Atlantic Council
DIGITAL FORENSIC
RESEARCH LAB

Written Testimony of Rose Jackson
Director of the Democracy + Tech Initiative, Digital Forensic Research Lab, Atlantic Council

Before the United States Senate Committee on Commerce, Science, and Transportation
Subcommittee on Communications, Media, and Broadband

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

December 9, 2021

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 US 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.

---

[1] Brooke Auxier, "64% of Americans Say Social Media Have a Mostly Negative Effect on the Way Things Are Going in the US 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/.

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, algorithmic 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 US 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 advertising

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.

[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.

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 US 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 US 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 emails 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.

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-

[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/.

[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/.

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

---

[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.

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 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.

[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 Wollebæk, 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.

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.

"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.

[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/.

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 US state laws on everything from privacy to content moderation. That patchwork of laws sometimes brings *de facto* improvements and protections to US 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 US 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 US 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

[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.

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 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 US 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.

---

[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.

[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_Safety Bill_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/.

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.

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

[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.

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, US leadership is necessary to help drive better global outcomes and ensure we have the ability to make these decisions for ourselves. US 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 US 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 US power is moving in a common, rights-respecting direction.

For **Congress,** prioritizing action around protecting privacy, enabling transparency and accountability, and ensuring the US 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

[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/.

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] Advancing those resources through the Senate would be a significant step forward on privacy and tech governance more broadly. Other efforts, like Chairman Lujan'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.

---

[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.

[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.

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. US 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 US Congress focused on this question, alongside major provisions in the European Union's DSA that mandate data sharing with regulatory authorities and qualified 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 explanability 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

[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.substack.com/p/-some-unsatisfying-solutions-for.

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, 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% of Americans Say Social Media Have a Mostly Negative Effect on the Way Things Are Going in the US 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.

[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.

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 Wollebæk, 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.