CENTER FOR
DEMOCRACY
& TECHNOLOGY

Testimony of Samir C. Jain
Vice President of Policy, Center for Democracy & Technology

For the U.S. House of Representatives Energy & Commerce Committee,
Subcommittee on Innovation, Data, & Commerce
Hearing Entitled “Legislative Solutions to Protect Kids Online and
Ensure Americans’ Data Privacy Rights”

April 17, 2024

Thank you Chair Bilirakis, Ranking Member Schakowsky, and Chair McMorris Rodgers and Ranking Member Pallone of the full committee, for the opportunity to testify today on the importance of protecting data privacy and kids online, and the urgent need for Congress to finally pass a meaningful federal privacy law to protect individuals, create certainty for businesses, and restore trust in the online ecosystem.

I am Samir Jain, Vice President of Policy for the Center for Democracy & Technology, a nonprofit, nonpartisan organization that defends civil rights, civil liberties and democratic values in the digital age. For almost three decades, CDT has advocated for Congress to adopt strong privacy protections. Dozens of Congressional hearings have built a detailed record demonstrating the clear need for a comprehensive federal privacy law. This Committee in particular has, to its great credit, done prodigious work on a bipartisan basis both to define the contours of the problem and to develop constructive solutions. Less than two years ago, of course, this Committee overwhelmingly passed the American Data Privacy and Protection Act (ADPPA). Although that bill never received a floor vote, the American Privacy Rights Act (APRA) that we will be discussing today builds on that prior work—on both a bipartisan and bicameral basis—and presents a renewed opportunity to finish the long overdue job of passing a federal privacy law. A baseline set of privacy protections for all would in turn provide both a context in which to also include further protections for kids and a necessary foundation for addressing artificial intelligence (AI).

I. The Need for a Comprehensive Federal Privacy Law is Clear.

Today's data ecosystem is out of control. Nowadays, companies follow you (and everyone) around the internet everywhere you go, collecting and retaining detailed information on what websites you visit and what you do there, who you communicate with, and what search queries you enter. Apps on your phone track nearly everything you do on your device, including your precise location – revealing where you live and work, where you socialize, what doctors you visit, and where you worship, both to the company directly collecting that information and further to people and companies you have never heard of or interacted with. Individuals also reveal information about themselves as they interact with online services and apps, ranging from personal photographs and messages to physical and mental health information shared through search queries or fitness and mental health-related apps.

All of that data and much more is commonly used for a variety of purposes, but is also often used to make inferences about you, shared, and/or sold so you can be targeted with ads and for other purposes that you did not expect or intend. Telehealth sites may have trackers that collect and reveal patients' answers to medical intake questions or that they have added an item like a prescription medication to their cart.[1] Predatory lenders can use individuals' data to hyper-target an audience that is vulnerable to payday loans and exploitative interest rates, as has

[1] 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.

happened with veterans and families navigating medical crises.[2] Scammers can use personal information they collect or purchase to target their ads to seniors who are more likely to fall for schemes hawking low-cost medical devices.[3] As this Committee knows through its prior work, the examples are legion.

Americans are well aware that they are the victims in this ecosystem. According to Pew Research Center, 81% of consumers say they lack control over what types of data companies collect and that the risks of companies collecting data outweigh the benefits.[4] Another poll found that 70% of "Americans agree that controlling who can access their online personal information has become more challenging."[5] Thus, it is hardly surprising that 92% of voters want a federal privacy law.[6]

The explosive emergence of artificial intelligence and related systems has accelerated the need for a privacy law. Data collection has run rampant in the digital age in large measure because companies have economic incentives to amass large pools of data, such as reaching desired audiences for ad campaigns by profiling people and using data to target advertising based

[2] 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.

[3] AARP, *Medical Equipment Scams* (Mar. 2022), https://www.aarp.org/money/scams-fraud/info-2019/medical-equipment html.

[4] 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/.

[5] *Most Americans say it is increasingly difficult to control who can access their online data,* Ipsos (Jan. 2022), https://www.ipsos.com/en-us/news-polls/data-privacy-2022.

[6] 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/.

on people's behavior. The need for large datasets to train AI systems provides yet another reason for companies to collect or repurpose extensive data about everyone online, even if they have not yet determined the purposes for which the systems will be used or particular data necessary for those purposes. Generative AI presents a heightened risk of widespread data scraping to power these systems.

