Statement of Caitriona Fitzgerald

Deputy Director, Electronic Privacy Information Center (EPIC)

Hearing on "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors"

Before the

House Committee on House Administration
United States House of Representatives

February 16, 2022

Chair Lofgren, Ranking Member Davis, and members of the Committee, thank you for the opportunity to testify today concerning the privacy risks from Big Data and the need for reform in both the public and private sectors. My name is Caitriona Fitzgerald, Deputy Director at the Electronic Privacy Information Center, or EPIC. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. For over 25 years, EPIC has been a leading advocate for privacy in both the public and private sectors. In 2020, EPIC released *Grading on a Curve: Privacy Legislation in the 116th Congress*,[1] setting out the key elements of a privacy law.

The United States faces a data privacy crisis. Large and powerful technology companies invade our private lives, spy on our families, and gather the most intimate details about us for profit. These companies have more economic and political power than many countries and states. Through a vast, opaque system of databases and algorithms, we are profiled and sorted into winners and losers based on data about our health, finances, location, gender, race, and other personal information. The impacts of these commercial surveillance systems are especially harmful for marginalized and multi-marginalized communities, fostering discrimination and inequities in employment, government services, health and healthcare, education, and other life necessities.

These industries and systems have gone unregulated for more than two decades. And the result has been uncontrolled data collection, large scale data breaches, and an ecosystem dependent on a few large commercial surveillance platforms. And the enormity of the challenge we face is only going to grow. Americans have no meaningful choice in limiting the collection and use of their personal data online; and they can't simply "log off" services that have become central to our modern society. The more we depend on online platforms to carry out our most basic and essential activities, the more important it is to ensure that those systems are secure and do not undermine our rights to privacy, autonomy, and equity. We need comprehensive, baseline privacy protections for every person in the United States, changes to the business models that have led to today's commercial surveillance systems, limits on government access to personal data, and strong enforcement of privacy protections.

In my testimony today I will discuss (1) the problems we face today due to the failure of policymakers in the United States to create adequate data protection standards; (2) the current state of privacy law in the U.S.; and (3) what a comprehensive approach to data protection and privacy in the United States should look like. EPIC recommends that Congress enact a privacy law that: (1) limits the collection and use of personal data; (2) prohibits discriminatory uses of data; (3) requires algorithmic fairness and accountability; (4) bans manipulative design and unfair marketing practices; (5) limits government access to personal data; (6) provides for a private right of action; (6) preserves states' rights to enact stronger provisions; and (7) establishes a federal data protection agency to enforce these new rules.[2]

[1] EPIC, *Grading on a Curve*, https://epic.org/documents/grading-on-a-curve/.
[2] Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Justice in the United States* (2021), https://epic.org/wp-content/uploads/2022/01/Privacy-and-Digital-Rights-For-All-Framework.pdf.

I. The United States' Data Privacy Crisis

A. Unfettered Data Collection and Exploitation Harms Autonomy and Democracy

The lack of a comprehensive U.S. privacy law threatens individual autonomy and undermines our democratic institutions and national security. Without clear and enforceable data protection rules, there has been widespread overcollection, abusive data practices, and targeting that threatens our rights and institutions. Robust data privacy standards are essential to ensure the protection of human rights, human dignity, and the healthy functioning of our democracy.

Due to the failure of policymakers in the United States to create adequate data protection standards, rather than innovating around privacy-protective ways to advertise, the business models of advertising firms were permitted to grow unencumbered into corporate surveillance systems driven by collecting and commodifying every tiny bit of personal data about us.[3] These firms track us across our devices and all over the internet, building detailed profiles about us simply so they can target us with more ads, at the cost of exposing us to ever-increasing risks of breaches, data misuse, manipulation, and discrimination.[4]

Cross-site and cross-device tracking is one reason why the notice-and-consent approach does not work when it comes to privacy. The intricacies and breadth of the commercial surveillance industry are impossible for the vast majority of Internet users to fully grasp. In 2020, The Markup found that one-third of websites they surveyed contained Facebook's tracking pixel, which allows Facebook to identify users (whether or not they are logged into Facebook) and connect those website visits to their Facebook profile.[5] The Markup also scanned hundreds of websites on sensitive topics and discovered an alarming amount of tracking, including:

