Testimony of Alexandra Reeve Givens
President & CEO, Center for Democracy & Technology

For the U.S. House of Representatives Energy & Commerce Committee,
Subcommittee on Innovation, Data, & Commerce
Hearing Entitled "Promoting U.S. Innovation and Individual
Liberty through a National Standard for Data Privacy"

March 1, 2023

Thank you Chair Bilirakis, Ranking Member Schakowsky, and Chair Rodgers and Ranking Member Pallone of the full committee for the opportunity to testify on the importance of data privacy, and the urgent need for Congress to pass a meaningful federal privacy law to protect consumers, create certainty for businesses, and restore trust in the online ecosystem that is so essential to our economy and our society.

I am Alexandra Reeve Givens, President and CEO of the Center for Democracy & Technology, a nonprofit, nonpartisan organization that defends civil rights, civil liberties and democratic values in the digital age. For over two decades, CDT has advocated for Congress to adopt strong privacy protections. We were one of the first organizations to propose a comprehensive privacy framework in the aftermath of the Cambridge Analytica scandal, when it was revealed that the data of almost 90 million Facebook users was collected without their consent by a political consulting firm to create profiles of people to more precisely target political advertising. Even in the short time since then, the public understanding of privacy harms has changed significantly, in part thanks to the work of this Committee and its Senate counterpart. By our count, this is the 31st hearing held in the U.S. Congress on consumer privacy in just the past five years: substantive hearings that have built a rigorous and detailed record about the overwhelming need for a comprehensive federal privacy law. We commend the Committee's focus on this issue early in the new Congress, because it is long past time for Congress to act.

This morning, I plan to briefly describe how the current commercial data ecosystem is harming consumers, how the current legal regime governing online privacy has failed to keep up with innovation, and why the U.S. needs a significant shift in how we protect consumer privacy and the use of consumers' data through passage of a meaningful federal privacy law.

i. How Current Commercial Data Practices Harm Consumers

Looking for information on your device can feel very private, but with every click and scroll, companies collect information about your activities, typically using, sharing or selling that information to make inferences about you or so you can be targeted with ads. A visit to a single webpage can involve hundreds or even thousands of cookies or beacons tracking your activities on that site, both from the company you are visiting ("first party" tracking) and from mostly unknown third parties ("third party tracking").[1] Websites you have visited and search queries you have entered can be collected and shared. In addition to your cellphone provider knowing your general whereabouts, apps on your phone can track and may share your location with anyone willing to pay a price – revealing where you live and work, where you socialize, what doctors you visit, and where you pray to people and companies you have never heard of or interacted with.[2] Those apps may have no business collecting that information except to target advertising. Apps and websites are even fingerprinting your device and web browser to more precisely identify you and to circumvent both technical protections and consent requirements for cookies.[3] Consumers also share an incredible amount of personal and private information

[1] Dan Rafter, *Tracking Cookies: What Are Tracking Cookies and How Do They Work?*, Norton (May 6, 2021), https://us.norton.com/blog/privacy/what-are-tracking-cookies.
[2] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.
[3] Chiara Castro, *Web trackers: What they are and how to protect from them*, TechRadar (June 21, 2022), https://www.techradar.com/features/web-trackers-what-they-are-how-to-protect-from-them ("Browser fingerprint: With cookies getting more regulated - in some countries websites *must* allow users to choose to enable them or not - new tracking techniques are rising. Every browser connected to a certain device brings with it some unique data, including device model, screen resolution, operating system, language,

with different apps and online services, whether it be details about our physical health, our sleep cycles, our mental health, or social messages and family photographs.[4]

All of that data (and inferences companies make about consumers based on that data) can be collected and stored indefinitely by companies, and they can share it with third parties such as data brokers, which are companies that aggregate information about users and market it for, among many things, targeting ads.[5] The huge variety and scale of data points gathered by data brokers allows precise inferences to be drawn about individual users. A 2014 report by the Federal Trade Commision described how data brokers assigned profiles to people based on the detailed information collected across the web, assigning users to categories like "Expectant Parent," "Diabetes Interest" and "Smoker in Household."[6] A 2013 report by the Senate Commerce Committee detailed how dataset titles included categories like "Suffering Seniors," "Rural and Barely Making It," "Ethnic Second-City Strugglers" and "Rough Start: Young Single

---

browsing history, and so on. That defines its own browser fingerprint, which can then be used to track down your online activities every time you open the browser.").

[4] Mozilla, *Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security* (May 2, 2022), https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security (detailing how apps that deal with private consumer information, such as health ailments, routinely have poor privacy practices).

