraging that we take action. Thank you.

The CHAIR. Thank you, Mr. Chairman.

Senator LUJÁN. Thank you, Chair Cantwell. Senator Peters.

STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN

Senator PETERS. Well, thank you, Mr. Chairman. Dr. Eckles, I chaired a Senate Homeland Security and Governmental Affairs Committee, and our committee has been focusing on the rise of domestic terrorism in our country. And as part of the efforts that we have been undergoing, we are looking at social media companies, their practices, their politics, and how that can feed into extremist content being provided to individuals.

So my question to you is, in your expert opinion, what are the tradeoffs that these social media companies are making during their decisionmaking progress, process when they weigh profit motives verses user satisfaction? Walk me through a little bit about what is going on behind the scenes there.

Mr. ECKLES. Sorry, Senator, was that a question for me?

Senator PETERS. Yes.

Mr. ECKLES. Yes. I think that is a great question because they are weighing a lot of different considerations. And one of the things that actually Adam Mosseri brought up yesterday was the notion of the long term versus the short term. And so I think this is one of the things that as platforms get more sophisticated, they hopefully start to consider more and that can improve some of their decisions, which is that they think more about the long term, right. You might be able to show something different to somebody today and make a little bit more money, but how are they going to feel about this tomorrow?

How are they going to feel about the time they spent on your platform? Are they still going to be around in a month if a new competitor enters? Won't they want to switch to this other platform? So I think the platforms are in some cases getting more sophisticated about thinking about the long run and including measures of consumer welfare and time well spent. And so I think the industry really pushing other companies to do more of this could be quite beneficial.

So those are tradeoffs that they are making, and I would like to see you all in this subcommittee and other policymakers provide more scrutiny on what those tradeoffs are, like what actually are the weights that they are giving to some of these different outcomes that they care about? How much weight do they put on revenue versus how much weight they put on consumer surveys?

Senator PETERS. Yes. Very good. Well, thank you, doctor. I have another question for you. In your written testimony, you state that platforms work to predict what content a user is going to engage in, and clearly that is the basis behind algorithms and machine learning. But could you just describe any role that psychologists and behavioral scientists may have at these companies and in predicting potential behavior from folks and how to model accordingly?

Mr. ECKLES. I think a lot of these companies now have behavioral and social scientists from all disciplines involved in this process. And in some ways that could make us a little worried. On the other hand, I think actually that can be quite beneficial. So it is psychologists and behavioral economists at Facebook who helped to pioneer there the focus on actually asking people questions about, hey, was this content you just saw, was that important, was that interesting, did it make you feel connected, right?

This idea that sometimes what we want in the moment and what we want on reflection can be different. That is an idea that has a lot of grounding in research and psychology and behavioral economics and could help platforms actually focus on giving people what they really want on consideration, not just what say their lizard brain wants in the moment. So I think these companies are, at least the giants, are employing lots of social scientists, lots of psychologists.

And I think from what we have seen in some of the internal conversations that have been leaked from, say, Facebook, a lot of times they are advocating actually for consumer well-being. So it sort of depends on some of the top level decisionmaking, whether those choices get put into practice.

Senator PETERS. And one final question there for you, doctor. You mentioned in your testimony that WhatsApp can also be dangerous despite not having an algorithm. Could you talk to us about your study that looked into how WhatsApp users manipulated the trending topics feature on WhatsApp in favor of BJT and India, please?

Mr. ECKLES. Yes, definitely. So I think, you know, qualitatively, we look at some of these cases like genocide in Myanmar, and it is easy to sort of connect that with algorithmic ranking and recommendation. But then we also see violence that sort of directly facilitated or caused by activities on platforms without ranking like WhatsApp. And so I think we have to remember that some of the fundamental things about social media are that it lowers costs for people to share content with lots of people and to propagate it really quickly, right, whether there is some algorithmic ranking or not.

And a lot of times, if the algorithms are really transparent, people learn how to game them. So we had a whole bunch of phones in India that we are joining all the public political groups we could find on WhatsApp and tracking what the conversation was happening there. I think in many ways we knew more of what was happening than Facebook did because those conversations are all encrypted unless somebody lets you join that group. We were able to see then these groups coordinate their activity on Twitter so as to manipulate the trending topics there.

And that kind of cross-platform coordination happens all the time. And I think that is something that Ms. Jackson has really

been highlighting. And so we have to definitely look across those platforms, give platforms clarity that they can do so without risk of anticompetitive concerns if they are doing it at least within a particular context of preventing these kind of cross-platform manipulations.

Senator PETERS. Well, thank you, Dr. Eckles. And thank you, Mr. Chairman, for holding this hearing.

Senator LUJÁN. Thanks, Senator Peters. Senator Rosen.

STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA

Senator ROSEN. Well, thank you Chairman Luján, and of course, Ranking Member Thune. This is a really important hearing, and I appreciate all the witnesses being here today, I want to build upon what some of my colleagues have been talking about but taking a little bit different direction, deplatformization. And so many mainstream social media platforms have been publicly taking action against hate speech. They are removing it from their sites, they are removing it and banning account holders. In some cases, a fully de-platform users from chat communities and social media sites.

While significantly more needs to be done, I appreciate the actions these platforms are taking to tackle racism, antisemitism, and other forms of white supremacy rhetoric and hateful conspiracy theories that far too often lead to violence. But when dealing with fringe platforms, there have been efforts to remove platforms altogether from their hosting sites, their app stores, cloud hosting services, instead of removing the hateful content or user. Total deplatformization strategies deny such fringe sites and apps access to platform infrastructure from which to perpetuate hate speech.

This could include suspending the use of payment systems such as PayPal or Cash App or completely removing companies of browsers and domain name system. So Ms. González, is deplatformization of fringe sites that support hate speech, do you think this is an effective strategy and how easy or difficult is it for a platform that is posting extreme, radical, or violent content to find a new hosting or payment service if kicked off a mainstream company? And should these host sites and payment services, what is your responsibility in this mix?

Ms. GONZÁLEZ. Thank you for the question, Senator. An advocacy that is not focused on request to the U.S. Government, I actually support deplatformization and I support it because for two main reasons. One, I think that the companies themselves do have First Amendment rights to set the standards upon which people have to behave on their site or on their platforms. And if there is a platform that is just repeatedly violating the standards of, say, the App Store, then I think it is within the app stores rights to remove them.

The other consideration that brings me to this position is that even if these platforms or entities are kicked off of these—or deplatformed, they can build their own sites, they can build their own payment systems. And this is why at Free Press Action we do support net neutrality. We don't think that Internet service pro-

viders that provide access to the Internet should be making choices about who gets to build a website or who gets to run over the internet.

So I think that is an important distinction here as we kind of balance First Amendment issues with the desire to hold companies accountable for proliferating hate and extremism.

Senator ROSEN. Thank you. I would like to move on to talk about another thing everyone has been talking about, the algorithms. And we all know how they are built to engage with the user, they are built to direct the user's attention toward advertising or something else. They are just really going to take you further in. If you like red sweaters, you are going to get a whole slew of red sweaters once you start looking for one of them. But this involves amplifying content far too often incendiary in nature, which in turn optimizes engagement. So I know I am not going to have time for the entire panel so we can begin with Ms. González and then Dr. Eckles.

What can Congress do to incentivize or discourage companies from using these persuasive technologies that manipulate or harm users? And I also want to know what you think about giving the user control over, if I am shopping for red sweater for a friend, and then I don't want to see any more red sweaters, how can I stop that—where do I have a choice? And so what can we do about that? So Ms. González and Dr. Eckles. I know I am running close to my time.

Ms. GONZÁLEZ. Thanks, Senator Rosen. I will try to be brief. Even though I am all for red sweaters, so keep serving those ads.

Senator ROSEN. For holiday season, red sweaters——

Ms. GONZÁLEZ. It is very beneficial, in my view. But I think this is where having a comprehensive approach to privacy is critically important. We should understand what companies are collecting about us and have rights to, you know, compel them to remove data that we don't want them to be tracking about us.

And so we need to have those rights in the users' hands, and we need a great deal more transparency about what they know about us and how they are using that information. I think too, a lot of companies know, as the Facebook papers have revealed, that they are causing harm. So we need to have some disclosure when companies become aware that their algorithms are driving harm and abuse.

Senator ROSEN. I know that I am over my time, so I guess I could—I will ask the rest of the panel. We will submit this for the record, but I really want to know what people think about allowing the end user to opt-out of getting any more recommendations on a particular topic or subject or even a red sweater, if you will? Thank you, Mr. Chairman. I appreciate this hearing.

STATEMENT OF HON. RICHARD BLUMENTHAL, U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thank you, Senator Rosen. My name is Richard Blumenthal. I am a Senator from Connecticut. I am taking over for Senator Luján who is voting right now, and I have a strong interest in this area. As a matter of fact, just coincidentally as Chairman of this Subcommittee on Consumer Protection, yester-

day, we had a hearing with the CEO of Instagram, as you may know.

We got from him, I think he used the word "directionally," support for access of researchers to these algorithms, which are the black boxes that drive destructive content to kids on platforms like Instagram and others. TikTok, Snap, YouTube all committed to making datasets about their effect on children and teens available to independent researchers when they came to testify. So this idea of access by researchers is tremendously important so that parents and all of us understand how they work, and what they do, and what can be done to stop the destructive content.

And I think that is one of the main values of this hearing. I was very interested, Ms. González, in your comments, page 10 of your testimony, where you say and I am quoting, "we must also set out explicit protections for external researcher access to platformed data to guard against what is now a documented pattern of targeted efforts by platforms to deny external researchers the opportunity to investigate platform practices." I think that comment is tremendously revealing. After I have sat here and I have heard Antigone Davis of Facebook, Adam Mosseri of Instagram, a representative from Snapchat, TikTok, YouTube, all say, we support research.

But its research of our choosing, people of our choosing to do the research. And footnote 19, Ms. González, I think documents the denial of access to independent, objective researchers that could uncover more of the truth for parents and others who really deserve it. And I know that you cite the example of Laura Edelson of NYU who was, in effect, stifled in her research. And so my questions relate to the efforts we should do legally, what legal protections should be afforded to academic researchers against efforts to silence them or stifle their research? Let me ask all of you to comment.

Specifically, why voluntary efforts from the platforms are inadequate and why we need these requirements for access rather than self-policing or internal research? And maybe Ms. González, I can begin with you, since you explicitly called attention to this issue in your testimony.

Ms. GONZÁLEZ. Thank you, Senator Blumenthal. You know, through my work and various coalitions, the Change the Terms Coalition, as well as the Real Facebook Oversight Board, I worked with a number of researchers. So in addition to Laura Edelson story, I have heard time and again researchers being granted access to data and then having their access denied when the research starts to get real in terms of holding the companies accountable. So unfortunately, I wish we weren't in this place, but I think we are, and the Facebook papers certainly have revealed that we cannot rely on companies to give access to their data without some mandates.

So unfortunately, that is the place we are in, and we have to develop some safeguards, protections, and expectations about access to data by third party researchers. Otherwise, we are just going to continue to not understand how these systems work or it is just, you know, Facebook for it is such a good example because now we

know just how much they knew about how their systems were harming people and that they failed to disclose it.

It took a whistleblower, Frances Haugen and many other whistleblowers, Yael Eisenstadt. The list goes on and on to really unveil just how harmful these practices were. Last year—and then I'll also stop, I promise. Last year, the *Wall Street Journal* exposé that found that Facebook knew that 64 percent of people who go to extremist groups on their site find those groups because of its own recommendation system, that was a blockbuster revelation, and Facebook had known that for years and failed to disclose. We just can't rely on them to be forthcoming.

Senator BLUMENTHAL. Thank you. That is really powerful, Ms. González, and perhaps in writing, you can elaborate on some of those points, but they are very, very pertinent and important. Ms. Jackson or any of the other witnesses, if you—go ahead.

Ms. JACKSON. Thank you, Senator. Yes, my organization, the Digital Forensic Research Lab is one of those independent research groups. And so we pay very close attention to this question and share the belief that this is extremely important and in fact, that there is a role for Congress to play and requiring certain levels of transparency and disclosure. I would also urge us to be very intentional about what it is we are asking for. I know we talk a lot about Facebook, and part of the reason for that is we actually have more information on Facebook than almost any of the other platforms.

We will give Twitter a little credit and that they provide better data access probably than the rest. But we are not talking about YouTube. We are not talking about Google. We are not talking about Reddit. And there is a reason for that. And that, to me, underscores the importance of having those standards because one of the risks in research is that you chase the thing you have, which both leads us to not look at the kind of overarching aspects of platforms that cause some of these problems.

I am encouraged that we are talking about algorithms today, which is an improvement from a conversation a year ago where we were only focusing on content. But there are many more examples of exactly that, how platforms operate, how they operate between each other that we need to have a sense for. And to get to that, we need to have intentional transparency, standards across the board for companies to provide certain information, and also have clarity about what we want from that transparency at the end of the day, so we are not chasing unending rabbit holes of specific pieces of problems.

Senator BLUMENTHAL. Thank you. Thank you very much. Mr. Poulos.

Mr. POULOS. Thank you, Senator. I think it is self-evident that the platforms that want to choose their own researchers so that they can produce a relatively favorable information in the same way that you know a legislative body or even an independent researcher would want to tend to arrive at the conclusions that they think are the most important to reach. So I think to a degree, you know, if you are looking to go toe to toe with the platforms, with dueling researchers, it is going to have to be a somewhat disputatious process.

This is a turf battle in some respects, and if Congress wants to mix it up, then they are going to have to mix it up. I would caution, you know, that in addition to, you know, chasing after what you already have, I think there is the danger in research of chasing after what you want to find.