- a state agency page on how to report child abuse sending data about its visitors to six ad tech companies;
- WebMD and Everyday Health sending visitor data to dozens of marketing companies; and
- Eighty U.S. abortion providers whose sites included third-party trackers, some of which sent data to Facebook to be connected to user profiles.[6]

These trackers collect millions of data points each day that are then sold or transferred to data brokers, who combine them with other data sources linked to us to build invasive profiles. Sometimes these profiles are used to target people with "personalized" advertisements that stalk them across the web, and in other instances the data profiles are fed into secret algorithms used

[3] *See generally* Shoshana Zuboff, *The Age of Surveillance Capitalism*, Profile Books (2019).
[4] *See* Consumer Federation of America, *Factsheet: Surveillance Advertising: How Does the Tracking Work?* (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-how-tracking-works/.
[5] Julia Angwin, *What They Know… Now,* The Markup (Sept. 22, 2020), https://themarkup.org/blacklight/2020/09/22/what-they-know-now.
[6] Aaron Sankin and Surya Mattu, *The High Privacy Cost of a "Free" Website*, The Markup (Sept. 22, 2020), https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites.

to determine the interest rates on mortgages and credit cards, raise consumers' interest rates, or deny people jobs.[7]

This expansive network of surveillance, profiling, and data extraction is creepy and exploitative, but it has also been weaponized in ways that undermine our political systems and public discourse. The Cambridge Analytica case[8] provided a clear illustration of the ways that limitless data collection and retention threatens election integrity and our democratic institutions.[9] When personal data is collected and used to refine, propagate, and amplify hate, extremism, and disinformation, that threatens our self-determination, our elections, and our democracy. Just as advertising companies use profiles about us to manipulate us into purchases, so too can they manipulate our views by filtering the content we see.[10]

When Congress was considering consumer privacy legislation in the 1990s, the problem was new and emerging.[11] But since then, data collection has grown unchecked for over two decades and it is now beyond a crisis. In poll after poll, Americans say they want privacy. In a survey recently conducted by the Future of Technology Commission, a staggering 86% of Americans agreed that "it should be illegal for private companies to sell or share information about people no matter what" and only 46% agreed that it would be okay for companies to "sell consumers' data as long as they are transparent about how the data is used and make it clear to consumers."[12] In a Morning Consult poll last year, more than 4 in 5 voters said Congress should prioritize privacy legislation.[13] Congress needs to address this crisis now.

B. Government Use of Personal Data

The commercial exploitation of personal data is not the only threat to privacy. Government agencies have also dramatically increased their collection and use of personal data

---

[7] *See* EPIC, *Data Brokers*, https://epic.org/issues/consumer-privacy/data-brokers/.
[8] Robinson Meyer, *The Cambridge Analytica Scandal, in Three Paragraphs*, The Atlantic (Mar. 20, 2018), https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/.
[9] *See e.g.* Corin Faife and Alfred Ng, *After Repeatedly Promising Not to, Facebook Keeps Recommending Political Groups to Its Users*, The Markup (June 24, 2021), https://themarkup.org/citizen-browser/2021/06/24/after-repeatedly-promising-not-to-facebook-keeps-recommending-political-groups-to-its-users; Heidi Schlumpf, *Pro-Trump group targets Catholic voters using cellphone technology*, Nat'l Catholic Reporter (Jan. 2, 2020), https://www.ncronline.org/news/parish/pro-trump-group-targets-catholic-voters-using-cell-phone-technology; Sam Schechner, Emily Glazer, and Patience Haggin, *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, Wall Street Journal (Oct. 10, 2019), https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889;
[10] Colin Lecher and Leon Yin, *One Year After the Capitol Riot, Americans Still See Two Very Different Facebooks*, The Markup (Jan. 6, 2022), https://themarkup.org/citizen-browser/2022/01/06/one-year-after-the-capitol-riot-americans-still-see-two-very-different-facebooks.
[11] *See Hearing on S. 809: The Online Privacy Protection Act of 1999*, S. Comm. on Commerce, Sci, and Trans., Subcomm. on Communications (July 27, 1999) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://archive.epic.org/privacy/internet/EPIC_testimony_799.pdf ("For those who are willing to look closely, there is little indication that self-regulation is working. Privacy policies read more like warning notices and disclaimers.")
[12] Benson Strategy Group, Future of Tech Commission: Tech Attitudes Survey (July 20, 2021 - July 29, 2021), https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/pdfs/bsg_future_of_technology_topline_c1-1.pdf.
[13] Sam Sabin, States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data (Apr. 27, 2021), https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/.

while failing to address the significant risks to privacy and cybersecurity posed by modern data systems. Agencies are far behind where they need to be in terms of securing, protecting, and properly minimizing data. The lack of up-to-date rules has led to a default presumption of broad collection and use without necessary protections. The two principal statutes that regulate the federal government's use of personal data, discussed below, were passed twenty and forty-eight years ago.