[5] Companies also use the data for fraud detection and credit check services, and sell data to law enforcement. *See* Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, *Legal Loopholes and Data for Dollars*, Center for Democracy & Technology (Dec. 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

[6] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014), at 42-43, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Parents."[7] This Committee explored these concerns in a report as early as 2006, and also held a hearing that addressed data broker practices in 2019.[8]

These data broker practices have not been reined in. A report published by researchers at Duke University just last month revealed that data brokers were selling mental health information, in some cases tied to consumer identities, including whether someone has depression, insomnia, or ADHD, among other medical conditions.[9] Data brokers made available 28 types of medical data, and 42 types of non-medical data about consumers. These categories include data from wearable medical devices, specific medications, income, credit score, Social Security Numbers, and information about children.[10] Data brokers are still grouping people and selling those lists, including specifically a list entitled "Consumers with Clinical Depression in the United States."[11] The logic, said one data broker, is to exploit that data to specifically target people with medical ads based on their illnesses: "households with ailments are more likely to be interested in targeted offers about medical needs."[12]

In addition, advertising trackers can detect specific and often personal information that users share with any given site. Last December, *The Markup* found that, out of the 50 telehealth

---

[7] Staff Report, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, S. Committee on Commerce, Science & Transportation (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

[8] *See* Internet Data Brokers: Who Has Access to Your Private Records?, Hearings Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 109th Cong. (2006); Protecting Consumer Privacy in the Era of Big Data, Hearing Before the Subcomm. on Consumer Prot. and Commerce of the H. Comm. on Energy and Commerce, 116th Cong. (2019). https://www.congress.gov/event/116th-congress/house-event/108942.

[9] Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke University Sanford Cyber Policy Program (Feb. 2023), at 9, https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf ("some firms clearly advertised data already directly linked to individuals, as they offered individual names, addresses, and various forms of contact information (such as phone numbers and emails) in a dataset.").

[10] *Id.* at 20, app'x. B.

[11] *Id.* at 14.

[12] *Id.*

websites they analyzed, 13 of them contained at least one tracker that collected patients' answers to medical intake questions.[13] Trackers on 25 sites told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan.[14] Since then, the U.S. Department of Health and Human Services has clarified that use of tracking technologies like cookies by entities covered by the Health Information Portability and Accountability Act (HIPAA) are subject to the HIPAA privacy and HIPAA security rules.[15]

When consumers learn about these practices and how careless companies are with consumer data, they are often gravely offended. But the issue is about more than just offensive stereotyping or privacy leakage – it can lead to social, psychological, and economic harm. It might not seem that important if a person is targeted with particular clothing ads. But it does matter when predatory lenders, for example, can hyper-target an audience that is vulnerable to payday loans and exploitative interest rates, as has happened with veterans and families navigating medical crises.[16] It matters when ads for diets and dangerous weight loss medications can persistently target people with histories of disordered eating, leading to depression and

---

[13] Todd Feathers, Katie Palmer, & Simon Fondrie-Teitler, *"Out of Control": Dozens on Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, The Markup (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[14] *Id.*

[15] *See* Department of Health and Human Services, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (HHS/OCR December Bulletin highlighting the important privacy obligations health providers - such as doctor's offices and hospitals - are required to follow when using apps and websites, under the Health Information Portability and Accountability Act, which limits how your doctor or insurer can share patient health information).

[16] Office of Representative Katie Porter, *AWOL: How Watchdogs are Failing to Protect Servicemembers from Financial Scams* (2021), https://porter.house.gov/uploadedfiles/va_home_loans_final.pdf; Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, Duke U. Sanford Cyber Policy Program (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf. *See also* Coulter Jones, Jean Eaglesh, & AnnaMaria Andriotis, *How Payday Lenders Target Consumers Hurt by Coronavirus*, Wall Street Journal (June 3, 2020), https://www.wsj.com/articles/how-payday-lenders-target-consumers-hurt-by-coronavirus-11591176601.

self-harm.[17] It matters when scammers can target their ads to seniors who are more likely to fall for schemes hawking low-cost medical devices.[18] It matters when inferences about people are used to unfairly target ads for jobs, housing or credit, the gateways to economic and social opportunity.[19]

Even when online platforms prevent advertisers from targeting audiences on their platform using explicit protected categories such as race, gender or age, research has shown how easily "interest categories" and other means of audience targeting can serve as proxies for those characteristics.[20] We have long known that zip code can be a proxy for race,[21] but so can a person's identified interest pages, the websites they have visited, or their likes. To give just one example, it is easy to determine someone's religion from the Facebook pages they have liked, which will often denote the church or faith community to which they belong.