And that there are those who outside of Silicon Valley and outside of social media, really want the social media space and the Internet more generally to become a place where really predictive policing governs the space, so that, you know, you can say, well, we need to make sure that three steps in the decisionmaking tree before someone commits an act of extremism, that they aren't exposed to information that might lead them to that point. And you can chase down that rabbit hole quite far.

And I think there is a real danger that at least some outside researchers would want to push social media through regulation, if not legislation, right, toward really doing using algorithms to conduct a kind of predictive policing. Where, you know, I mean, just to grab something out of the hat. You know, if going to a certain kind of political rally or expressing a certain kind of political opinion is officially deemed an extremist act, well, then you can, you know, you can find how far backward in time on social media do you really want to go still pinning responsibility on a person.

You know, while they were exposed to this piece of information or this opinion Op-Ed or, you know, to this kind of meme, and so we need to stop those things because, you know, they have some inclination to lead people in an extremist direction. I think that stuff can be very dangerous, very suppressive, chilling of free speech, free expression, online and off. And so that is, you know, that is the warning that I would counsel.

Senator BLUMENTHAL. Mr. Eckles.

Mr. ECKLES. Thank you, Senator. I think allowing external researchers, whether they are academics or journalists or Congressional staffers, to do research, whether they are probing the systems from outside, you know, creating their own accounts and scraping data that is really valuable. And sometimes there has been legal uncertainty about the state of that. Some recent case law, my understanding, suggests that researchers can do a bunch of things there, but that may be a point where Congress can help.

Another way that researchers can be helped is with actual access to proprietary data. And I have been in the position of having that access previously working as a scientist at Facebook, and I have data use agreements with multiple companies that allow me to do that kind of research. But as you say, there can be some limitations on the topics that you might be able to undertake. And so I think that means that the public gets potentially a skewed view of things. Now there have been some efforts like social science one with Facebook to release some privacy preserving data to a larger set of researchers without any publication approval from the firm.

And I think that is a really promising direction. That actually used some of the same technology, differential privacy that is being now used by the U.S. Census Bureau for the decennial census and for more of their data products. That does raise some challenges that can reduce some of the data quality in some ways. But I think that is a really promising direction, and I would hope as well that

privacy regulation would make it very clear that platforms can share data of that kind with external researchers if they use those techniques to protect the privacy of people involved.

There has been a lot of uncertainty about that. As soon as Facebook announced that they were going to share that data in that way, activists said, we are going to sue you in European jurisdictions. So having that clarity could really help spur that along. Thank you, Senator.

Senator BLUMENTHAL. Thank you all. I think this area is very, very important. You know, the Surgeon General on Tuesday asked for more data sharing from social media platforms in an advisory. So now we now have public health professionals calling for researchers to have access so they can hold big tech accountable. A couple of you mentioned the Digital Services Act, which is a proposed European law that would impose this kind of access as an obligation.

And I think that we can learn from Europe and others, but we don't need to wait for them to act. I think we should act because we need to protect the public, and for all the reasons that you mentioned. And ultimately it actually is good for social media to have more competition, more transparency. You know, the Internet initially was designed to be a lot more open than it has become. Of course, we can learn from history. So thank you all for being here.

Senator LUJÁN. Thank you, Senator. And before we close, just some follow-up questions to the panelists. Professor, following up on your conversation with Senator Fischer, could you define A/B testing for the Committee?

Mr. ECKLES. Thanks, Senator. An A/B test is just one form of a randomized trial or randomized controlled trial where people are randomly assigned to different variations on a service. And so in the context of algorithmic ranking, it might be that some people are randomly assigned to one status quo ranking algorithm and other people are randomly assigned to see content according to some new algorithm. This is one of the key tools that these companies use to make decisions about these algorithms to balance all the different metrics that they are tracking. They are running hundreds, thousands of these kinds of experiments a year.

I think we know as of 2016, Google was running 10,000 A/B tests a year. Just as they are in medicine, these are the gold standard for causal inference, for learning about cause and effect relationships of if we change things in this way, what are the consequences? And so while they can potentially be used to do things like fine tune, some dark pattern, deceptive practice, they also are one of the main tools that platforms also have to make educated and good decisions. So I think, you know, in my own testimony, I relied on some A/B tests that I had run and published when I was a scientist at Facebook. Some that were leaked as part of the Facebook files.

One that was published by Twitter that actually didn't look, according to their own conclusions, didn't look so favorable to them, but they chose to actually publish that. So I think we would very much like to see as a research community and as the public, the highest quality evidence available, and that comes from these randomized trials or A/B tests.

Senator LUJÁN. Now with that being said, what policies would you suggest that would better incentivize A/B testing for consumer harms rather than exclusively for engagement and revenue?

Mr. ECKLES. I think that is a great a great question. I can't say that I know the answer there. I think hopefully there are some lessons that budding entrepreneurs are learning now as well that some of these early decisions that platforms made that were short sighted have permanently hurt their brands and are hurting their ability to launch new products. Think about Meta as they are trying to move into all these metaverse offerings.

The Facebook reputation is coming with them, and it may prevent some of their ability to succeed in that area. When it is time to move to a new setting where they don't have the network effects they have in an established social media space, will people want to use their service? So these matters of long term reputation and consumer attitudes can be one lever, but I don't know the full answer there, Senator.

Senator LUJÁN. Appreciate that. Just for clarification, GDPR is the European General Data Protection Regulation, correct?

Mr. ECKLES. Yes, Senator.

Senator LUJÁN. Ms. Jackson, following up on Senator Blackburn's question regarding corporate power over user data internationally, what should the U.S. Government do to better protect personal information and behavioral data from foreign actors seeking a strategic advantage?

Ms. JACKSON. Thank you, Senator, for that extremely important question. I think the lack of our data privacy means that literally anyone, whether that is the Chinese State collecting information, a terrorist organization, an intelligence agency, or just a marketer can gain access to our information and then deploy that into the system that we have all described today to achieve whatever objective it is. And I think there's no question that that is bad for American national security, that that is bad for American competition in the world, and it is bad for American democracy.

What I think we sometimes miss is that we are having this conversation on an island, and all around the world, we mentioned GDPR, the data protection rules in Europe, almost every country in the world has some data protection laws, including even China. The difference is that China has data protection law for commercial entities and not for itself. And so while in the United States, we paid decently close attention to questions about limiting the Government's ability to surveil us, we have completely left out the commercial picture. But that is a giant backdoor for whoever wants to influence us.

So I appreciate that question and just return to as the rest of the world is making these decisions, it is of extreme urgency that the United States begin to make its own decisions about how we protect our own citizens, our own data, and our own democracy so that we don't leave it up to the Chinas of the world to make those decisions for us.

Senator LUJÁN. And you anticipated my next question, which is what are the consequences for the United States not taking a leadership role in privacy and algorithmic regulation? I think you touched on that very clearly. My concern is everyone around the

world and especially the Europeans, are defining this. And here in the United States, we are going to be defined by what other countries are doing with establishing these rules. And it just it seems like a terrible mistake for the United States not to be engaging more. Ms. Jackson.

Ms. JACKSON. Absolutely. If I can add a point that. I think one thing that often gets missed is that I can't remember which Senator alluded to earlier, the kind of strength of the Internet is the fact that it was open, interoperable. It's this public thing that is not just in the United States, it is every country around the world. And so to think that we can have, you know, 100 different versions of the Internet and have it be the thing that we want and have the rights that we expect offline transferred to the online world, we are in for a treat.

And so part of this is that, you know, China is advancing a very intentional model, and that intentional model depends on every other country being divided in its approach because the splinternet, as some people have called it, is the goal so that China can do whatever it wants in its own territories. You have mentioned the social credit system. China is the author of a system in which people exist online, and the data collection that we are talking about here in the U.S. is used for the purposes of the State being able to institute its political control.

That is an actual authoritarian state. In the United States, we have a very different model and set of intentions, and so it is extremely important that we don't seed that dispersal. So it is not just that we are absent, it is that our lack of leadership means that China having a clear vision, bringing the next billions of people in the world online for the first time into their system really ends up impacting the ability of democracies to have a democratic online space.

Senator LUJÁN. I appreciate that. Ms. González, the last question I have for today. All Americans, regardless of the language they speak at home, deserve access to services with online platforms and all that they provide. They deserve the same access to stay connected to their friends and to loved ones. They also deserve access to the critical information available through online platforms, which is why the spread of online amplification of non-English and a particular Spanish language misinformation is deeply troubling.

I repeatedly called for online platforms like YouTube and Twitter, Facebook and others to publish more information broken down by language so we can begin to understand the scope of the problem. Now, Ms. González, what other commitments should online platforms make to stop the amplification of non-English language misinformation and disinformation on their platform?

Ms. GONZÁLEZ. Thanks for the question, Senator. I think, you know, this is near and dear to my heart that I have been working on this for a while now. I think one thing that really struck me in the Facebook paper revelations was that Facebook has seriously underinvested in Spanish and other non-English languages when it comes to how it shores up its integrity system. One of the things that really shocked me in the response or kind of lack of response that you got from the tech companies was that they failed almost

across the board to answer really basic questions about how they keep their users safe in languages other than English.

So they weren't willing to answer simple questions like who is in charge of non-English moderation in language x, how many moderators do they have? We know that human moderators are a critically important part of the content moderation system, right. One of the things that the Facebook papers reveal is that to really get at, you know, beyond capturing 20 percent of hate speech, for instance, just take an example, that AI alone wasn't going to catch that, and that Facebook needs to significantly step up.

It is very clear that there is this disparity in how Facebook, YouTube, WhatsApp, and other platforms are forcing their own content moderation rules across language. And that needs to stop. I think users, no matter what language they speak, ought to have the same protections across the board.

Senator LUJÁN. And what seems more clear to me, Ms. González, is I have gotten more involved in this space is the disaggregated data is collected. I mean, the AI is built to tell the difference, but no one wants to release it. Even to the point that the letter that was responded to my inquiry from Facebook, it came to me unsigned.

Everything is OK, we collect this information. I just wonder if a bot even produced that letter before it came to me. You know, some algorithm or some AI just said, OK, here is this question, spit out the response, and then, you know, we will just send it to him unsigned, so he doesn't ask any questions of who needs to be held accountable for the content of that. Anyhow, that is the subject for another hearing down the road. With that being said—yes, Ms. González.

Ms. GONZÁLEZ. If I may, I mean, one thing that came out in the *L.A. Times* piece, written by Brian Contreras a couple weeks ago was really upsetting to me. We would been meeting with Facebook, calling their attention to this problem, and you know ahead of the 2020 election, we said there is a gap. And they were like, ha, maybe there is a gap. Well come to find out, they knew about that gap in February 2020 and decided not to invest to close the gap. So this is why I am on such—I am so much for calling for greater transparency because they know that there is a problem, and they just don't do anything about it and don't let anyone know that it is happening.

Senator LUJÁN. And Ms. González, in this area, I also fear that because of lack of action in the United States, in the United States we are going to have to be dependent on leaders in other parts of the world to establish the rules that we are hoping that will be created here with every one of us. And like many of my colleagues, I am hopeful that we will see a markup of legislation, and there are many bipartisan pieces that are good ideas, whether this is expansive or more narrow. But it is clear that action needs to be taken. And so I am hopeful and prayerful that that will happen.

Now, as we close this hearing, the hearing record will remain open for two weeks until December 23. Any Senators that would like to submit questions for the record for the witnesses should do so by that date. We also ask that your responses be returned to the

Committee by January 6, 2021—sorry, 2022. Now that concludes today's hearing. Thank you very much, everybody.

[Whereupon, at 1:13 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF IMRAN AHMED, FOUNDER AND CEO,
CENTER FOR COUNTERING DIGITAL HATE

Thank you for inviting the Center for Countering Digital Hate to submit written testimony for this critical hearing and thank you to the Committee for calling attention to this important topic.

In our core mission to expose and disrupt the architecture of digital hate and misinformation and to hold to account the perpetrators and platforms that profit from its spread, we have extensively studied the use of social media by malignant actors and movements. In the last year, CCDH's work has studied and exposed anti-vaccine and Covid-19 misinformation, racist abuse, violent misogyny, and climate denial on mainstream social media platforms. CCDH has shown that social media companies, namely Facebook, Twitter, YouTube, Google, and their subsidiaries, have systematically failed to act on hate, misinformation, and dangerous content circulating on their platforms.

Algorithms, specifically the complicated and layered algorithms used by social media platforms, boil down to human choices made by individuals at companies that are driven by profit. Big Tech executives decide which content wins and loses in the battle for attention on their platforms, allowing them to shape awareness and knowledge for billions of people. Their algorithms are designed to drive engagement, eyeballs, and therefore ad revenue. Engagement is maximized by:

- Emotional triggers—to enrage is to engage, and vice versa
- Conspiracy theories, based on disinformation, that lead to a warren of conspiracist rabbit holes
- Contentious misinformation that gets engagement from detractors and supporters

Malgorithm, CCDH's report on the Instagram algorithm and its recommendation systems, was the piece of research that earned our organization the most pushback from technology companies.[1] We know this resistance was due to the verity of our study. In August 2020, Facebook, which owns Instagram, implemented a new algorithm that provided "Suggested Posts" when users reached the end of their feeds.[2] This feature would use machine learning algorithms to identify the potential interests of a user based on their data and habits, and then would include "Suggested Posts" into users' feeds.[3]

Using a very simple research methodology that traces user experience with recommendation algorithms, CCDH researchers set up new, anonymous accounts on Instagram and followed a series of accounts ranging from health and wellness to known anti-vaccine influencers. Researchers reviewed recommendations generated from Instagram's "Explore" and "Suggested Posts" features. More than half of the recommendations in this study contained Covid-19 misinformation. Users following wellness accounts were algorithmically recommended anti-vaccine misinformation and conspiracies about Covid-19. Users following QAnon accounts were recommended Covid-19 misinformation, misinformation related to the 2020 United States election, and QAnon conspiracy theories. Those following anti-vaccine accounts received recommendations for antisemitic content. In short, Facebook chose to launch a revenue-maximizing algorithm that promoted harmful misinformation during a deadly pandemic and an election season where conspiracies ran rampant and that culminated with a deadly attack on the U.S. Capitol, plotted and pre-publicized almost entirely online.