We saw a glaring example of agency failure to properly consider privacy risks of data collection just this month. Reports that the Internal Revenue Service had contracted with third-party vendor ID.me for identity verification, requiring taxpayers to submit to facial recognition identification in order to access tax records online, sparked immediate controversy.[14] The plan would have forced individuals to submit biometric data to ID.me, who would have held on to that data for a minimum of seven years. Following pressure from advocates and members of Congress, the IRS announced last week that it was reversing course and will not go through with the plan to require individuals to use the privacy identity verification service ID.me to access the IRS website.[15]

And government agencies are especially vulnerable to data breaches. A recent Department of Homeland Security Inspector General report found that Customs and Border Protection (CBP) failed to safeguard pictures of travelers obtained for a facial recognition pilot program.[16] 184,000 facial images were exposed in a data breach of a CBP subcontractor, Perceptics, LLC. The Inspector General found that the CBP failed to undertake sufficient information security practices to prevent Perceptics from obtaining the data.

Rashida Richardson has outlined best practices for government procurement of data-driven technologies.[17] Many of these solutions could be implemented without legislative or regulatory action.

C. Self-Regulatory Approaches Have Failed Time and Again to Protect Privacy

Congress should not need further evidence to prove that industry self-regulation does not work when it comes to personal data – it has had nearly three decades to succeed, but instead had led us to the crisis we face today.[18]

---

[14] Drew Harwell, *IRS plan to scan your face prompts anger in Congress, confusion among taxpayers*, Wash. Post (Jan. 28, 2022), https://www.washingtonpost.com/technology/2022/01/27/irs-face-scans/.
[15] Alan Rappeport and Kashmir Hill, *I.R.S. to End Use of Facial Recognition for Identity Verification*, N.Y. Times (Feb. 7, 2022), https://www.nytimes.com/2022/02/07/us/politics/irs-idme-facial-recognition.html.
[16] Joseph Cuffari, Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020).
[17] Richardson, Rashida, *Best Practices for Government Procurement of Data-Driven Technologies* (May 2021), available at https://ssrn.com/abstract=3855637.
[18] *See* Robert Gellman & Pam Dixon, Many Failures: A Brief History of Privacy Self-Regulation in the United States (Oct. 2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf; *see also* Center for Digital Democracy and U.S. PIRG, *Cookie Wars, Real-Time Targeting, and Proprietary Self Learning Algorithms: Why the FTC Must Act Swiftly to Protect Consumer Privacy*, FTC Privacy Roundtables – Comment, Project No. P095416 (Nov. 4, 2009),

In November 1999, the FTC and Department of Commerce announced the formation of the Network Advertising Initiative (NAI), shortly after DoubleClick, an online target advertising company, was the subject of an FTC investigation. Less than a year later and with little involvement from consumer and privacy groups, the self-regulatory NAI principles were publicized.[19] The NAI standards were unsurprisingly weak. NAI members could transfer information between themselves to an unlimited degree, so long as it is used for advertising. No meaningful enforcement mechanism was incorporated.

Around the same time, the World Wide Web Consortium (W3C) released the Platform for Privacy Preferences (P3P) protocol.[20] P3P was a complex and confusing protocol that made it more difficult for Internet users to protect their privacy.

Despite stating in a report to Congress in May 2000 that self-regulatory programs fell "well short" of expectations,[21] the Federal Trade Commission itself released self-regulatory principles in 2009 and again in 2012.[22] The 2009 principles sparked the creation of the Digital Advertising Alliance (DAA), which was comprised of industry associations. The DAA promoted weak privacy standards with little enforcement, rubber stamping existing business practices.

Most recently, the Digital Advertising Alliance has promoted its self-regulatory principles,[23] which involve "opt-out" models that are inscrutable and hard for average users to navigate. These systems are designed in every way possible to push people away from privacy protections, to give the appearance of user "control," but in fact to prevent individuals from exercising any agency over what is done with their data.