Other harms can result from loose commercial data practices. In 2018, it was revealed that a fitness app was inadvertently revealing secret information about the location and layouts of U.S. military bases because personnel were recording their exercise regimes and sharing it with the application. Following a public outcry, the company made changes to its platform, and I am sure military personnel now receive stronger briefings on privacy protections. But the example

---

[17] Liza Gak, Seyi Olojo, & Niloufar Salehi, *The Distressing Ads That Persist: Uncovering The Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating* (2022), https://doi.org/10.48550/arXiv.2204.03200.
[18] AARP, *Medical Equipment Scams* (Mar. 2022), https://www.aarp.org/money/scams-fraud/info-2019/medical-equipment.html.
[19] *See* Dept. of Justice, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising* (June 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.
[20] Till Speicher *et al.*, *Potential for Discrimination in Online Targeted Advertising*, Proceedings of Machine Learning Research, Conference on Fairness, Accountability, and Transparency (2018), http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf.
[21] Madeline St. Amour, *ZIP Codes and Equity Gaps*, Inside Heigher Ed (July 2020), https://www.insidehighered.com/news/2020/07/09/report-finds-racial-equity-gaps-college-attendance-debt-and-defaults-based-zip-codes.

illustrates the revealing nature of location information, and the inadequacy of requiring users to be the sole guardians of their privacy, when it is often hard for users to know how an app will collect, use, or share their data with the world.

Security experts and members of this Committee have raised additional concerns over the national security effects of sharing data with other countries, including China. The permissive nature of the current U.S. privacy framework allows for data to be collected and shared by companies with impunity, which could be helped by imposing substantive guardrails on commercial data practices through federal privacy reform.

ii. The Need for Comprehensive Federal Privacy Legislation

While some companies have taken important steps to protect their users' privacy, the lack of a comprehensive federal privacy law is leaving consumers open to exploitation and abuse. Under current law, Americans' primary comprehensive privacy protections are based on the Federal Trade Commission's limited Section 5 authority over unfair and deceptive practices. Under Section 5, the primary mode of enforcement has relied on a theory of notice and consent, under which companies can set their own privacy rules and collect whatever data they like provided they disclose it to their customers.

Any modern user of technology can understand why this "notice and consent" approach is inadequate. Companies typically give notice to consumers through long privacy policies, often buried deep within the fine print of their terms of service. One academic study showed that a person would need to spend 244 hours to read all the privacy policies they encounter in a single year.[22] Even if a consumer does read and understand the privacy policies, their choices are

[22] Aleecia M. Mcdonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society (2008), https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf; Geoffrey A. Fowler, *I Tried to*

limited: either accept the service's terms, or do not use it. But many online services like internet service providers and social media companies are such an important part of everyday life that quitting is effectively impossible—and often there are few, if any, alternatives to use instead. If a social media service is the only way a consumer stays in touch with family and friends, asking them to quit is unreasonable.

Nor are countless pop-up windows asking a user to "accept or reject" a company's privacy practices the answer, as Europeans have found after the European Union's passage of the largely consent-based General Data Protection Regulation (GDPR). Users find these pop-up windows annoying and hard to navigate, and companies often establish default settings that funnel users into accepting less privacy-protecting options.[23] There is a rich academic literature about dark patterns, the ways in which privacy notices, consent boxes, and other design elements of a website or app can nudge consumers to accept certain policies through design choices intended to induce consent, even when the consumer would otherwise take the more privacy-protective action.[24] Dark patterns include misleadingly positive language, omitting details of how a person's data will be used or shared, or adding friction to privacy interfaces that make it hard for users to find how to change their settings.[25]

Read All My App Policies. It Was 1 Million Words, Wash. Post (May 31, 2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/.

[23] Colin M. Gray *et al.*, *The Dark (Patterns) Side of UX Design*, Proceedings of the 2018 CHI Conf. on Human Factors in Computing Systems, Paper 534, at 5 (2018), https://dl.acm.org/doi/pdf/10.1145/3173574.3174108 ("Nagging behaviors may include pop-ups that obscure the interface, audio notices that distract the user, or other actions that obstruct or otherwise redirect the user's focus.").