The power of AI also threatens to exacerbate the harms stemming from collection and processing of data. The ease, speed, and scale with which AI functions will make personalized content more frequent, intrusive, and harmful. For instance, an AI system may flag a consumer researching weight loss, and then may target that person with any number of personalized predatory ads ranging from harmful drugs to extreme diets, all without the company or the individual knowing how it happened.[7] Generative AI and applications such as chatbots can effectively "memorize" personal information contained in the training data.[8] If left unchecked, this memorization can result in such personal information being included in the output of generative AI systems and revealing such information to unauthorized third parties. Moreover, the prompts and other information that users enter when interacting with generative AI applications can reveal personal details, especially when the design of a chatbot encourages more detailed or intimate "conversations" about health or other personal subjects than the mere entry of a search term. A privacy law is needed not only to protect individuals from privacy-related harms, but also to engender the trust necessary to promote the adoption and use of AI.

Finally, a comprehensive federal privacy law is also a national security and foreign policy imperative. Today, adversary nations can easily collect or purchase detailed information about

[7] *See generally* 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*, Vol. 6, Proceedings of the ACM on Human-Computer Interaction, Art. 377 at 11 (2022), https://arxiv.org/pdf/2204.03200.pdf.

[8] Nicholas Carlini, *et al*., *Extracting Training Data from Large Language Models* (Jun. 15, 2021), https://arxiv.org/pdf/2012.07805.pdf.

Americans from data brokers and use that data for purposes including training their AI models and targeting Americans with personalized content such as disinformation. Through data minimization, restrictions on data brokers, user rights to access and deletion, and other protections, Congress can substantially curtail those threats. Further, the absence of a federal privacy law puts the United States on its back foot as it tries to lead globally on technology policy. We cannot plausibly claim to have a coherent model for technology regulation that others should follow and adopt when we lack a basic building block that China, Europe, and other leading countries all have. Passing a federal privacy law will put the United States in a much better position to influence other countries to adopt a model for technology regulation that respects people's rights and reflects democratic values.

II. APRA Provides a Sound Framework for a Comprehensive Privacy Law

APRA builds on the many prior privacy bills from both parties and includes critical elements necessary for an effective privacy law: data minimization, effective consumer rights, prohibition of discrimination, restrictions on data brokers, requirements for data security, and an enforcement regime with complementary roles for the Federal Trade Commission (FTC), state Attorneys General, and individuals.

Data minimization. Data minimization—the principle that companies generally should only collect and process data necessary to provide the product or service the individual requested—is an essential element of effective privacy legislation. For too long, we have relied on notice and consent, premised on the fiction that individuals review lengthy privacy policies and make informed choices. We know that people do not spend the literal hundreds of hours they would need to read all the privacy policies they encounter in a single year.[9] Nor do they generally

[9] 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;

have meaningful choices: often the only choice is to accept the proffered terms or not use the service at all, an unreasonable choice when online services play such a central role in everyday life.

The time has come to shift the primary privacy burden away from individuals and instead place it on the companies that collect and profit from people's data. APRA's data minimization provisions would do just that by requiring companies to justify their data collection and processing as being "necessary, proportionate, and limited to provide or maintain . . . a specific product or service requested by the individual to whom the data pertains" or for a list of other enumerated permissible purposes. APRA would also provide additional opt-in consent protections for transfers of "sensitive covered data," with additional restrictions on permissible purposes for use, retention, and transfer of specific highly personal types of sensitive data such as biometric and genetic information.

Enacting data minimization would mark a fundamental change to our current data ecosystem, which is currently characterized more by data *maximization*. As discussed above, companies have incentives to collect and hoard massive amounts of data to develop detailed individual profiles to target advertising, to train AI systems, and just in case it becomes useful for some other purpose. Those large data stores become targets for hackers and data breaches that result in downstream harms like identity theft, reputational damage, or some other type of injury.[10] Data is further sold to and compiled by data brokers, who in turn transfer the data to innumerable third parties for uses well beyond what an individual knew about or wanted. We

Geoffrey A. Fowler, *I Tried to 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/.

[10] Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 Boston U. L. Rev. 793 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222.

need to bring this unbridled data market under control by imposing a data minimization obligation.