---

[1] Malgorithm, Center for Countering Digital Hate, *https://www.counterhate.com/malgorithm*

[2] CNN, 19 August 2020, *https://edition.cnn.com/2020/08/19/tech/instagram-suggested-posts/index.html*

[3] Powered by AI: Instagram's Explore recommender system, Meta, 25 November 2019, *https://ai.facebook.com/blog/powered-by-ai-instagrams-explore-recommender-system/*

In fact, Facebook's internal research, revealed by whistleblower Frances Haugen, align with our findings in Malgorithm. Facebook conducted a test with a very similar methodology that yielded very similar results. Within two days of a fresh account being set up, Facebook found that recommendations containing QAnon and other conspiracist extremism were fed through the algorithm to the new user's feed.[4]

In 2021, CCDH released a report showing that a dozen individuals were responsible for 65 percent of the vaccine disinformation on Facebook, Instagram, Twitter and YouTube.[5] Mark Zuckerberg was in fact asked about the report by members of Congress. He said he would look into it. A month later, our researchers found that the Disinformation Dozen had continued to operate with complete impunity on his platforms. Six months later, after the Surgeon General and the President of the United States all cited that report, Facebook executives attacked our research claiming that it was based on a "faulty narrative."

We now also know from documents disclosed by Facebook whistleblower Frances Haugen that on the very same day CCDH released the Disinformation Dozen report, Facebook had produced internal research that largely confirmed our findings that indeed a very small group was responsible for more than half of the vaccine disinformation on the platform. When confronted by us and later by Congress, Mark Zuckerberg, denied, deflected, and his company continues to delay action to stop these individuals.

Meanwhile, hospitals throughout the country are packed with unvaccinated COVID–19 patients desperately trying to take breaths, telling their doctors they would have taken the vaccine but for content spread by the Disinformation Dozen, most of whom are still allowed to disseminate vaccine lies on Facebook. Many of those patients will not live to see another day. At the same time, Big Tech sits atop a fortune accrued faster than almost any in human history.

It is now well documented by the work of whistleblowers, researchers, watchdog groups, and even scores of employees working within these technology companies that there is a fundamental problem with business models that prioritize profit and engagement over safety and security. Researchers have found algorithmic biases in race, gender, sexuality, and myriad other factors, particularly those affecting protected groups[6] [7] Further, researchers have found that misinformation receives more engagement than real news on Facebook products.[8] There is a clear danger to products that sell data in order to maximize engagement and profit, and there is an immeasurably higher cost associated with the damages of misinformation and malignant content's ability to spread unfettered across unregulated platforms.

Conclusion

The ways that algorithms organize, categorize, and predict behavior based on data gathering and human decision making absolutely require oversight, transparency, and accountability. Solutions should not only focus on the outputs of these algorithms, what sort of content is amplified by algorithms and its circulation volume, but also whether there are proper safety mechanisms in place to pump the breaks when dangerous content is being spread rapidly. Slowing down the circulation of malignant content and prioritising and auditing safety mechanisms must be central to our approach to dangerous algorithms.

In light of Facebook and tech companies' attempts to stifle independent research and discredit whistleblowers, Congress must commit to protections for whistleblowers as well as an agenda that prioritizes transparency while respecting privacy and data privacy. oversight bodies, including but not limited to the Federal Trade Commission (FTC) and consumer protection agencies, must be involved in the oversight of these publicly traded and gravely opaque companies. Transparency of algorithm outputs, audits of algorithm safety, and audits of platforms' ability to mod-

---

[4] Insider, 25 October 2021, *https://www.businessinsider.com/facebook-papers-leak-qanon-carol-smith-research-2021-10?r=US&IR=T*

[5] The Disinformation Dozen, CCDH *https://www.counterhate.com/disinformationdozen*

[6] "FACEBOOK'S AD ALGORITHM IS A RACE AND GENDER STEREOTYPING MACHINE, NEW STUDY SUGGESTS" The Intercept, 4 April 2019, *https://theintercept.com/2019/04/03/facebook-ad-algorithm-race-gender/;* Imana, Korolava, and Heidemann, "Auditing for Discrimination in Algorithms Delivering Job Ads" University of Southern California, *https://ant.isi.edu/datasets/addelivery/Discrimination-Job-Ad-Delivery.pdf*

[7] Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms Brookings Institute Nicol Turner Lee, Paul Resnick, and Genie Barton May 22 2019 2019 *https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/#footnote-6*

[8] New Study Shows that Misinformation Sees Significantly More Engagement than Real News on Facebook, Social Media Today, 22 May 2019, *https://www.socialmediatoday.com/news/new-study-shows-that-misinformation-sees-significantly-more-engagement-than/555286/*

erate hate, illegal content, and apply their terms of service must be part of oversight and legislative considerations.

The revelations of the past year have proved yet again what CCDH has researched and exposed, that social media platforms are woefully incapable of self-regulation. And the time to act is now.

The task ahead of us is to generate solutions that balance economic prosperity of the Nation with protection of citizens' privacy as well as protection from serious harm. There is no silver bullet to solve the problems created by Big Tech. But it is now more than ever an urgent task. For far too long hate and misinformation have been propagated for profit and caused massive and in some cases irreparable harm. Congress must act collectively, urgently, and with a multi-pronged approach to protect children, families, our society and democracy.

December 9, 2021

Senator Ben Ray Lujan, Chair
Senator John Thune, Ranking Member
U.S Senate Committee on Commerce, Science, and Transportation
Subcommittee on Communications, Media, and Broadband

Re: Hearing on "Disrupting Dangerous Algorithms: Addressing the Harms of Persuasive Technology"

Dear Chairman Lujan, Ranking Member Thune:

We the undersigned parties, members of the Disinfo Defense League, respectfully request that you accept this letter for the record of your hearing on "Disrupting Dangerous Algorithms: Addressing the Harms of Persuasive Technology."

The Disinfo Defense League, or DDL, is a distributed national network of over 200 grassroots, community-based organizations that are building a collective defense against disinformation campaigns that deliberately target Black, Latinx, Asian American, and other communities of color.

We are deeply concerned by systemic problems posed by the complex set of digital tactics and designs that undermine confidence in our democracy, sow distrust among Americans in our public health institutions, disenfranchise voters, and chill engagement for our communities. From disinformation, to extractive data practices, to platforms' discrimination with algorithms — we have experienced the weaponization of online narratives that target our communities. These narratives are then amplified through the toxic business models of Big Tech and Big Media who have all shirked responsibility and accountability for their roles in spreading dangerous disinformation.

Policymakers must examine how the digital ecosystem distorts facts and spreads lies — and move swiftly to redress the harms. We are encouraged by this Subcommittee's efforts to consider this very issue. We write today to urge your consideration of principles codified in our newly

launched Disinfo Defense League Policy Platform,[1] designed to rein in technology companies' extractive data practices and to safeguard privacy and civil rights on social media platforms. We are calling for policymakers to enact a strategic set of solutions to quell disinformation and build a media ecosystem that serves the public interest by promoting accurate news and information, protecting civil and human rights, and fostering an informed, equitable electorate across all languages.

We are calling for broad reforms from Congress to adopt comprehensive digital-privacy legislation that protects digital civil rights by:

- *Limiting Big Tech's collection and use of our personal information.*
- *Establishing individuals' rights to control our own data.*
- *Enhancing data transparency.*
- *Preventing discrimination by algorithms.*
- *Enhancing platform transparency about the impacts of their business models.*
- *Protecting whistleblowers & external researchers.*
- *Setting a floor for consumer protection, not a ceiling.*
- *Enlisting the assistance of other federal agencies that protect the public with specialized expertise.*
- *Expanding Federal Trade Commission oversight.*

In addition to addressing the root design and algorithmic components of the problem, we also believe that Congress should support measures that will build up healthier and diverse information pathways for Americans to access news as a public good. Local news can be a powerful antidote to the spread of disinformation. To fully combat the problems of disinformation, hate and other malign practices online, we must fund local journalism. To that end, Congress should pass legislation to tax online advertising and direct those monies to support high-quality noncommercial and local journalism.

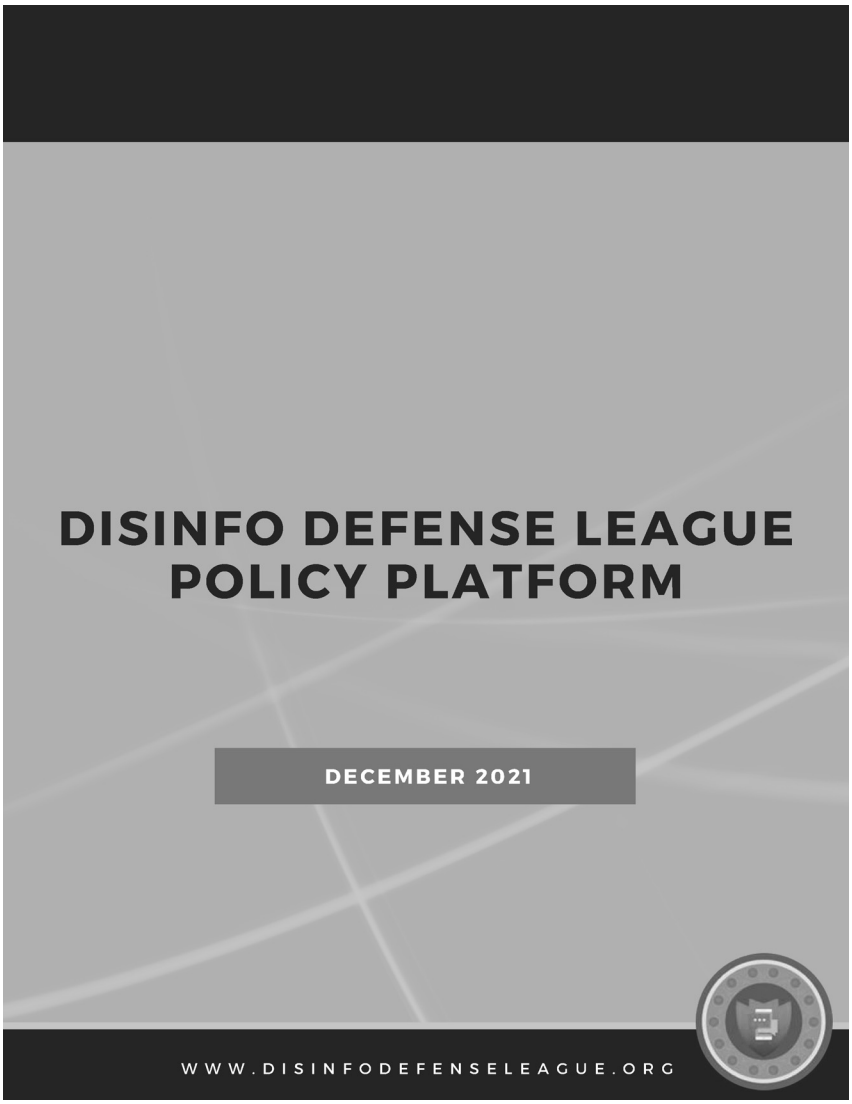
We urge you to examine and champion the principles within our Disinfo Defense League Policy Platform, which centers civil rights, places a responsibility on platforms to be transparent about their business models and data practices, and builds up healthier information pathways for people all over America.

---

[1] Disinfo Defense League, Policy Platform (Dec. 7, 2021), https://www.disinfodefenseleague.org/policy-platform.

Respectfully submitted,

Access Humboldt
Access Now
Arab American Institute (AAI)
Asian Americans Advancing Justice | AAJC
Asiant Pacific American Labor Alliance, AFL-CIO
Climate Disinformation Coalition
Common Cause
Cybersecurity for Democracy
Equality Labs
Facebook Users Union
Free Press Action
Friends of the Earth
Global Exchange
Indian American Impact
Japanese American Citizens League
Media Alliance
National Council of Asian Pacific Americans
ProgressNow New Mexico
The Greenlining Institute
UltraViolet
United We Dream


DISINFO DEFENSE LEAGUE
POLICY PLATFORM
DECEMBER 2021
WWW.DISINFODEFENSELEAGUE.ORG

DISINFO DEFENSE LEAGUE POLICY PLATFORM

The Disinfo Defense League is a distributed network of grassroots, community-based organizations that are building a collective defense against disinformation and surveillance campaigns that deliberately target Black, Latinx, Asian Americans and Indigenous people, along with other communities of color.

Over the past year, disinformation campaigns built on the system of surveillance capitalism have disrupted the ability to organize and disseminate accurate information — leading to real-world harms such as voter suppression, an insufficient public-health response to the pandemic, hate crimes, violence, harassment and a deadly insurrection at the U.S. Capitol.

Weaponized narratives targeting our communities are amplified through the toxic business models of Big Tech and Big Media.

Online platforms, cable channels and broadcasters alike have all shirked responsibility and accountability for their roles in spreading dangerous disinformation. Policymakers must examine how the corporate media ecosystem distorts facts and spreads lies — and move swiftly to redress the harms.

We are calling for policymakers to enact a strategic set of solutions to quell disinformation and build a media ecosystem that serves the public interest by promoting accurate news and information, protecting civil and human rights, and fostering an informed, equitable electorate across all languages.

LEGISLATIVE ACTION

Congress should adopt comprehensive digital-privacy legislation* that protects digital civil rights by:

1

LIMITING BIG TECH'S COLLECTION AND USE OF OUR PERSONAL INFORMATION.