None of these self-regulatory systems have worked. They simply cement the existing harmful business practices that form surveillance capitalism. It is past time to move away from self-regulation.

D. Corporate Surveillance is Especially Harmful to Marginalized Communities

The monetization of Americans' personal data has an acute impact on marginalized communities.[24] Invasions of privacy deprive people of opportunities and they perpetuate

---

https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00013/544506-00013.pdf.

[19] *See* Letter from EPIC to S. Comm. on Commerce (July 28, 2000), https://archive.epic.org/privacy/internet/NAI_letter.html.

[20] EPIC, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy* (June 2000), https://archive.epic.org/reports/prettypoorprivacy.html.

[21] Fed. Trade Comm'n, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report To Congress* 35 (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

[22] Fed. Trade Comm'n, FTC Staff Report: *Self-regulatory Principles For Online Behavioral Advertising: Tracking Targeting, And Technology* (Feb. 2009); Fed. Trade Comm'n, *Protecting Consumer Privacy In An Era Of Rapid Change: Recommendations For Businesses And Policymakers* (Mar. 2012).

[23] Digital Advertising Alliance, DAA Self-Regulatory Principles, https://digitaladvertisingalliance.org/principles.

[24] *See Protecting Consumer Privacy in the Age of Big Data*, 116th Cong. (2019), H. Comm. on the Energy & Comm., Subcomm. on Consumer Protection and Comm. (Feb. 26, 2019) (testimony of Brandi Collins-Dexter, Color of Change),

systemic inequities in our society. We have all had the experience of being creeped out by an ad targeted at us – many people assume that companies like Facebook must be using the microphones on our phones to listen to us because the ads are so often related to something we just had a conversation about. They are not really listening to us, but the reality is even creepier - they do not need to hear us to know what we are saying or thinking because that is how much data they are collecting about us – the websites we visit, where we are going, who our friends are, and what those friends are reading and doing.[25] They are tracking so many data points about us that it really seems like they are listening to us.

For some people, that means being creeped out by an ad. But for marginalized communities, it can often mean not being shown ads for housing or job openings, depriving individuals of life opportunities, and perpetuating systemic inequities in our society.

These data practices threaten individual privacy and autonomy, and companies have proven time and again that they cannot police themselves. Rather than continuing to tweak a system that demonstrably does not work, this problem requires a legislative and regulatory solution.

II. Current Law is Inadequate to Protect Individual Privacy and our Democracy

A. Federal Agencies are Subject to the Privacy Act and E-Government Act

The Privacy Act of 1974[26] was created in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. Executive departments, military departments, independent regulatory agencies, and government-controlled corporations are all covered by the Privacy Act. It safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it includes a private right of action, allowing individuals to sue the government for violating the Privacy Act's provisions.

The important purposes of the Privacy Act have been undermined over the last three decades by the numerous and broad exceptions asserted by most agencies. These exceptions (as well as the practical difficulties involved with maintaining and regulating such a vast system of databases) mean that individual privacy is not often as carefully protected as the drafters of the Privacy Act might have liked. Since "records," "systems of records" and "agencies" are narrowly defined, the Act may not cover many types of databases and data-gathering activities. Also, there are certain exceptions given for "law enforcement purposes." Finally, the "routine use" exception

https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Brandi%20Collins%20Dexter%2002.26.2019.pdf.

[25] Elec. Frontier Foundation, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance* (2019), https://www.eff.org/wp/behind-the-one-way-mirror.

[26] 5 U.S.C. § 552a.

allows government agencies to disclose individually identifiable information simply by stating their plans to disclose that type of information when they create or alter the database.

The Privacy Act simply defines "routine use" as "the use of such record for a purpose which is compatible with the purpose for which it was collected."[27] Note that a routine use does not have to be a purpose identical to the purpose for which the record was collected, only a compatible purpose. This phrasing can often lead to mission creep for a system of records, in which the routine uses for a particular database gradually increase until its scope is far greater than its originally stated goals.[28]

The rights provided for under the Privacy Act have also been severely curtailed by a series of misguided court decisions. In 2004, the Supreme Court ruled that individuals whose data is misused by a federal agency are not entitled to the statutory damages that the Privacy Act is intended to provide, but must instead prove actual damages.[29] In 2012, the Court ruled that individuals cannot recover damages under the Privacy Act for mental and emotional distress, even when an agency wrongly discloses highly sensitive information like a person's HIV status.[30] These decisions have not only made it exceptionally difficult for individuals to obtain relief for the misuse of their personal information by federal agencies; they have also weakened a key incentive for agencies to comply with the Privacy Act in the first place.