Civil rights. 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 affect people's lives and livelihoods.[11] As the National Institute of Standards and Technology (NIST) has explained, one of the key characteristics of a trustworthy AI system is that it be fair and avoid harmful bias and discrimination.[12] APRA would prohibit using data in a way that perpetuates or exacerbates discrimination based on protected characteristics such as race, sex, religion, or disability status, whether a Black person looking for a job, a woman seeking a loan to start a business, or a veteran with a disability trying to find housing. It also would increase transparency into algorithms used by large data holders to help regulators and Congress to understand what the purpose of the algorithm is, how it was designed, and the steps the company has taken to mitigate various foreseeable harms. Such information is necessary to improve policymaking on AI going forward, as well as companies' and customers' understanding about whether an AI system is functioning fairly and well.

Consumer rights. APRA would provide consumers with basic rights over their data, including the ability to access, delete, and correct data about them held by covered entities. At this point, these rights are table stakes for any meaningful privacy law and not new to companies,

[11] *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/.

[12] Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST, Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf; NIST Special Publication 1270, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence* (2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

particularly given that almost every state privacy law has included some form of these rights.[13] APRA would also permit consumers, where technically feasible, to require covered entities to export their data in human- and machine-readable forms. Such data portability would help promote competition by allowing consumers to switch from one online service to another without the obstacle of having to "start over" or to reconstruct their data in a more laborious fashion.

Restrictions on data brokers. The expansive data broker industry is built on purchasing and collecting numerous types of personal data from a variety of sources and selling or otherwise providing that data to third parties. As the industry has grown, so has the severity of privacy- and data-related harms to consumers.

The harms for data broker practices have been well known for years. A 2014 report by the FTC described how data brokers assigned profiles to people based on detailed information collected across the web, assigning users to categories like "Expectant Parent," "Financially Challenged," "Political Leanings," and "Thrifty Elders."[14] A 2013 report by the Senate Commerce Committee detailed how datasets included categories like "Suffering Seniors," "Rural and Barely Making It," "Retiring On Empty: Singles," and "Rough Start: Young Single Parents."[15] These reports called for increased transparency and accountability, but nothing in our federal legal regime has changed.

[13] IAPP, U.S. State Privacy Legislation Tracker 2024, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf (last updated April 8, 2024).

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

[15] 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.

Just last year, this Committee held another hearing on data brokers. Testimony described how:

> Brokered data is widely available; purchasable at low cost; often sold by brokers with little to no vetting; and can be used to profile, track, and target consumers, including people in marginalized communities, veterans, military servicemembers, government employees, first responders, elderly Americans, people with Alzheimer's, students, and teenagers.[16]

Data brokers have used data of elderly people and people with Alzheimer's disease to create lists of people who are more vulnerable to scams.[17] Researchers have found that numerous mental health apps share sensitive data about users' depression, anxiety, suicidality, victimization by domestic violence, disordered eating, post-traumatic stress disorder, and other mental health conditions.[18] Data brokers collect and sell information about members of our military.[19] They compile information about our driving habits from automakers and others and provide them to insurance companies.[20] Data brokers also sell information to law enforcement and intelligence agencies and thereby allow those agencies to evade the warrant or other legal process that would

[16] Justin Sherman, "Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security," *Testimony Before U.S. House Committee on Energy and Commerce* (Apr. 19, 2023), https://d1dth6e84htgma.cloudfront.net/Sherman_Testimony_4_19_23_b40d947a8e.pdf?updated_at=2023-04-17T17%3A40%3A42.415Z.

[17] Alistair Simmons, *The Justice Department's Agreement With a Data Broker That Facilitated Elder Fraud*, Lawfare Blog (Nov. 7, 2022) https://www.lawfareblog.com/justice-departments-agreement-data-broker-facilitated-elder-fraud.

[18] 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/; *see also* Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke University Sanford Cyber Policy Program (2023), 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 (data brokers sell people's mental health and medication data with demographic and other non-medical data, grouped into lists such as "Anxiety Sufferers" and "Consumers with Clinical Depression in the United States" to target advertisements related to these mental health conditions).

[19] Justin Sherman, et al, *Data Brokers and the Sale of Data on U.S. Military Personnel* (Nov. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf.

[20] Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, New York Times (Mar. 13, 2024), https://www nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html.

otherwise be required for those agencies to collect that information directly.[21] Even while collecting all this sensitive information, many brokers have poor security practices that have led to breaches exposing information of tens of millions or even a billion people.[22]

Through all of this activity, data brokers generate substantial streams of revenue. The global data broker market was valued at an estimated $254 billion in 2022.[23] Meanwhile, the people whose data fuels this shadowy industry have little or no visibility into which data brokers obtain their data, from whom their data is obtained, to whom their data is sold, and to what additional uses their data is put, and they are powerless to scrub their data from the brokers that have obtained it.