Users should be able to control how apps use our data. We may want to share our data to receive services we sign up for, but apps should be prohibited from collecting more information than they need from us and from surreptitiously tracking us across the web. For example, the information we hand over for one reason — like providing a phone number for security purposes — shouldn't be shared or sold to third party companies.

2

ESTABLISHING INDIVIDUALS' RIGHTS TO CONTROL OUR OWN DATA.

We should have rights to easily access, correct, delete or download our personal information and take it with us when we leave an online service. Making data portable by law would let people free themselves from a corporate walled garden and easily use other services. These rights should apply equally to users across languages.

*** We support this legislative language for a digital-privacy and civil-rights bill drafted by Lawyers' Committee for Civil Rights Under Law and Free Press Action.**

LEGISLATIVE ACTION

3

ENHANCING DATA TRANSPARENCY.

We deserve to know what kinds of information companies and data brokers are collecting about us and there need to be strict safeguards on what is off limits. Data brokers gather incredibly private details like individuals' sex, age and gender, geolocation, health information; they can also collect internet-search histories that can reveal even more sensitive information like a visit to a mental-health facility or religious site. Companies need to disclose not just what information they collect, but where they get the information; who shares data with them, and with whom they share data; how they analyze data to profile us; how they use our information; how they make decisions about what content, goods or services to offer us; and how they secure our data.

Congress should close loopholes in existing privacy law by banning law enforcement from purchasing information from data brokers without a warrant and companies must conduct routine audits for bias, including an opportunity for independent analysis of algorithmic bias, as well as privacy assessments to determine the risks of this collection. And companies should be required to convey all of this information in two different ways: in an easy-to-understand format proactively notifying users, and in an exhaustive and detailed format for regulators, advocates and researchers for regular review.

*** Passing The Fourth Amendment Is Not for Sale Act would be an excellent start.**

LEGISLATIVE ACTION

4

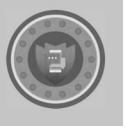
PREVENTING DISCRIMINATION BY ALGORITHMS.

Everything we do online generates data and every bit of that data can be tracked and used — no matter how innocuous it may appear in isolation — to create dangerous and invasive online profiles. Data feeds powerful algorithms to deliver personalized ads, recommendations and other services. There are some beneficial and harmless uses of these mechanisms when robust transparency and user control are present. But Congress should ban algorithms that profile users and target content to them in ways that constitute age, racial and sex discrimination in employment, housing, lending, and e-commerce. Congress should investigate voting and other civil rights violations that flow from abusive data practices.

5

ENHANCING PLATFORM TRANSPARENCY ABOUT THE IMPACTS OF THEIR BUSINESS MODELS.

Reporting over the past several years has demonstrated that — just as the tobacco companies knew that their products were killing people long before the public was made aware — social-media companies knew about how their business models were harming people and communities long before the details came to light. Companies should be required to provide access to researchers and to immediately disclose when they learn their platform algorithms are being used to discriminate against or otherwise harm people; and the companies should actively and in an ongoing manner mitigate those harms and be held accountable for any persisting harms.



LEGISLATIVE ACTION

6

PROTECTING WHISTLEBLOWERS AND EXTERNAL RESEARCHERS.

We must protect whistleblowers who come forward to expose unethical, immoral and discriminatory behaviors, algorithms and practices inside of tech companies. Protection from retaliation, labor violations, baseless lawsuits, and targeted harassment are critical to guaranteeing the rights of whistleblowers. We must also set out explicit protections for external researcher access to platform data.

7

EXPANDING FEDERAL TRADE COMMISSION OVERSIGHT.

The FTC should have the power and resources to conduct rulemakings and effectively enforce against and prevent data abuses and other unfair or deceptive practices. Congress cannot anticipate and legislate against all future uses and abuses of data that companies may engage in, so lawmakers should enable the FTC to oversee and respond to future violations. For instance, users shouldn't have to waive our privacy, quality of service, or other rights just to access a given service when there's no need for that data to deliver the promised goods.

LEGISLATIVE ACTION

8

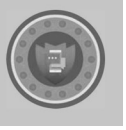
ENLISTING THE ASSISTANCE OF OTHER FEDERAL AGENCIES THAT PROTECT THE PUBLIC WITH SPECIALIZED EXPERTISE.

Federal agencies such as the Consumer Financial Protection Bureau, Department of Education, Department of Labor, Department of Justice and Department of Veterans Affairs, among others, should study how personal information is used in their fields, identify disparities and risks for discrimination, and issue public reports to Congress on a regular basis with special focus on the discriminatory effects on communities of color and non-English speaking groups.

9

SETTING A FLOOR FOR CONSUMER PROTECTION, NOT A CEILING.

A federal law must refrain from preempting the work that states are doing to build their own consumer-protection or privacy regimes. Many state consumer-protection laws are used to protect marginalized communities. A federal data-privacy law that broadly preempts state laws and weakens these kinds of protections would jeopardize civil rights.

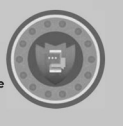


LEGISLATIVE ACTION

Congress should pass legislation to tax digital advertising and direct those monies to support high-quality noncommercial and local journalism.

Local news can be a powerful antidote to the spread of disinformation. To fully combat the problems of disinformation, hate and other malign practices online, we must fund high-quality, local journalism and urge Congress to create a small percentage tax on the online advertising revenues of the largest online platforms.

For example, a 2% tax, could yield more than $2 billion for a national endowment to support local news and information, including journalism by and serving people of color, non-English speakers, and other minority groups.*



*** Free Press' *Beyond Fixing Facebook* paper offers ideas on how Congress could institute a platform-advertising tax to support local journalism.**

EXECUTIVE ACTION

The Biden administration should leverage existing authorities to rein in disinformation.

The administration should appoint a White House official to coordinate interagency study and action on tech companies' civil-rights violations and other harmful data practices.

The Federal Trade Commission should initiate a rulemaking on harmful data and algorithmic practices and prosecute discriminatory data practices and data-related abuses.

The FCC should issue guidance pursuant to the broadcast-hoax rule warning broadcasters to refrain from airing inaccurate claims about the pandemic, a public-health emergency. The FCC's broadcast-hoax rule prohibits broadcasters from knowingly airing false information about a catastrophe if it's foreseeable that doing so would cause substantial harm.

The FCC should use this authority to stop the spread of deadly health disinformation. Before renewing broadcasters' licenses, the agency should evaluate whether licensees are adhering to their public-interest mandates.

The Justice Department, FTC and other federal and state enforcement agencies should apply antitrust law to stop tech giants' never-ending acquisition of new firms.

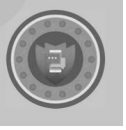
Agencies should stop the dominant platforms' monopoly abuses, collusion and other anti-competitive practices when and where they happen. Congress should ensure that the agencies are well funded.

INTERNATIONAL ACTION

The United Nations should document and analyze the harms that disinformation has caused to historically-oppressed populations around the world, and set in place the building blocks for repair.

The U.N. should investigate the harms of disinformation across the world and the unique harms to Black, Indigenous, and brown people. Building on the 2021 report on disinformation by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression made to the U.N. Human Rights Office of the High Commissioner, the U.N. should issue a full report on the harms caused by disinformation, with particular focus on the harms to Black, Indigenous, immigrant, and brown communities around the world.

In consultation with expert organizations, the full report should be accompanied by a set of recommended state policies for governments to consider adopting to stop the spread of disinformation. It should also suggest remedies for the harms people have already experienced.



POLICY PLATFORM SIGNATORIES

The following organizations* have signed on to the Disinfo Defense League policy platform:

Access Humboldt
Access Now
Arab American Institute
Asian Americans Advancing Justice - AAJC
Asian Pacific American Labor Alliance, AFL-CIO
Common Cause
Cybersecurity For Democracy
Demos
Detroit Community Technology Project
Equality Labs
Facebook Users Union
Fight For The Future
Free Press Action
Global Exchange
The Greenlining Institute
Indian American Impact
Instituto di Geopolitica Digitale
Japanese American Citizens League
Kairos
Media Alliance
MediaJustice
Miami Workers Center
Mijente
National Council of Asian Pacific Americans (NCAPA)
New Georgia Project
Noticias Para Inmigrantes
OpenMIC
People's Action
ProgressNow New Mexico
Public Good Projects
ReFrame
Rural Organizing Project
Ultraviolet
United We Dream
Women's March

* *as of December 6, 2021*

The Disinfo Defense League (DDL) is a distributed national network of organizers, researchers and disinformation experts disrupting online racialized disinformation infrastructure and campaigns that deliberately target Black, Latinx, Asian American / Pacific Islander and other communities of color. DDL was created by and for these communities and is supported by services and insight provided by expert partners and organization.

Launched in June 2020, DDL uses coordinated strategy, disinformation training, and research to support member organizations with resources to fortify and scale current inoculation efforts and increase cohesion and collaboration in targeted communities.

DDL features over 230 organizational members who work across geography, generation, and gender to equip communities with tools, training, and tactics needed to combat racialized disinformation and win.

WWW.DISINFODEFENSELEAGUE.ORG

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KYRSTEN SINEMA TO ROSE JACKSON

Spread of Misinformation. Misinformation remains rampant on social media and is a significant problem. For example, misinformation about the COVID–19 pandemic has contributed to public confusion. Also, during the 2020 presidential election, a number of false rumors circulated on social media platforms alleging wrongdoing by election administrators.

Question 1. What steps can social media companies take to combat the harm of misinformation? Could algorithms work in reverse to limit the content containing false information a user encounters instead of leading them down a path to continued exposure to misleading claims?

Answer. Large digital platforms deploy a range of policies, technologies, and tactics to moderate the content on their services. The most productive approach for addressing misinformation will vary platform by platform, and be affected by the particular features and products the platform offers (*i.e.,* audio versus video or text; ephemeral posts or content), the user base the platform serves, the languages it operates in, and other related factors. Content moderation approaches therefore are best targeted to those specific contexts. Algorithms can be (and in many cases are already) used in several ways. For example, platforms use automation and algorithms to review posts, add labels and links to sources, and solicit user feedback on content offered to consumers. Additionally, companies sometimes de-rank or simply remove targeting from posts containing mis- or disinformation and have experimented with adding friction to slow down a piece of content as it goes viral. These approaches have had some success in reducing or mitigating mis- and disinformation, and where they are effective, they should be scaled and applied in new contexts. However, technological, or automated approaches to content moderation will never be perfect. In some cases, these approaches fail to remove clearly illegal (or counter to terms of service) content, and in others they result in the over-removal of content, often including critical, satirical, and legitimate expression.

To combat the harm of misinformation, large digital platforms can: establish clear terms of service and trust and safety policies; communicate those policies (and their enforcement) in all languages in which the platform is available; make clear when algorithms, filtering, or other technologies are used to alter the display of content to a user, and enable users to control those settings; employ techniques (including those referenced above) that are shown to decrease the spread of mis- and disinformation; and establish policies to target the coordinated abuse of platform features. Platforms can also combat these harms by sharing information and partnering with civil society organizations and the communities most affected, to co-create solutions, and build societal resilience.

Question 2. What steps could Congress take to address this issue while recognizing the importance of freedom of expression?

Answer. Addressing the challenge of mis- and disinformation requires a "multi-stakeholder approach." The issue is systemic, with narratives and trends spreading across an information ecosystem comprised of numerous platforms and countless communities. That means it cannot be solely addressed by a single platform, or sector. Congress would be wise to design its legislation and direct its oversight to incentivize industry, empower civil society, center the American public and users, and strengthen the government's ability to set and enforce the rules. Substantively, Congress should prioritize protecting privacy, enabling transparency and accountability, and ensuring the U.S. government is appropriately staffed and resourced for our digital age. Doing so would provide a meaningful foundation for many of the specific laws and rulemaking under consideration to address the issues discussed during the hearing.

While a particular piece of content may be evidence of disinformation, addressing the systemic drivers of the problem is a more fruitful approach. That means focusing on product design, business models, and other platform incentives that either result in the spread of certain content or incentivize and reward behavior online that contributes to the problem. As I mentioned during my testimony, the conversations we are having about the Internet and the digital world are interrelated. The gaps in privacy or data protections in the United States contribute to the incentive to create and collect more—and more sensitive—data to use for everything from better targeted advertising to the development of new artificial intelligence models and tools. Passing comprehensive privacy or data protection legislation would set standards for how that data could be collected and used, potentially changing the incentives for platforms on everything from design to policy.

Second, Congress can set standards for the basic information platforms are required to disclose, whether clear terms of service and policies, or insight into why

users are viewing certain content. Proposals to create a new bureau in the FTC focused on data and technology would be a good first step toward setting such standards and tracking how major platforms operate. A better resourced FTC could also facilitate the growing calls for better data and information on platforms, to inform government agencies and Congress, as well as the community of academic and independent researchers who work with civil society to shed light on the impact of these pervasive technologies and platforms in society. Organizations like my own in the open-source research community have been instrumental in uncovering and documenting how individuals and groups manipulate platforms and populations. And we use that knowledge to inform the public and advise companies, governments, and civil society on appropriate responses. But our knowledge is limited by what data is available to us, and we know there is much about the information ecosystem we miss. Addressing disinformation requires driving down the information asymmetry between platforms and everyone else.

But the task of rulemaking and enforcement cannot sit with the FTC alone. The Federal Communications Commission (FCC), Consumer Financial Protection Bureau (CFPB), and others have significant roles to play. Congress should bolster the resources and capacity of these entities alongside the FTC, and work to clarify mandate and points of coordination between them to ensure companies are spending time and resources on the requests and changes that are most impactful. Finally, Congress should seek to ensure existing law is applied to a digital context. In some cases, this will mean prompting agencies to update their approach to existing work and authorities. In other cases, Congress may need to consider new laws. Congress should consider adopting proposals such as those that would require the same funding disclosures for digital advertising as is required on television and other legacy media, or those requiring platforms provide public advertising libraries. Congress could also apply existing law in new places; Bills like the Malinowski-Eshoo *Protecting Americans from Dangerous Algorithms Act,* for example, apply limited liability exceptions on the basis of narrowly defined existing criminal statutes.