[24] *See, e.g.,* Jamie Luguiri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. Legal Analysis 43 (2021), https://academic.oup.com/jla/article/13/1/43/6180579; Lauren E. Willis, *Deception by Design*, 34 Harvard J. L. Tech 116 (2020), https://jolt.law.harvard.edu/assets/articlePDFs/v34/3.-Willis-Images-In-Color.pdf; Johanna Gunawan, Amogh Pradeep, David Choffness, Woodrow Hartzog, and Christo Wilson, *A Comparative Study of Dark Patterns Across Mobile and Web Modalities*, Proceeding of the ACM on Human-Computer Interaction, https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Gunawan-Pradeep-Choffnes-Hartzog-Wilson-A-Comparative-Study-of-Dark-Patterns-Across-Mobile-and-Web-Modalities.pdf.

[25] Federal Trade Commission, *Bringing Dark Patterns to Light* (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

Against this backdrop, it is no surprise that consumers have lost trust in online companies.[26] Consumers are worried about their data and their privacy online, but are powerless to control that privacy.[27] They know they are being tracked by companies.[28] Consumers also have little confidence that companies will admit when they misuse data.[29]

This lack of trust is bad for the economy, for businesses, and for consumers, as they feel powerless and like their only recourse is to simply stop using certain products and services—which many have.[30] But it doesn't have to be that way. Consumers have been asking for years for the government to protect their privacy.[31] It is time to heed that call.

---

[26] *See, e.g.*, Orson Lucas, *Corporate Data Responsibility: Bridging the Consumer Trust Gap*, KPMG (Aug. 2021), at 1, https://advisory.kpmg.us/articles/2021/bridging-the-trust-chasm.html (stating that 40% of consumers do not trust companies to use their data ethically).

[27] *See e.g.*, Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (81% of consumers say they lack control over what types of data companies collect; 81% say the risks of companies collecting data outweigh the benefits; 59% say they lack understanding of how companies use data); *Most Americans say it is increasingly difficult to control who can access their online datai,* Ipsos (Jan. 2022), https://www.ipsos.com/en-us/news-polls/data-privacy-2022 ("Seven in ten (70%) Americans agree that controlling who can access their online personal information has become more challenging").

[28] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans concerned, feel lack of control over personal data collected by both companies and the government*, Pew Research Center (Nov. 2019), https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/ (72% think all or mostly all of what they do online is tracked by companies).

[29] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (79%).

[30] *Most Americans Say it is Increasingly Difficult to Control Who Can Access Their Online Data*, Ipsos (Jan. 7, 2022), https://www.ipsos.com/en-us/news-polls/data-privacy-2022 (36%).

[31] Privacy for America, *New Data Reveals Americans' Overwhelming and Bipartisan Support for Federal Privacy Legislation* (Nov. 18, 2021), https://www.privacyforamerica.com/new-data-reveals-americans-overwhelming-and-bipartisan-support-for-federal-privacy-legislation/ (stating 92% of voters want a privacy law).

iii. Elements of a Comprehensive Federal Privacy Law

Congress can make the U.S. a global leader by passing meaningful comprehensive privacy legislation, building on the foundational work of this Committee, its Senate counterpart, and Republican and Democratic administrations over more than a dozen years.[32] The most important thing Congress can do is free consumers from a regime that primarily relies on notice-and-consent as a privacy protection. We need privacy laws that work in the 21st century digital economy, that give consumers the baseline protections they need and create clear rules of the road for businesses. As discussed below, we also need to ensure any privacy law can be effectively enforced.

There are several elements of a federal privacy law that would address the harms I have discussed today and significantly increase consumer trust:

- Data minimization requirements that restrict companies to collecting and using only data that is necessary for the services they perform,
- Specific protections for sensitive data such as biometric information, location information, health information, or information revealing someone's race, religion, sexual orientation, and similar factors,
- Civil rights protections and algorithmic transparency and assessment provisions to prevent companies from discriminating against people based on protected characteristics,
- Data security requirements ensuring that companies take steps to avoid data breaches and other unauthorized access to data,
- The rights for consumers to access, correct, delete, and port data pertaining to them that is held by a company,
- Effective, easy-to-use mechanisms for consumers to opt-out of targeted advertising,

[32] Congressional Research Service, *Privacy Protections for Personal Information Online* (April 2011), https://www.everycrsreport.com/files/20110406_R41756_d4893c5a84e54603899b9471b9d853219c03424a.pdf. ("Beginning with the 109th Congress, every Congress has held numerous privacy-related hearings. The current Congressional privacy agenda is broad and includes items that Congress has worked on for several years, new issues posed by advances in technology, and items related to efforts to update the electronic surveillance laws for advances in technology.").

- Children's protections that take into account the inability of children to protect themselves against exploitative data practices,
- Limits on sharing or selling data with third parties, including a national registry for data brokers and the right for consumers to delete data about them held by a data broker, and
- Meaningful enforcement by the Federal Trade Commission, state Attorneys General, and a private right of action.