APRA would, finally, start to rein in this activity. Its data minimization provisions would significantly reduce the amount of personal data being collected and sold through this ecosystem. Moreover, it would start to give individuals greater visibility and control by, among other steps, establishing a publicly available data broker registry in which data brokers would be required to provide basic identification and contact information and through which a person could submit a request to all registered data brokers (other than consumer reporting agencies under the Fair Credit Reporting Act) to no longer collect covered data about the person without affirmative express consent unless the broker was acting as a service provider. Another bill under consideration in this hearing, the DELETE Act, would go a step further and establish a centralized mechanism through which individuals also could seek to have all data brokers delete

[21] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, Center for Democracy & Technology, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers* 19 (2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

[22] Justin Sherman, *Data Brokers and Data Breaches*, Duke Sanford School of Public Policy (Sept. 27, 2022), https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/.

[23] Data Broker Market - Global Industry Size, Share, Trends, Opportunity, and Forecast, 2018-2028 (Nov. 2023), https://www researchandmarkets.com/report/data-broker.

information about them, a requirement we support. In addition, the House will soon be voting on the Fourth Amendment is Not for Sale Act,[24] which would prohibit law enforcement and intelligence agencies from purchasing information from data brokers in place of obtaining required legal process. We urge Congress to pass this legislation as an initial but critically important step. These types of limitations and controls on data broker activity are long overdue.

Data security. One way in which the collection of large stores of personal information can give rise to harm to a large number of individuals is through unauthorized access to that data, whether by insiders or as a result of a data breach by an outside party. According to one report, over 2.6 billion personal records were breached in 2021 and 2022, and in just the first nine months of 2023, 1 in 4 people in the United States had their health data exposed in a data breach.[25]

Although the FTC has brought enforcement actions in the context of certain breaches, there are currently no generally applicable federal rules establishing a data security standard. States, at best, have an incomplete patchwork of laws. Here again, a meaningful federal data security standard that applies to all companies is sorely needed. APRA would provide that, requiring covered entities and service providers to have reasonable data security practices, keyed to factors such as their size.

Effective enforcement: A privacy law cannot be effective without meaningful enforcement provisions that can operate at the scale of the online digital ecosystem. APRA would achieve that goal through a complementary approach that provides enforcement authority

[24] H.R. 4639, 118th Cong. (2023).

[25] Stuart E. Madnick, *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase* (Dec. 2023), https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf; Faustine Ngila, "One in four Americans have had their health data compromised this year," Quartz (Oct. 20, 2023), https://qz.com/hackers-heath-data-hospitals-california-ransom-breach-1850942235.

to the FTC and state officials such as State Attorneys General, as well as a limited private right of action.[26]

The FTC has an established history of bringing cases involving data privacy harms and the expertise necessary to handle enforcement of a new privacy law. Members of Congress should not let any short-term dissatisfaction with the agency cloud their judgment about enforcement—the FTC has the jurisdictional expertise needed to enforce the bill and help businesses and consumers alike interpret its provisions. Relatedly, Congress should ensure that the FTC is properly resourced to carry out those responsibilities given the size and scope of the laws it is tasked by Congress to enforce. Providing those resources will not only help ensure that the privacy law is effective, but also would be a good investment: according to an analysis from the Congressional Budget Office, every dollar invested in the FTC reduces the deficit by over three dollars.[27]

Even with greater resources, the FTC cannot possibly keep up with the entire ecosystem of commercial data practices. Accordingly, state enforcers should play an active role in enforcing this privacy law, as many have already begun doing with their own privacy laws. Here again, State Attorneys General and other state regulators have existing expertise in fraud, privacy, and data security and are well-positioned to investigate and bring enforcement actions when necessary to protect their citizens.[28]

[26] Elysa M. Dishman, *Enforcement Piggybacking and Multistate Actions*, 2019 BYU L. Rev. 421, 424, 430 ("The multienforcer system provides accountability by allowing other enforcers to step in to remedy lackluster enforcement resulting from problems of agency capture, resource constraints, informational disadvantages, and political impediments.... When all enforcers focus their resources and efforts on large corporate targets, it deprives enforcement resources from other targets that may cause more localized harm but lack the deep-pockets to pay large fines or create splashy headlines.").

[27] 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).

[28] *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 748-51, 755-57 (2016).