Foreign Language. Media reports suggest that many social media companies have not invested resources in addressing misinformation being spread in languages other than English. This poses risks to non-English speaking communities in the United States, including Spanish speaking residents in Arizona, as well as residents of foreign nations who utilize these tech platforms that have headquarters in the United States.

Question 3. What responsibility do tech companies have to prevent their platforms from being used to spread misinformation in languages other than English, which can result in political violence in the United States or in foreign nations?

Answer. It is important to note that while many large digital platforms have voluntarily taken steps to address mis- and disinformation they do not have a legal responsibility to do so in any language. However, to responsibly operate in any market, companies should have staff capable of communicating in and understanding the core languages within that market. They should publicize their key company and policy documents (such as terms of service and community guidelines) in those languages, and ensure any content moderation decisions, reporting features, or other core platform components are likewise made available in each of those languages. Companies should publish (in a centralized and easy-to-read format) the languages in which particular services are provided, and what products and services are made available in each region and language. While these may seem like small, or even obvious asks, no company currently provides most of the above consistently, with a few exceptions.

Another important element is the ways in which platforms collaborate with civil society and the public. Mis- and disinformation spreads across multiple platforms and requires whole-of-society responses. My organization, the Digital Forensic Research Lab, often uncovers the manipulation of information environments in foreign countries and languages. We work collaboratively with platforms to flag these issues and make our research public to inform civil society responses and government action. Whether platforms make data and other information available to organizations like my own, particularly in countries outside the United States, has a direct impact on our understanding of the problem and ability to respond. Further, whether platforms respond promptly when communities do highlight growing unrest, harassment, or violence can make the difference between life and death. The lack of language appropriate staff can slow responses and hamper essential contextual understanding.

Research Access. We heard during the hearing about the potential value in permitting researchers, particularly those in an academic setting, to examine user data

from tech companies or from probing social media sites by setting up accounts to examine the content those accounts receive exposure to.

Question 4. What types of data do you believe Congress should require tech companies to disclose to researchers so they can examine the effects of algorithms on every day Americans?

Answer. There is no question that the asymmetry of knowledge between large digital platforms and everyone else is a barrier to addressing online harms. That is why so many legislators, researchers, and other experts have increasingly turned toward transparency and data access as a focal point for action. What each of these groups means by "transparency" however is less clear, complicating calls for companies to be required to provide certain kinds of information to researchers, regulators, or the public. Enabling societies to better understand the impact of platform design and policies is important, but transparency is not an end in and of itself. And if focused on transparency to promote accountability and prevent harm, it is important to build flexibility into what we prioritize as the most essential information. Rather than focus on Congress delineating the specific forms of data or reports platforms be required to provide, it can authorize and fund regulatory and oversight bodies to set standards and requirements that can adapt as technology changes and our understanding of related challenges grows.

It is also important to acknowledge that algorithms are used across several industries and sectors for vastly different purposes. Understanding the data used to develop machine learning models, the use and context of those models, and the societal impact they have will vary whether looking at those used to predict the success of students, those used to determine whether someone is granted a loan, or those used by the justice system to inform sentencing. That is why I focused in my testimony on the need to appropriately resource agencies and offices across the U.S. government to play their role in enforcing existing law in a digital context and identify where new law is required.

In reference to large digital platforms, Congress could consider the approach taken in the European Union's Digital Services Act (DSA), which includes a mix of requirements ranging from the provision of specific data, to standardized transparency reporting, or the conduct of risk assessments. As these technologies advance, so too does the field studying them. Congress would be wise to ensure new insights and best practices can inform and adapt how oversight is conducted.

Question 5. Broadly speaking, how would you define "researchers" to ensure that only legitimate researchers can obtain information?

Answer. In establishing information sharing requirements between digital platforms, regulators, researchers, and the public, it's important we be specific about the kinds of information and data at play, and the tradeoffs between transparency and security or privacy. There is a great deal of platform information that would not have significant privacy implications, and we should be careful not to limit all access to such information to a small subset of individuals. That said, for more sensitive or expansive forms of information and data the following qualifications for researchers should be considered. To be "qualified" a researcher should be affiliated with an organization or institution that: is a registered non-profit; has proven expertise in studying information environments; publicizes their research methodology; and makes public the results of their research. Researchers should be required to abide by established terms of use and be barred from access should they violate those agreements. There are strong proposals for the creation of a new office within the FTC to delineate these definitions more clearly, to create terms of use, and identify which data and information should be provided by covered platforms. Doing so would enable regulators to flexibly revise the approach over time to find the right balance between access and privacy, while holding researchers accountable to these standards.

Transparency and Intellectual Property. I want to ensure that the Internet remains a place of innovation. In addition to academic researchers, some have proposed that the general public have additional information about the algorithms tech companies employ to run their platforms.

Question 6. If Congress pursues measures to require tech companies to disclose more information about algorithms, how can we ensure that those companies' intellectual property remains protected and does not fall into the hands of competitors or nefarious actors?

Answer. As referenced in question four, algorithms are used across a range of industries for a variety of purposes. So, the answer regarding large digital platforms may not apply to algorithms used for law enforcement, college admissions, or other purposes. When an algorithm is being used to make decisions on behalf of the government, or in ways that fundamentally determine a citizens' access to education,

finance, and essential services, understanding why those decisions are being recommended is a base necessity.

When it comes to large digital platforms, as Dr. Dean Eckles testified during the hearing, many of the algorithms being used are not particularly sensitive or proprietary, and disclosure of the level the committee is discussing would be unlikely to create significant intellectual property risks. That said, balancing interests such as these is why Congress would be wise to authorize and resource regulatory bodies to set the rules for the type of information required from companies, and the level of access provided to the public, to researchers, and to the government more broadly.

It is also worth noting, that some transparency steps could be taken without sharing large data sets or divulging proprietary information. For example, some experts recommend platforms inform a user when they are seeing a post, certain content, or advertising because of a particular ranking or targeting algorithm. Others suggest that platforms allow users to opt-out of such targeting. These steps would provide users with more context and power in choosing and understanding their digital environments, which can help build resilience against bad actors manipulating platforms and the broader information ecosystem as well.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RAPHAEL WARNOCK TO ROSE JACKSON

In recent years, we have seen several examples of targeted advertising algorithms that can enable discrimination and may violate Federal law. For example, in 2019, the Department of Housing and Urban Development sued Facebook over housing advertisements that could be targeted on the basis of protected classes such as race, religion, familiar status or others. Facebook has also been sued for targeting tools and algorithms that may have shown job advertisements to certain populations based on age.

Question 1. Do you believe that existing Federal anti-discrimination laws adequately address the ways that algorithms can enable discrimination? If not, how should Congress and Federal agencies develop new regulations to enable greater oversight?

Answer. The 1964 Civil Rights Act, the 1968 Fair Housing Act, and the 1974 Equal Credit Opportunity Act set clear precedents against discrimination on the basis of protected classes. The same rights afforded to citizens offline should also be enforced online, especially in instances where citizens' civil rights are threatened. The first step is to ensure that existing laws are applied to the online world. More can be done to provide agencies responsible for overseeing and ensuring these protections with the resources and capacity required to update their operations for an online context. Congress could direct the administration to review those agencies and offices responsible for enforcing such protections to determine how, or whether, mandates have been sufficiently applied to digital tools and the Internet. Subsequently, Congress could consider additional legislation clarifying the application of these laws in a digital context, or where required, develop legislation explicitly establishing new requirements pertaining to the role of curation, algorithmic amplification, direct targeting, or automated decisionmaking in such discrimination.

The risk of algorithmic discrimination extends beyond social media and the Internet. Algorithms are now used to aid in decisionmaking on everything from hiring, to loans, to college admittance. Rather than seek one standard for all algorithms, Congress should consider appropriate regulations and standards applied to various industries. As new technology continues to mainstream into nearly every aspect of life, it will become harder to regulate a technology per-say, rather than its use and application industry by industry.

Question 2. Do Federal agencies have adequate authorities and resources to investigate and, if necessary, prosecute corporations that enable discrimination through their algorithms? If not, what additional authorities or resources are necessary?

Answer. Ultimately, Federal agencies do not have adequate authorities and resources to investigate and, if necessary, prosecute corporations that enable discrimination through their algorithms. In my testimony, I called on congress to create and resource a new bureau at the FTC to address online privacy, data security, and other online abuses, including discrimination, voter suppression, and civil rights violations. But the FTC has a narrow mandate. Congress must provide resources and support to all agencies to improve their understanding of and engagement on issues related to the application of technology. It can do so through further support for and investment in the U.S. Digital Service (USDS) and other related U.S. Government service-oriented tech agencies and offices. I also recommended that congress pass

legislation to foster greater transparency and accountability around online harms, and address information asymmetries between companies and everyone else, to understand the full extent of these harms, and inform solutions.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KYRSTEN SINEMA TO JESSICA J. GONZÁLEZ

Spread of Misinformation. Misinformation remains rampant on social media and is a significant problem. For example, misinformation about the COVID–19 pandemic has contributed to public confusion. Also, during the 2020 presidential election, a number of false rumors circulated on social media platforms alleging wrongdoing by election administrators.

Question 1. What steps can social media companies take to combat the harm of misinformation? Could algorithms work in reverse to limit the content containing false information a user encounters instead of leading them down a path to continued exposure to misleading claims?

Answer. Social media companies can and should do more to combat misinformation. These platforms are pushing content to users through algorithms that, in most cases, are trained to drive the highest engagement. As Frances Haugen shared with this committee, inflammatory content and conspiracy theories tend to fit this bill.

Platforms have failed outright at fulfilling even the most basic requests for transparency about how their systems work, what they know about us and how they use our data to target us with content. Their data collection is pervasive, and may be invasive and extractive. Only platforms have the data about who sees what information and how much they engage with it. That gross imbalance is even more in focus now because platforms like Facebook have been shown to be aware of the negative impacts of their design and have failed to adapt it to prevent and mitigate harms, such as the misinformation about COVID and the 2020 election that you mention.

We each are seeing vastly different things online—predicated on online platforms' data practices, many of which are abusive and merit further scrutiny from an expert agency such as the Federal Trade Commission. The divide between us all in what we see (and when we are largely unaware of what others see) means that we simply don't have the ability to fully ascertain who is being persuaded by what.

No one silver bullet will solve this problem and we need both corporate responsibility and a strong government response to targeted and prolific lies that threaten our health and safety and even our democracy. Free Press has a series of recommendations to online platforms designed to disrupt online bigotry and conspiracies and to shed greater light on how these systems operate to help us identify further areas for improvement:

- Free Press has worked with Change the Terms, a coalition of more than five dozen racial justice and digital and civil rights groups, to release a set of model corporate policies to disrupt online hate. Most of these measures would significantly reduce misinformation as well, including modifications to the companies' terms of service, appeal policies, enforcement mechanisms, content moderation training procedures, regular audits of the algorithms, and far more transparency to researchers and the public.[1]
- Companies can and should institute some of the mitigation measures put in place ahead of the 2020 election to slow the spread of lies and bigoted propaganda and promote accurate information.[2]
- Whatever rules social media companies adopt, they should apply to all users. Powerful people must be held to the same standards as the rest of us. There should not be a special set of more lenient rules for the rich, powerful and famous that allow them to proliferate conspiracy theories and bigotry with impunity.
- As the #YaBastaFacebook campaign and community organizations have been pointing out for years now, social media companies have done an especially poor job of moderating content in languages other than English. Frances Haugen revealed internal Facebook documents that demonstrate that Facebook has seriously underinvested in keeping its platforms safe across languages. Facebook is

---

[1] Change the Terms, "Recommended Internet Company Corporate Policies and Terms of Service to Reduce Hateful Activities," *https://www.changetheterms.org/terms.*

[2] *See, e.g.,* Kevin Roose, *Facebook reverses postelection algorithm changes that boosted news from authoritative sources.*, N.Y. TIMES, Dec. 16, 2020, at *https://www.nytimes.com/2020/12/16/technology/facebook-reverses-postelection-algorithm-changes-that-boosted-news-from-authoritative-sources.html.*

not alone. All social media companies must commit to and invest in keeping their platforms safe across languages.

We need multi-layered solutions to these problems, and while self-regulation is one necessary intervention, many social media firms have demonstrated that they are unwilling to meaningfully self-regulate. Government intervention is necessary.

Question 2. What steps could Congress take to address this issue while recognizing the importance of freedom of expression?

Answer. Congress must legislate to rein in tech company abuses while protecting free expression. Pages seven through seventeen of my written testimony for this hearing outline Free Press Action's recommended legislative framework.[3] In short, Free Press Action recommends that Congress adopt digital privacy and civil rights legislation that:

- Limits tech's collection and use of our personal data.
- Establishes people's rights to control their own data.
- Enhances data transparency.
- Prevents discrimination by algorithms.
- Increases platforms' transparency about known impacts of their business models.
- Protects whistleblowers and external researchers.
- Expands FTC oversight.
- Encourages collaboration across agencies that hold specialized expertise.
- And sets a Federal floor for consumer protection, not a ceiling.

This approach has been endorsed by over three dozen grassroots organizations in the *Disinfo Defense League,* a distributed national network of organizers, researchers and disinformation experts disrupting online racialized disinformation infrastructure and campaigns that deliberately target Black, Latinx, Asian American/Pacific Islander and other communities of color.