Last year, this committee passed in an overwhelmingly bipartisan fashion the American Data Privacy and Protection Act (ADPPA), which includes all of these protections and more. CDT commends the Committee for its tireless work on that bill. To be clear, it is not a perfect bill. For instance, we would like to see narrower preemption of state laws and a broader private right of action, and higher penalties for data brokers failing to register. But we recognize that to ensure bipartisanship, compromise is necessary. ADPPA represents a reasonable middle ground for protecting privacy and civil rights online, and we encourage this Committee to take it up again without delay.

iv. Ensuring Meaningful Enforcement

It is essential that any privacy law passed by Congress can be meaningfully enforced and can keep up with rapidly changing innovations in commercial data practices. Given the complexity and scale of the modern digital ecosystem, this can be achieved only through a complementary approach that empowers the Federal Trade Commission, State Attorneys General, and a private right of action for consumers to enforce their rights.

The expert staff of the FTC is well positioned to bring cases involving data privacy harms. Congress should ensure, however, that the FTC is properly resourced to handle enforcement of a new privacy law. Investing in the FTC is good for consumers who receive more money in refunds

from FTC enforcement,[33] and good for the federal government because, according to an analysis from the Congressional Budget Office, every dollar invested in the FTC reduces the deficit by over three dollars.[34] Congress should also ensure the Commission provides resources to help businesses understand their obligations and pursue responsible data practices, for example by staffing a resource center.

Even with greater resources, federal enforcers cannot possibly keep up with the entire ecosystem of commercial data practices. State Attorneys General can and should play an essential role in protecting consumers' privacy, building on the existing expertise many have demonstrated in fraud, privacy, data security, and digital civil rights. In addition to bringing enforcement actions, Attorneys General frequently work with business leaders and advocacy organizations to identify concerns about products and services and to develop best practices, playing a vital role in protecting consumers' interests.[35] Finally, a private right of action is essential. Even with multiple levels of government enforcers, resource constraints will limit effective application of the law. Consumers should have the ability to be made whole through the court system if their issues are not taken up by government enforcers. A private right of action would help ensure that people's wrongs can be made right.

---

[33] Since 2018, for every dollar invested in the FTC, consumers have been refunded $2.44. *See* Federal Trade Commission, FTC Appropriation and Full-Time Equivalent (FTE) History, https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation (showing FTC funding betwee 2018 and 2022 at $1.675 billion); Federal Trade Commission, *Data on Refunds to Consumers*, https://public.tableau.com/app/profile/federal.trade.commission/viz/Refunds_15797958402020/RefundsbyDate (showing total refunds between 2018 and 2022 at $4.1 billion).

[34] Congressional Budget Office, *Estimated Budgetary Effects of Title III, Committee on Energy and Commerce, H.R. 5376, the Build Back Better Act* (Nov. 18, 2021), https://www.cbo.gov/publication/57623 (showing that a $1 billion investment in the FTC over the course of ten years equates to a reduction in the deficit by $3.1 billion).

[35] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 759 (2016). *See also* Senate Commerce Committee, Testimony of Laura Moy (Oct. 10, 2018), at 12-13, https://www.commerce.senate.gov/services/files/baf68751-c9bc-4b15-ab0f-d4a5f719027c.

v. Why Congress Must Also Address AI and Automated Decision-Making

A final issue I would like to highlight is the need to address artificial intelligence and automated decision-making. Increasingly, AI systems that leverage large amounts of data are being used in decisions about employment, lending, tenant screening and other settings that can dramatically impact people's lives.[36] These tools raise significant risks of bias, lack of transparency, and unfair decision-making. In particular, these issues come up when tools evaluate people based on factors that do not actually relate to the decision in question (causing hidden errors and unfair outcomes), or when they make inferences about people that approximate protected characteristics such as race, gender, religion, or disability status (perpetuating bias and discrimination).

The ADPPA takes a meaningful step in the right direction. It increases transparency into algorithmic systems, used by large data holders, to help people, regulators, legislators, and others to understand what the purpose of the AI system is, how it was designed, and the steps the company has taken to mitigate various foreseeable harms. More public and detailed information will better inform policymaking going forward.

Thank you very much for your time and I look forward to your questions.

[36] *See, e.g.*, Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms; Pranshu Verma, *AI is Starting to Pick Who Gets Laid Off*, Wash. Post (Feb. 20, 2023), https://www.washingtonpost.com/technology/2023/02/20/layoff-algorithms/.