Even with federal and state enforcement, resource constraints will limit effective application of the law. Individuals should have the ability to be made whole, or to stop harmful and illegal practices, through the court system if government actors do not have the resources or desire to take up their claims, just as they do under other laws regarding consumer protection, civil rights, competition, worker protection, and numerous other areas. A private right of action will provide for redress for harms suffered by individuals, create incentives for companies to engage in privacy-protective behaviors to minimize the risk of those harms from occurring in the first place, and help to engender trust in the online digital ecosystem.

III. APRA Will Need Refinement in Certain Areas.

While APRA's basic framework is strong, as a discussion draft, it will need further refinement as it moves through the legislative process. Some of those refinements include the following:

Protections for kids. A comprehensive privacy bill that establishes baseline protections for everyone is the right context in which to consider what additional protections are needed for kids. Protecting children's privacy is particularly important because children—especially younger children—are less able to understand the difference between advertising and editorial content,[29] are unable to provide informed and meaningful consent, and may be particularly susceptible to some of the harms that can arise from targeted advertisements, such as ads for diets and dangerous weight loss medications that target teens with histories of eating disorders.

The Children's Online Privacy Protection Act (COPPA) already provides some protections for kids, and it is due for an update along the lines that the Children and Teens' Online Privacy Protection Act (COPPA 2.0) would provide. APRA treats information about kids

[29] FTC Staff Paper, *Protecting Kids from Stealth Advertising in Digital Media* (Sept. 2023), https://www ftc.gov/system/files/ftc_gov/pdf/p214505kidsadvertisingstaffperspective092023.pdf.

as sensitive and therefore subject to heightened protections.[30] ADPPA provided explicit protections for children similar to those in COPPA, including a ban on targeted advertising to anyone under 17 years of age, as well as a ban on transfers of children's data without consent. It also created a new "Youth Privacy and Marketing Division" within the FTC that could focus specifically on enforcing privacy protections for minors. These types of bipartisan reforms would provide further meaningful and important protections for kids online.

Some other proposals such as the Kids Online Safety Act (KOSA), while well-intentioned, raise concerns and must be carefully considered by this Committee, especially to the extent they would restrict access to certain types of content that the government would deem harmful to children.[31] Although bills to address online child safety pursue an important goal, content-based restrictions can hurt young people, particularly teenagers, who need to access important information. In some states, teenagers can begin to work, marry, and make their own healthcare decisions starting at the age of 16, requiring unrestricted access to information to inform their decision-making. Children who grow up in highly restricted environments or face parental or domestic abuse in particular have a strong need for access to information and private communications channels to ensure their safety and mental health, which may be jeopardized by legislation that empowers government officials to sue companies for enabling access to information that they deem "harmful" to young people.

Moreover, no consensus exists as to what content should be restricted under such a standard. Researchers are divided on what type of content and online services are and are not

[30] APRA's definition of "covered minor" should be modified to include a knowledge standard akin to that included in ADPPA to avoid a strict liability regime that could effectively force covered entities to age verify all users.

[31] *See, e.g.,* CDT, ACLU, EFF, and Fight for the Future Send Letter Ahead of Senate Judiciary Hearing to Protect Kids Rights (Jan 2024), https://cdt.org/insights/cdt-aclu-eff-and-fight-for-the-future-send-letter-ahead-of-senate-judiciary-hearing-to-protect-kids-rights/, which highlights concerns with the latest draft of the Kids Online Safety Act in the Senate Commerce Committee, some of which also exist in the House version of the bill.

harmful to young people.[32] In practice, this means that the government officials charged with enforcing such laws would be left to make often politicized decisions to curtail access to lawful speech they claim leads to adverse effects for kids. Government attempts to protect minors by restricting access to content also raise significant constitutional concerns as they can infringe on the rights of users, including children and teenagers, who have the right to access constitutionally-protected information.[33]

Further, while protecting children online through legislation is important, Congress should work to ensure that whatever protections it decides to put in place do not inadvertently create incentives to reduce privacy and increase barriers to accessing information for everyone, such as through broad requirements or heavy incentives to adopt age verification or age estimation systems for all users. Implementing age verification of all users to identify children may require further data collection and processing for children and adults alike. For example, age verification methods that require individuals to provide driver's licenses or other government credentials require collection and processing of personal data that services might not otherwise collect.[34] Age verification requirements may also impact specific communities differently. Young people often do not have IDs, and adult users including immigrants and low-income individuals