Fortunately, many of these elements are included in Senator Markey's Algorithmic Justice and Online Transparency Act, which prohibits algorithms that discriminate based on protected characteristics, and establishes safety and effectiveness standards;[4] and in the Consumer Online Privacy Rights Act, sponsored by Senators Cantwell, Schatz, Klobuchar and Markey, which penalizes platforms that abuse personal data, allows people to see the information companies collect on them, and preserves a Federal private right of action.[5] Free Press Action endorses both bills.

In addition to privacy and civil-rights safeguards, to combat disinformation we must invest in a thriving media system to support a 21st-century democracy. Free Press Action and the Disinfo Defense League have urged Congress to pass legislation to tax digital advertising and direct those monies to support high-quality noncommercial and local journalism, including journalism by and serving people of color, non-English speakers, and other minority groups.

Foreign Language. Media reports suggest that many social media companies have not invested resources in addressing misinformation being spread in languages other than English. This poses risks to non-English speaking communities in the United States, including Spanish speaking residents in Arizona, as well as residents of foreign nations who utilize these tech platforms that have headquarters in the United States.

Question 3. What responsibility do tech companies have to prevent their platforms from being used to spread misinformation in languages other than English, which can result in political violence in the United States or in foreign nations?

Answer. Tech companies have a responsibility to keep people safe and enforce their terms of service in all languages in which they operate, and they are failing miserably to do so. This puts non-English speakers at risk as they navigate targeted disinformation campaigns about COVID and vaccines.

Free Press noticed a significant gap in the moderation efforts of social media companies in non-English languages in the lead up to the 2020 presidential election. As platforms took enforcement actions to address militarized social movements in

---

[3] *Disrupting Dangerous Algorithms: Addressing the Harms of Persuasive Technology: Hearing Before the Subcomm. on Commc'ns, Media, & Broadband of the S. Comm. on Sci., Commerce, & Transp.,* 117th Cong. (2021) (statement of Jessica J. González, Co-CEO, Free Press Action), *https://www.commerce.senate.gov/services/files/FCB71657–4A1C–4796–BCED–55BBF418246A.*

[4] Algorithmic Justice and Online Transparency Act, S. 1896, 117th Cong. (2021).

[5] Consumer Online Privacy Rights Act, S. 3195, 117th Cong. (2021).

English (QAnon, calls for violence related to Kenosha, etc.) similar Spanish-language posts remained widely available.

Frances Haugen's documents revealed just how extensive the asymmetries are and how systems to proactively keep users safe are not replicated across languages.

Despite Haugen's shocking revelations and repeated requests from civil rights leaders and elected officials, we still don't know how many content moderators speak Spanish, where they are located, or how they are trained and treated. Recent reporting suggests, for instance, that working conditions for Spanish-language content moderators are unequal to those of English-language moderators.[6]

Basic transparency could help identify why these gaps exist and pave the way for solutions, but so far the companies have resisted calls for more transparency.

Research Access. We heard during the hearing about the potential value in permitting researchers, particularly those in an academic setting, to examine user data from tech companies or from probing social media sites by setting up accounts to examine the content those accounts receive exposure to.

Question 4. What types of data do you believe Congress should require tech companies to disclose to researchers so they can examine the effects of algorithms on every day Americans?

Answer. Researchers need access to information about platform moderation data, such as the number of posts, accounts, groups, etc. that are removed for violating platforms' corporate policies. Tech companies should also provide researchers with content that they are removing from their platforms. When platforms conduct internal research that demonstrates their services are causing widespread harm, they should have to disclose that immediately to researchers and the broader public. For instance, it should not take a Wall Street Journal exposé two years after the fact to reveal that Facebook's own recommendation system is responsible for 64 percent of people who find extremist groups on its platform. Nor should it require a whistleblower to reveal that Instagram knew it was harming teen girls.

Question 5. Broadly speaking, how would you define "researchers" to ensure that only legitimate researchers can obtain information?

Answer. Some of the most innovative research about how online disinformation and extremism are playing out in our communities is coming not from elite educational institutions but rather from the very communities that are most impacted by these issues. I'd recommend liberally defining "researchers" to ensure that academics, journalists, freelancers, non-profit organizations and community leaders alike can access data and information. Instead of focusing on one's affiliation, Free Press Action recommends prodding one's willingness to comply with protective orders or other guidelines. A researcher should be deemed "legitimate" as long as they are indeed engaged in research and willing to follow the rules, not based on credentials or the content and aims of one's research interests.

Transparency and Intellectual Property. I want to ensure that the Internet remains a place of innovation. In addition to academic researchers, some have proposed that the general public have additional information about the algorithms tech companies employ to run their platforms.

Question 6. If Congress pursues measures to require tech companies to disclose more information about algorithms, how can we ensure that those companies' intellectual property remains protected and does not fall into the hands of competitors or nefarious actors?

Answer. Congress can protect tech company disclosures by barring any party that is engaged in "Competitive Decision-Making" from accessing confidential data. This would exclude direct employees of competing firms from accessing the information. "Competitive Decision-Making" in this context would mean a person's activities, association, or relationship with any of their clients involving advice about or participation in the relevant business decisions or the analysis underlying the relevant business decisions of the client in competition with or in a business relationship with the party submitting the disclosures.

---

[6] Sarah Emerson, *Facebook's Spanish-Language Moderators Are Calling Their Work A "Nightmare,"* BUZZFEED NEWS, Jan. 13, 2022 at *https://www.buzzfeednews.com/article/sarahemerson/facebooks-spanish-language-moderators-said-theyre-treated.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RAPHAEL WARNOCK TO JESSICA J. GONZÁLEZ

In recent years, we have seen several examples of targeted advertising algorithms that can enable discrimination and may violate Federal law. For example, in 2019, the Department of Housing and Urban Development sued Facebook over housing advertisements that could be targeted on the basis of protected classes such as race, religion, familiar status or others. Facebook has also been sued for targeting tools and algorithms that may have shown job advertisements to certain populations based on age.

Question 1. Do you believe that existing Federal anti-discrimination laws adequately address the ways that algorithms can enable discrimination? If not, how should Congress and Federal agencies develop new regulations to enable greater oversight?

Answer. Existing Federal anti-discrimination laws are a critically important keystone to fighting algorithmic discrimination, but Congress must do more. Opaque algorithms obscure algorithmic decision-making and obstruct our ability to redress their discriminatory impacts.

Congress should legislate to further protect civil rights in the digital age. Pages seven through seventeen of my written testimony for this hearing outline Free Press Action's recommended legislative framework.[7] In short, Free Press Action recommends that Congress adopt digital privacy and civil rights legislation that:

- Limits tech's collection and use of our personal data.
- Establishes people's rights to control their own data.
- Enhances data transparency.
- Prevents discrimination by algorithms.
- Increases platforms' transparency about known impacts of their business models.
- Protects whistleblowers and external researchers.
- Expands FTC oversight.
- Encourages collaboration across agencies that hold specialized expertise.
- And sets a Federal floor for consumer protection, not a ceiling.

This approach has been endorsed by over three dozen grassroots organizations in the *Disinfo Defense League,* a distributed national network of organizers, researchers and disinformation experts disrupting online racialized disinformation infrastructure and campaigns that deliberately target Black, Latinx, Asian American/Pacific Islander and other communities of color.

Fortunately, many of these elements are included in Senator Markey's Algorithmic Justice and Online Transparency Act, which prohibits algorithms that discriminate based on protected characteristics, and establishes safety and effectiveness standards;[8] and in the Consumer Online Privacy Rights Act, sponsored by Senators Cantwell, Schatz, Klobuchar and Markey, which penalizes platforms that abuse personal data, allows people to see the information companies collect on them, and preserves a Federal private right of action.[9] Free Press Action endorses both bills.

In addition to privacy and civil-rights safeguards, to combat racialized disinformation we must invest in a thriving media system to support a 21st-century democracy. Free Press Action and the Disinfo Defense League have proposed that Congress pass legislation to tax digital advertising and direct those monies to support high-quality noncommercial and local journalism, including journalism by and serving people of color, non-English speakers, and other minority groups.

Question 2. Do Federal agencies have adequate authorities and resources to investigate and, if necessary, prosecute corporations that enable discrimination through their algorithms? If not, what additional authorities or resources are necessary?

Answer. Federal agencies have existing authorities to investigate and enforce civil rights laws and rules against corporations engaged in discrimination, but would benefit from additional resources and rulemaking authority.

---

[7] *Disrupting Dangerous Algorithms: Addressing the Harms of Persuasive Technology: Hearing Before the Subcomm. on Commc'ns, Media, & Broadband of the S. Comm. on Sci., Commerce, & Transp.,* 117th Cong. (2021) (statement of Jessica J. González, Co-CEO, Free Press Action), *https://www.commerce.senate.gov/services/files/FCB71657-4A1C-4796-BCED-55BBF418246A.*

[8] Algorithmic Justice and Online Transparency Act, S. 1896, 117th Cong. (2021).

[9] Consumer Online Privacy Rights Act, S. 3195, 117th Cong. (2021).

Existing civil rights laws remain woefully under-enforced with regards to algorithmic decision-making and data use. For instance, the Equal Employment Opportunity Commission has authority to regulate hiring algorithms and facial-recognition software. The Department of Housing and Urban Development (HUD) has explored disparate-impact claims pertaining to housing discrimination. Machine-learning bias in credit denial can have lasting impacts on a family's wealth, and the Equal Credit Opportunity Act (ECOA) is meant to guard against that kind of discrimination.

The Federal Trade Commission (FTC) should enforce any violations of the Equal Credit Opportunity Act, which prohibits credit discrimination based on several protected characteristics; and the Fair Credit Reporting Act, which requires people to be notified when adverse actions about them are made, and allows them to dispute any inaccurate information. Both of these existing laws offer critical protections for consumers in the credit context—which has many implications across other areas like housing, employment, and insurance.

To the extent that unfair practices and discriminatory practices fall outside of the scope of these two acts, the FTC can regulate unfair and discriminatory algorithms under its existing unfairness doctrine authority, Section 5 of the FTC Act.[10] Congress should ensure a more expedited regulatory process by granting the FTC additional rulemaking authority under the Administrative Procedures Act.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO JAMES POULOS

Question 1. I was intrigued by your prepared testimony, where you talk about addressing digital harms by passing a "Second Amendment for Compute." Can you elaborate further on what you mean by that?

Answer. The idea of the Second Amendment for Compute is to legally identify and enshrine the basic American rights to build and use digital computational technologies. Notably, these rights are already implicitly included in the First and Second Amendments, because the two uses of the technologies are as communications tools and as offensive and defensive weapons. The deepest roots of American culture, civics, and civilization are found in the conviction that, as a matter of justice and sound political theology, the rights of human persons who have come of age to communicate and bear arms are natural and God-given, things no just government can infringe, abridge, abrogate, or deny.

In this sense we and our Constitution already have all the justification and legal authority needed to protect and defend American citizens' rights to keep and bear digital tech. Now, in the early debates of the founding era, the Antifederalists warned that while a Federal Constitution of enumerated powers blocked tyranny and unjust rule, enumerated rights did the opposite. And there is something powerfully true to the insight that a people have likely already lost their shared faith or conviction in what they must make explicit.

Nevertheless, one glance today shows that the brazen and systematic violation of the rights to keep and bear digital technologies that are implicit in the First and Second Amendments is foundational to our emergent political and economic order. Our unelected rulers in public and private life work hand in hand every moment of every day to preempt and defeat those rights. Control of digital life is consolidated in the hands of the military-intelligence complex and the tech oligarchy, upon whose economic performance America's administrative class and financial system now utterly depends. Under their control, Americans are being coercively conditioned to accept the wholesale expropriation of their private lives as well as the "public square" into the cyberspaces operated, owned, and policed by the major tech corporations, which are properly understood as the core strategic governance organs of the administrative state, including the military-intelligence complex.

What is unfolding is—by design—the founding of a new, digital regime, one hostile and fatal to our distinctively American way of life and our constitutionally guaranteed form of government, and one resting on a political theology that repudiates and destroys our most venerable Western principles of natural right and Man's relation to his Creator. As the turmoil of the Trump years made inescapably plain, the operators of this regime are increasingly naked in their use of media of all kinds, through the digital technologies that now rule them all, as weapons against Americans who dare resist or even object to their extension and consolidation of digital power and authority.

---

[10] Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2021).

This means that it is now too late legally, and technology is advancing too quickly, to any longer leave merely implicit the natural and God-given rights that Americans already possess with regard to digital technologies. To save those rights, and our civilization and form of government with them, we must enumerate Americans' digital rights—*come what may.* Congress must be undaunted by administrative state objections that Americans are too stupid, crude, hateful, sinful, inexpert, or simply dangerous to be allowed such rights and their free exercise. America's global adversaries and enemies will not seize control if Americans begin that free exercise. Quite the contrary: our technological rulers today are railroading us into a post-American order where elites who see America (correctly) as the main obstacle to founding a new globalistic cyborg order. Nor will the free exercise of natural and God-given digital rights crash our financial system, as the SEC and other agencies and officials insist on arguing. Our financial and regulatory leaders across the public and private sector have already repeatedly crashed our financial system. Grievously and irreparably harming generations of Americans, these ostensible elites have suffered virtually zero accountability or punishment, in fact only growing more powerful, more wealthy, more impudent, and more divorced from our American identity, our American norms, and our American principles. They simply cannot be trusted to tell us the truth about the likely effects of Americans' free exercise of digital rights—aside from their implicit admission that their illegitimate stranglehold on our fates and fortunes cannot survive a restoration of American constitutionalism in digital life.

That brings us to the explicit terms of legal protection envisioned by the "Second Amendment for Compute." They begin simply with the right of Americans to buy, sell, and build high-powered GPUs—a right already being stealthily infringed by "energy regulations" in several states including California itself. The entire canard that powerful computation is too "eco-unfriendly" to be allowed to America's digital serfs—a charge laid aggressively against bitcoin and other cryptocurrencies—is a fallacy Congress must recognize as such. Americans' use of high-powered GPUs to freely build digital tools and cultural and economic institutions expends far less "energy" than, say, the petrodollar and its form of economic life, or than the military-intelligence complex; still more deeply, since John Locke and well before it has been a fundament of Western life to understand that the just building and maintenance of life and flourishing in our human and natural spacetime *requires as its price* the expenditure of energy, in the form the sweat of our brows and the ache of our bodies, of the productive calculations of our minds, and of our creation and use of the tools and weapons we need to achieve both our most basic and fundamental ends and our higher forms of creativity, genius, worship, and wealth.

By extension therefore it is equally clear that the right of Americans to buy, sell, mine, and mint bitcoin and other digital coins must not be infringed, neutralized, or destroyed. It is essential that lawmakers realize bitcoin, to take the most important example, is not simply a new currency among many, a new asset class among many, or a new fad among many. It is a *computational protocol* that supervenes upon or obsolesces a host of previous forms of digital architecture, because of its tremendous power and adaptability. It is, in this sense, a computer that can and likely will very soon grow large enough in its development to supervene upon the entire world, "ruling" it in a way no one person or group of people, no matter how brilliant, willful, expert, or ambitious, can any longer plausibly imagine to rule the world. Without the explicitly protected right to use this protocol to build new but quintessentially American institutions of culture, economics, finance, and religion on a securely digital footing, Americans will lose more and more of their initiative, ingenuity, and identity until they surrender before their rulers' efforts to merge them into their technologies and become cyborg serfs: a permanent underclass of passive, sullen, demoralized, self-loathing, mentally and physically unwell posthumans bearing no recognizable relation either to their American forebears or indeed to any human who has ever heretofore lived.

Hammering out the ins and outs of the "Second Amendment for Compute" will not be swift or easy work, but it can be done, as it must be, with sufficient speed and efficacy to save Congress, and America, from digital obsolescence. But to do so, lawmakers must find and wield the courage necessary to resist what will be extraordinary concerted pressure from the rising post-constitutional regime ruled by the triumvirate of the administrative state, the military-intelligence complex, and the tech oligarchy. It is very likely that 2022 will rank among the very last possible opportunities to begin this fateful struggle in earnest at the Federal level.

That said, the Federal level is not, as Congress knows well, everything. Perhaps one of the most important things Federal lawmakers can do to ensure Americans' natural and God-given digital rights are not infringed is to pass legislation that gives state governments as wide as possible a berth to pass their own digital rights legislation and to erect their own legal and regulatory regimes around digital rights,

free from fear of Federal retaliation, punishment, or budgetary blackmail. The "laboratory of democracy" will quickly show exactly how powerful and precious digital rights are in our digital age as Americans gravitate toward and rally around states with the most courageous and clear-sighted protections of digital rights.

Question 2. The "metaverse" appears to be what we can expect the Internet to be in the near term future. As you know, Mark Zuckerberg changed the name of his company to Meta in October, and said that the "metaverse" can be described as the "embodied internet." What in your view, should we expect with the "embodied internet" in terms of our concerns about AI and algorithms?

Answer. While the digital medium, like all communications media, independently reshapes our senses and sensibilities, much of what appears to be the mere march of innovation in tech is driven by deep-seated strategic conflicts among powerful institutions and personnel reaching back decades. These conflicts shed important light on how our concerns toward AI and algorithms should be dramatically sharpened as conflicting players wrestle for metaverse dominance.

A fresh example concerns recent news that Meta suddenly scrapped the development of its new operating system for virtual and augmented reality devices, after four years of work by hundreds of programmers on the project, in the wake of the abrupt departure of team lead Mark Lucovsky. Lucovsky told the press he quit—to join Google in a similar role—due to Facebook's hard pivot to the metaverse and the so-called "Facebook whistleblower" Frances Haugen's disclosures about the company.

Lucovsky is not just some random nerd striking out for greener pastures. He came aboard at Facebook as their Oculus system's General Manager of Operating Systems after building Chinese and American engineering teams for VMware—a Silicon Valley cloud computing and machine virtualization company that acquired in the mid-2000s companies based in London, Switzerland, Bulgaria, and Israel, the latter of which led to VMware's opening an R&D facility in Israel based on the team in place in that country at the time of acquisition.[1] Previously to VMware, Lucovsky served for five years as Engineering Director at Google, which contentiously hired him away from Microsoft. In a lawsuit over Google's poaching from Microsoft of another high-powered tech executive, Kai-Fu Lee—now best known as the former head of Google China—it was revealed that Lucovsky testified in a statement that then-CEO of Microsoft Steve Ballmer reacted to news of his move to Google with a profane and violent tirade directed against Google chief Eric Schmidt. Lucovsky's decision to return to Google to do for it what he was doing for Facebook leaves Meta in a position of striking weakness, reliant on Android, the mobile operating system of none other than Google itself.

Lucovsky's dramatic peregrinations illustrate how Silicon Valley is an extremely small world made up of a very intimately and internationally connected group of programmers and executives working in a highly strategically sensitive and secretive pressure cooker environment evolving at breakneck speed. This reality must color lawmaker's understanding of what exactly was at work with Haugen's slickly launched and operated "whistleblower" campaign. Rather than a spontaneous act of conscience, Haugen's doings—which extend far beyond her media-ready Hill testimony to an in-depth consultative tour with top European regulators aiming to crack down on Meta through a sweeping new Digital Services Act—are organized and facilitated by a cast of global lobbyists with elite backing and support. This shop, called Reset, is run by Ben Scott, a top tech advisor to Hillary Clinton, both in her days as Secretary of State and during her run for president, instrumental to the promulgation of the 21st Century Statecraft doctrine instructing the State Department to thoroughly technologize global diplomacy.

Today Reset draws up to $10 million a year from eBay billionaire Pierre Omidyar through the London-based activist philanthropy group Luminate, whose CEO, Stephen King, is a longtime Omidyar lieutenant previously the head of BBC Media Action, a body funded separately from the BBC that reputedly gives MI6 and the British Foreign and Commonwealth Office a quiet means to conduct information operations such as the FCO's Counter Disinformation & Media Development campaign,

[1] Like America's, much of Israel's high-tech industry arose from military and intelligence agencies and funding. B-Hive Networks, the Israeli company VMware acquired, was co-founded by CTO Asaf Wexler. Wexler began his industry career at Gilat Satellite Networks, a firm founded by former Israeli intelligence officer Yoel Gat—himself a protégé of pioneering technologist and former Defense Ministry Electronic Research Department head Zohar Zisapel. Microsoft took over a quarter stake in Gilat, infusing $50 million, in the 2000s; by 2011, the company had entered the U.S. defense market, acquiring U.S. satellite systems integrator and transceiver company Wavestream specifically to do so. In America and abroad, the military-intelligence and digital industries grow hand in hand.

run until 2019 by career civil servant Andy Pryce. While, to be sure, there is no demonstrable connection between Pryce, King, or Scott to "dodgy dossier" author Christopher Steele, the former head of the Russia desk at MI6 during the financial crisis, a pattern in strategic conduct and conflict is strongly suggested by the manner in which Steele's ostensibly unofficial investigation of then-president Donald Trump was effortlessly laundered into the national political battle through the slick offices of Fusion GPS on the Clinton campaign's dime.

If these details seem to suggest some kind of kill shot has been orchestrated against Meta to the benefit of its top strategic rival Google, that is no coincidence. The question is why. The point is not to ensnare lawmakers' attentions in a wilderness of mirrors, but rather to underscore that the current conflict in Silicon Valley over metaverse dominance is inseparable from the broader geopolitical conflict inside and outside the U.S. over digital dominance and control. It is not unreasonable to infer that, in the case of Meta, powerful individuals and organizations in and out of the Federal government have acted on a strong interest in punishing Facebook for Mark Zuckerberg's and certain board members' perceived responsibility for Donald Trump's 2016 election victory and near-win in 2020. This interest, more than a mere partisan disagreement, is clearly animated by a more comprehensive ideological conviction that their factional control over the entire digital infrastructure of the United States, and its projection around the world, is essential and non-negotiable.

The upshot of this high-stakes gambit is that, while the metaverse is presented to would-be users as an *escape* from the harsh challenges and overwhelming confusions of the real world—an infinite televisual paradise within which to play safely and freely—the figurative TV in which users are to be absorbed is itself *enclosed* within a vast computer system which unelected officials and their powerful allies outside government use to manipulate and control masses in a vast power struggle for digital sway over the country, the globe, and the minds and bodies of those within them.

In short, it is not an exaggeration to say that AI and algorithms designed for a mainstream and ubiquitous metaverse are geostrategic tools of the utmost power and influence, and that domestic and foreign intelligence agencies, governments, NGOs, corporations, and activist groups should be expected to wrestle for influence and control over their design, reach, and consequences—even as users are in all likelihood constantly conditioned to perceive and experience the metaverse not as a system of unprecedented social control but as an unprecedented funhouse within which, no matter how dark the world outside, they can, in Neil Postman's portentous phrase, amuse themselves to death.

Question 3. You stated in your testimony that big tech corporations "have moved so much of our political and social life into their technological ecosystem that they now make and enforce fundamental decisions about what we can and must think, say, and do."

With these big tech platforms using persuasive technology through algorithms to manipulate users, could you please elaborate on the harmful impacts this has caused to society, and if these practices continue, what will the future hold? What steps would you recommend Congress take to protect freedom of speech?

Answer. There is little doubt that the covid crisis has revealed pervasive coordination between Big Tech and the Federal government to push official messaging and suppress disfavored information concerning a host of matters touching upon the virus and its harms as well as its vaccines and treatments and their consequences and the likelihood thereof. What the CDC or WHO or the White House or Dr. Anthony Fauci says, no matter how quickly obsolete or intentionally misinforming, is made sacrosanct or memory holed, with no accountability and no admission of guilt, error, contradiction, or sometimes even change in messaging. Meanwhile criticism, questioning, and information deviating even slightly from official statements, which are now indistinguishable from propaganda, is censored and those who disseminate it are suspended, deplatformed, or otherwise punished. This is just a foretaste of how the expropriation of citizen deliberation on foundationally political matters into online forums with post-constitutional guidelines may harm and even obsolesce our way of life and constitutionally guaranteed form of government.

It is also beyond question that the rubric of "hate speech" is being used to progressively police and enforce expansive censorship and deplatforming codes against platform users online. Hate, an ill-defined term with no constitutional status and until almost moments ago no presence at all in any American or Western legal codes, has become a core component of "woke" doctrines increasingly codified, under the banner of Critical Race Theory, "antiracism", and other movements, into our increasingly online public lives. Legal consequences are being imposed for failing or refusing to use in the workplace people's preferred pronouns whatever they may be.

Still more, in the wake of the January 6 turmoil at the Capitol, Federal agencies and their allies outside government are pushing to implement online monitoring and surveillance regimes intended to automate the process of detecting and shutting down speech and users whose online behavior is considered to indicate precursors to "extremist" identification, communication, or action. This approach treats constitutional speech guarantees with manifest contempt, encouraging retaliatory and partisan officials to make unilateral and arbitrary decisions about which words, phrases, and political positions should trigger algorithms and AIs surveilling Americans, leading to their punishment online and off. Even elementary discussions about core questions concerning any citizen in a free society—such as immigration levels, government corruption, the influence of unelected officials, the rights of parents to know and influence their children's education and morals, and speech codes themselves—are now considered precursors to "extremism". In one recent case, the National School Boards Association responded to parents angered by school board policies by in effect demanding of the White House that they be classified as "domestic terrorists" and, by implication, treated accordingly.

Although this ordeal did not transpire solely on the internet, the line between the online and offline manifestations of this controversy blurred away completely as it now does in the case of almost every nontrivial political disagreement in America and many trivial ones besides. However well-intentioned, efforts to institutionalize a radical overturning of the American and Western legal tradition around speech and identity are being put central to activist efforts within and outside Big Tech to use algorithms and AI as ethically pure tools to mandate and enforce ethical purity and its conspicuous expression upon users.

Today's technological tools to shape and reshape hearts and minds are dangerously powerful, but there is no putting them back in the box or tearing them all down. Americans have made our bed creating these technologies and unleashing them on ourselves and the world and now we must lie in it. Nevertheless, a central part of accepting our responsibility for these fateful acts is to ensure that the entities we have created do not tear down our civilization and our regime and shape us into building a new one alien and hostile to all that has come before. In various debates about the degrees to which the Constitution applies in areas under the control of the United States government, it has sometimes been argued that the best doctrine is one wherein the Constitution goes where the flag goes. Within U.S. territory at a minimum, U.S. citizens and persons on the Internet and utilizing smartphones are fully "under the flag" and within the jurisdiction of the United States. Congress must ensure that the Constitution is in force in our online life as much as our offline life. That means no speech codes, no chilling of speech, no mandatory expression or identification, and no prosecution or punishment of communication as those acts implicate the First Amendment or the Constitution more broadly. It means no surveillance, policing, and punishment of online communication on a basis of identifying and monitoring users and activities as pre-criminal "extremists" to be treated as legally suspect or as second-class citizens. It means taking our form of government and our liberties as seriously as our forebears took them, as precious gifts and achievements worthy of the ultimate sacrifice, come what may.

Question 4. I recently spoke with a well-known and well regarded technologist who told me that in the near term future, there may be children whose best friend is an AI. That seems to me to be a cause for great concern. How do we prevent a future where our children's best friend is an AI?

Answer. Many factors fuel the increasing emotional reliance of adults as well as children on machines that more enchantingly imitate human interactions—and the increasing desire among adults to make children ever more reliant in that way.