[32] *APA Chief Scientist Outlines Potential Harms, Benefits of Social Media for Kids,* American Psychology Association *(*February 2024), https://www.apa.org/news/press/releases/2023/02/harms-benefits-social-media-kids*;* *Surgeon General Issues New Advisory About Effects Social Media Use Has on Youth Mental Health,* U.S. Department of Health and Human Services (May 2023), https://www.hhs.gov/about/news/2023/05/23/surgeon-general-issues-new-advisory-about-effects-social-media-use-has-youth-mental-health.html*;* Claire Cain Miller, *Everyone Says Social Media Is Bad for Teens. Proving It Is Another Thing,* The New York Times (June 2023), https://www.nytimes.com/2023/06/17/upshot/social-media-teen-mental-health.html**.**

[33] *Brown, et al. v. Entertainment Merchants Assn. et al*., 564 U.S. 786 (2011); *Erznoznik v. Jacksonville*, 422 U. S. 205, 212–213 (1975) ("[M]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them.") (citation omitted).

[34] Scott Brennen and Matt Perault, *Keeping Kids Safe Online: How Should Policymakers Approach Age Verification,* Utah State University's Center for Growth and Opportunity. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/

may have outdated or limited access to IDs.[35] Moreover, requirements that incentivize or mandate age verification and age assurance systems erect barriers to accessing legal content for everyone, raising significant constitutional concerns.[36] In some cases, a site or service operator may know or have reason to know a user is a child without needing further information, such as through self-reporting or by inference from a user's activity on a site. ADPPA included a three-tiered system to define whether a covered entity had "knowledge" of a user being a covered minor. COPPA focuses more on the content of the website or service to determine what is covered.

Government service providers. APRA should include within its scope service providers to government entities. Currently, both government entities themselves and their service providers are fully exempt from APRA. Service providers to government entities, however, should not be exempt. Many of the provisions applicable to covered entity service providers, including that they should adhere to the directions of the government entity; limit their collection and processing of data to that which is necessary, proportionate, and limited to provide the service requested by the entity; return the data used when the relationship is over; and implement data security safeguards, should apply to government service providers as well. Relatedly, under the current draft, data brokers acting as service providers would be completely unregulated for those activities.

[35] *UMD Analysis: Millions of Americans Don't have ID Required to Vote,* Maryland Today (April 2023), https://today.umd.edu/umd-analysis-millions-of-americans-dont-have-id-required-to-vote; Vanessa M. Perez, *Americans with Photo ID: A Breakdown of Demographic Characteristics*, Project Vote (February 2015), https://www.projectvote.org/wp-content/uploads/2015/06/AMERICANS-WITH-PHOTO-ID-Research-Memo-February-2015.pdf.

[36] *Reno v. ACLU*, 521 U.S. 844 (1997) (invalidating an age verification requirement because it "effectively suppresse[d] a large amount of speech that adults have a constitutional right to receive and to address to one another").

Effects on advertising. The digital advertising system needs fundamental change, and APRA would move in that direction. However, APRA should be clearer in its advertising language. It treats ads differently depending on whether they are matched with an audience based on context, on first-party data, or on third-party data, but all of these key terms lack definitions. Moreover, it is not completely clear what restrictions APRA places on these three types of ads.

Data broker provisions. APRA should have stricter requirements for data brokers. The legislation should include a one-stop-shop for data deletion requests. As currently written, an individual may request all data brokers to stop collecting data on a forward-looking basis, but has to request deletion at each individual data broker. APRA should include language modeled from California's Delete Act, or the DELETE Act being considered by this committee, and allow individuals to request deletion from all data brokers in one request.

Further, the "do not collect" provision should not fully exempt credit reporting agencies under FCRA. The Consumer Financial Protection Bureau (CFPB) is currently engaging in a proceeding to determine whether data brokers trafficking in financial and related data should be considered consumer reporting agencies under the Fair Credit Reporting Act.[37] A categorical exemption to the "do not collect" requirement would then exempt all those data brokers, and would put the CFPB's goals of protecting financial privacy at odds with the legislation.

*   *   *

CDT is encouraged by the release of the bipartisan and bicameral draft of APRA, and thanks this Committee for its bipartisan work to consider and advance comprehensive privacy legislation. The time for a comprehensive federal privacy law is long overdue. We look forward

[37] CFPB, *CFPB Launches Inquiry Into the Business Practices of Data Brokers* (Mar. 15, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/.

to working constructively with the Committee and Congress to make any needed changes to APRA and helping to move it forward through the legislative process and into law.