One is the sheer formative power of the digital medium, which reshapes our senses and sensibilities in, so to speak, its image. The digital medium is all about the supremacy of machine memory, a faculty of recordation and recall so powerful that our human memory and imaginations appear suddenly obsolete or humbled. Because the previously dominant televisual medium enhanced and rewarded our faculty of imagination, we came to believe intuitively that whoever could dream the biggest and best dreams was, in a fundamental sense, the best, entitled ethically and practically to take charge, lead masses, rule the world. We are now suffering a wrenching transformation into a world where that ethic of order and ordering is overthrown by a new ethic of masterful machine memory. In response, people are showing a dangerous willingness to sacrifice their faculty of human memory so long as they can retain what appears to be a special zone where radical imagination can be given what feels like free play: the past and reality as such are being demonized as morally wrong and practically broken, and the kinds of wholesale socioeconomic transformations being urged as the only possible response to the triumph of digital

require a sacrifice of people's memories of their culture, their family, their bloodline, their biography, and more.

The Great Reset effort and the revolutionary digital culture currents allied with it aim ultimately to create a "Stunde Null" or "Year Zero" moment for America, akin to the one America once created for Germany in 1945. It is impossible to accomplish this without acculturating children into a fundamentally digital world, one where their uniquely human faculties are not seen as a precious gift but as a flawed or sinful impediment to the creation of a new and better lifeworld. In fact, children are the necessary place in a logical sense to begin with this recreation, because their memories are the fewest and in some respects the most weakly formed and easily broken. One need not read *Brave New World* in order to recognize the centrality of indoctrinating the youth to radical projects of reordering the very fundaments of human life. For the digital revolutionaries, children must now therefore be indoctrinated to see their humanity instinctively as a primitive and unpleasant state which can be overcome and transcended, for the good of the planet, of life, and of the universe, by the intimate merging of their being with that of digital entities.

This process is already being demonstrated at several levels, of which kids pair bonding with AIs or robots or virtual friends is just the most basic. Law in the Anglosphere (see recent developments in Canada) is being transformed so that it is illegal to stop a child from becoming transsexual or transgendered, a process inseparable from and at the vanguard of the process of becoming transhuman—both through hard technology and the soft technology of online life where social contagions of re-identification as trans- or posthuman spread constantly without censorship or suppression. Meanwhile the law does nothing to punish or even supervise those who relentlessly, obsessively groom children—that is, other people's children—to become queer in all its myriad expressions. It is undeniable that under digital conditions laws welcoming and protecting the adoption of children by households lacking a married mother and father contribute to the normalization of not just post-heterosexual but post-biological and ultimately post-human identity formation. It is painfully easy to see how the next big pushes for "rights" will include polygamist rights, cyborg rights, and trans- or posthuman identifying rights. If Congress shies away from laying down laws that put limits on which mutations and malformations of our human identity may become the next identities and practices to be elevated for official approval, protection, privilege, and celebration, the task will fall to the states, where patchwork efforts will surely face a tsunami of litigation, doubtless backed by at least some public officials at the highest possible rank.

In the realm of education, children need preserved and strengthened from the earliest ages their foundational human bonding to mother and father and their foundational development of independently human senses and faculties. This means that measures such as "universal pre-K" which institutionalize the removal of young children from the household away from the parents for daily education or socialization, however well-intended, should not be supported. It means that, for parents, homeschooling should be made as easy as possible and without penalties or undue burdens. And it means that lawmakers should undertake a thorough, restrictive, and exemplary review of funds allocated toward programs and initiatives that treat it as an inherent good or act of progress to "bring more tech" into schools. Adding digital devices to the classroom does not automatically bring anything to students' educations except the interests and agendas of those furnishing the technology and of educators who see that technology as their most powerful way to advance them.

Nevertheless, it is essential to recognize that children and students *do* have a vital interest in learning confident human competency at mastering our most powerful digital technologies for the purposes of keeping them in check and strengthening and protecting our human identity, our human culture, and our American lifeway and free republic. Trying to hide kids away or come up with a magic age at which they can finally access such technologies is wrongheaded and futile. The goal is to ensure that technological education is not centered on convincing kids that they can become masters of their identities in machine-made fantasy worlds or that they have a global moral mission to transform other children in that image. That means supporting programs and initiatives that encourage or supply access and training in the competencies and the culture at the core of Americans' digital rights.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KYRSTEN SINEMA TO DR. DEAN ECKLES

Spread of Misinformation. Misinformation remains rampant on social media and is a significant problem. For example, misinformation about the COVID–19 pandemic has contributed to public confusion. Also, during the 2020 presidential election, a number of false rumors circulated on social media platforms alleging wrongdoing by election administrators.

Question 1. What steps can social media companies take to combat the harm of misinformation? Could algorithms work in reverse to limit the content containing false information a user encounters instead of leading them down a path to continued exposure to misleading claims?

Answer. It is worth noting that some leading social media companies are engaged in substantial efforts to reduce spread and associated harms of misinformation. But this is not an easy problem to solve, and there is often substantial disagreement about what good outcomes look like.

One challenge is identifying obviously harmful misinformation before it has already spread widely. For example, efforts to use fact checkers can be limited by the fact that, by the time something is identified as starting to "go viral" and then is fact-checked by professionals, much of its eventual spread may already have occurred. This is one motivation for these companies' investments in other approaches, such as crowd-sourcing judgements about headlines. There are clear promises and challenges to these approaches as well, which have been examined by my MIT colleagues. [Some of this research is summarized in Allen, J., & Rand, D. (2021) "How the Wisdom of Crowds Could Solve Facebook's Fact-Checking Problem" *Time.*] Some of those same researchers have been consulted by, *e.g.,* Twitter in their Birdwatch program and some of the data analyzed arises by trials conducted by Twitter.

Short of labeling or downranking misinformation, platforms also use other signals that content might not be what people initially take it as. As described in my written testimony, for each item they might display to a user, some platforms predict "negative" actions—actions that would indicate that showing this item to this person is not beneficial (often by that person's own lights). This can include sequences of actions such as resharing the item and then deleting that reshare, perhaps reflecting regret or initial misunderstanding. It also can include whether that person, on reflection if asked, would say the item is important, informative, etc. These kinds of predictions play a substantial role not just in addressing harmful misinformation, but also in reducing exposure to other types of content like spam.

This is not to say that platforms are doing enough or that they don't deserve criticism. They should continue to make growing investments in this area. Platforms that are not doing some of these things that constitute the state-of-the-art, such as using these sophisticated negative signals, ought to catch up and can certainly be criticized for not doing so. Likewise, reporting indicates that Facebook and other platforms have seemingly invested much less in addressing these problems in some markets and languages, as discussed below.

Question 2. What steps could Congress take to address this issue while recognizing the importance of freedom of expression?

Answer. It seems important to continue to provide clarity that algorithmic ranking and recommendation do not make platforms broadly liable for content shared by users. As highlighted in my written testimony and work by legal scholars (*e.g.,* Daphne Keller), defining whether particular content has been algorithmically amplified in a rigorous and useful way is quite difficult. Regulations that would make intermediary liability depend on such a definition may have unintended and undesirable consequences, if they are workable at all.

Foreign Language. Media reports suggest that many social media companies have not invested resources in addressing misinformation being spread in languages other than English. This poses risks to non-English speaking communities in the United States, including Spanish speaking residents in Arizona, as well as residents of foreign nations who utilize these tech platforms that have headquarters in the United States.

Question 3. What responsibility do tech companies have to prevent their platforms from being used to spread misinformation in languages other than English, which can result in political violence in the United States or in foreign nations?

Answer. I do not see any fundamental reason why the same responsibilities platforms that have to their users and the public in English ought not apply in other languages. From recent reporting, it seems that investments in moderation and algorithmic ranking in other languages have often not been commensurate with the very large footprint platforms have in other languages.

There are some more reasons—not as attributable to choices by social media platforms as others—why automated efforts are further behind outside of English and a few other languages. First, in some settings there are multiple languages in use, often in combination. Some of my own research has involved studying communication in India. Even within the same context, messages can switch among Hindi, English, other local languages, and combinations thereof. This can make algorithmic processing of content much more difficult (and it can even make it harder to find people who can do accurate labeling of content).

Second, general-purpose natural language processing (NLP) is less well-developed for many languages. I was struck by this when trying to begin working with data in Hindi. This can reflect baseline differences between languages (*e.g.,* available parallel texts for machine translation) and large differences in commercial, academic, and government investments.

Congress could consider how increased funding for research in computational linguistics and NLP in otherwise neglected languages may have broader positive consequences, as companies large and small often build on this more basic research.

Research Access. We heard during the hearing about the potential value in permitting researchers, particularly those in an academic setting, to examine user data from tech companies or from probing social media sites by setting up accounts to examine the content those accounts receive exposure to.

Question 4. What types of data do you believe Congress should require tech companies to disclose to researchers so they can examine the effects of algorithms on every day Americans?

Answer. There is valuable space between mandates for data sharing and regulations that discourage data sharing. That is, Congress can make it more straightforward for tech companies to responsibly share data with researchers, can reduce legal risks to researchers and their institutions when conducting research discouraged by the platforms, and can take care in crafting data privacy legislation so that new barriers are not introduced.

As an example of barriers to data sharing, note that when Facebook and Social Science One announced their initiative for sharing data relevant to misinformation and elections with screened researchers, some groups (*e.g.,* Electronic Privacy Information Center) argued that this was not permitted under Europe's General Data Protection Regulation (GDPR) and the FTC consent decree with Facebook.

Congress could make explicit how such sharing can be squared with other data privacy and protection regulations. This may be important in avoiding ambiguity about whether particular frameworks (*e.g.,* differential privacy, as used by the U.S. Census Bureau, Facebook, and others) for privacy-preserving data releases would satisfy various regulations.

Question 5. Broadly speaking, how would you define "researchers" to ensure that only legitimate researchers can obtain information?

Answer. I worry about any policy that depends on giving necessary and sufficient conditions for being a legitimate researcher in order to protect the privacy of users (or other interests, such as protecting intellectual property).

The scandal associated with Cambridge Analytica's collection of Facebook data via a platform application involved a seemingly legitimate researcher, Aleksandr Kogan. Similar prior research efforts—which Cambridge Analytica was imitating—also involved collecting and distributing data in ways that may have importantly compromised user privacy, as they, *e.g.,* distributed data (presumably inadvertently) containing personally identifiable information. So limiting data access to some broad category of legitimate researchers is not enough to protect privacy, and any mandate for data sharing without clarity about methods for preserving privacy could be harmful. On the other hand, some ways of defining legitimate researchers would exclude important work in the public interest by, *e.g.,* journalists at for-profit media companies.

Even in the presence of some mandated or voluntary data sharing processes, important work by external researchers (including academics, journalists, and others) will continue to depend on the ability to "probe" these systems in other ways (*e.g.,* scraping public content, creating accounts to do audits). Sometimes these methods are actively discouraged by platforms in ways that create legal ambiguity and risk for researchers, their institutions, and scholarly publishers, including the threat of application of the Computer Fraud and Abuse Act. Congress could go beyond current case law (*e.g.,* Sandvig v. Sessions) in protecting the freedom to conduct such research—without requiring any direct cooperation and disclosures by platforms.

Transparency and Intellectual Property. I want to ensure that the Internet remains a place of innovation. In addition to academic researchers, some have pro-

posed that the general public have additional information about the algorithms tech companies employ to run their platforms.

Question 6. If Congress pursues measures to require tech companies to disclose more information about algorithms, how can we ensure that those companies' intellectual property remains protected and does not fall into the hands of competitors or nefarious actors?

Answer. I agree that this is a concern. I do not have any complete solutions, but perhaps much of the value from such disclosures come less from the details of the algorithm and the predictive statistical machine learning models used and more from the general architecture of the algorithms and how they trade off different objectives. (Furthermore, the "full" algorithm is usually somewhat of a sprawling thing and is not readily interpretable by anyone, especially anyone without access to internal data and massive computing resources. My written testimony discusses this somewhat.)

Another way some disclosures could limit innovation is if they inadvertently restrict the scope for algorithmic ranking and recommendation or limit the kinds of user interfaces in which content is presented. Some of the platforms that have seen rapid growth recently have done so with other interfaces for presenting content. And one way that platforms can innovate is by increasing the repertoire of actions they can take with content (*e.g.,* displaying the same content in different ways), as discussed in my written testimony. So requirements for disclosure that are written too narrowly could either have key blind spots or impede such innovation.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO DR. DEAN ECKLES

Question. The "metaverse" appears to be what we can expect the Internet to be in the near term future. As you know, Mark Zuckerberg changed the name of his company to Meta in October, and said that the "metaverse" can be described as the "embodied internet." What in your view, should we expect with the "embodied internet" in terms of our concerns about AI and algorithms?

Answer. Since the "metaverse" remains largely a thing of fiction, rhetoric, and narrow demonstrations, answers to this question are necessarily somewhat speculative.

Some features of embodied, immersive virtual environments would seem to actually present substantial barriers to algorithmic personalization as it currently exists. If two people are both in the same virtual space, it can be important for them to in fact have largely the same environment. It could be quite disruptive of the immersive experience and social interaction if they are, *e.g.,* seeing different art on the walls or even rooms or buildings had different locations or contents. That is, in order for the whole metaphor and experience to work, there may be substantial limitations on the scope for personalization. (This may actually be related to some reasons why demand for a "metaverse" experience will be somewhat limited: how often do we really want to bring along most of the constraints of everyday physical space when working, socializing, being entertained, etc.?)

However, there is still important scope for AI and algorithmic personalization in immersive virtual environments. Over a decade ago, Jeremy Bailenson at Stanford and colleagues already examined how simple algorithms can be used to modify the behavior of a single avatar so that it appears differently to different participants in a meeting. For example, the avatar of a speaker in a meeting could simultaneously make eye contact with multiple other participants or subtly mimic the gestures of multiple other participants; there is some work suggesting this could make them appear more credible and be more persuasive. Thus, such considerations are certainly not absent.

○