The lesson from the Privacy Act when applied to comprehensive privacy legislation covering the private sector is that if legislation does not set strict purpose and use limitations, and establish robust mechanisms for enforcement of those limitations, there will always be an incentive for companies to retain and use data beyond its initial purpose—to the point where the restriction becomes no restriction at all.

The E-Government Act, enacted in 2002, was intended to make federal agencies more accessible to the public by electronic means. The Act created an Office of Electronic Government within the Office of Management and Budget and requires that regulatory proceedings and other material appear on agency web sites. Crucially, section 208 of the Act requires agencies to perform Privacy Impact Assessments (PIAs) before procuring an information system that will process personal data or initiating a new collection of personal information.

When implemented properly, PIAs force government agencies and other institutions to carefully evaluate and publicly disclose the privacy risks of a proposed action, system, or project. An impact assessment enables the entity to identify privacy risks, to determine how and if those risks can be mitigated, and to make an informed decision whether the proposed collection or system can be justified in light of its privacy impact. An impact assessment also serves to inform the public of a data collection or system that poses a threat to privacy.

[27] *Id.* at § 552a(a)(7).
[28] Gellman, Robert, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974*, 23-37 (May 12, 2021), *available at* https://ssrn.com/abstract=3844965.
[29] *Doe v. Chao*, 540 U.S. 614 (2004).
[30] *FAA v. Cooper*, 566 U.S. 284 (2012).

Privacy impact assessments—or data protection impact assessments—are also required by the European Union's General Data Protection Regulation (GDPR) for all high-risk data processing activities. Article 35 of the GDPR states:

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[31]

However, the key to making impact assessments effective lies in enforcement. Without proper guidance and enforcement mechanisms, agencies and private companies will simply see PIAs as a box-checking exercise that must be completed for compliance rather than a substantive analysis of whether and how the entity should collect or use personal data.[32]

A recent example lies in the PIA conducted by the Internal Revenue Service prior to contracting with third-party vendor ID.me for identity verification.[33] The PIA lifts language directly from ID.me's corporate materials.[34] The PIA also doesn't make mention of the one-to-many facial recognition system that ID.me has admitted to using.[35] In fact, despite the massive and well-known privacy and bias issues with facial recognition technology, the only facial matching technology referenced in the PIA is "comparing still … or video ... selfies against the photo evidence uploaded by the user."[36]

As with the Privacy Act, courts have made it exceedingly difficult to enforce the personal data provisions of the E-Government Act through private action. In a pair of decisions from 2017 and 2019, the D.C. Circuit held that organizations and individuals cannot rely on an agency's failure and publish a PIA to stop the agency's unlawful processing of personal information.[37] As a result, there are few if any consequences for agencies that bypass the requirements of section 208.

This demonstrates just how critical it is that Congress establish a broad and express private right of action in privacy legislation. Rulings under the Privacy Act and E-Government Act have shown that without a robust private right of action, statutory rights will not be adequately enforced and privacy harms will continue undeterred. As I discuss later in my testimony, it also demonstrates the need for a federal Data Protection Agency that can serve as a

---

[31] Regulation (EU) 2016/679 of the European Parliament, Article 35.
[32] *See* Ari Ezra Waldman, *Privacy, Practice, and Performance*, California Law Review, Vol. 110, 19-21 (2021).
[33] Internal Revenue Service, *Privacy Impact Assessment: SADI CSP – ID.me* (Nov. 2021), https://www.irs.gov/pub/irs-pia/id-me-pia.pdf (hereinafter "IRS PIA").
[34] *See Id.* at 10 and ID.me, Privacy Policy, 5, https://www.id.me/privacy.
[35] Tonya Riley, *ID.me CEO backtracks on claims company doesn't use powerful facial recognition tech*, Cyberscoop (Jan. 26, 2022), https://www.cyberscoop.com/id-me-ceo-backtracks-on-claims-company-doesnt-use-powerful-facial-recognition-tech/; Ina Fried, *ID.me CEO apologies for misstatements on IRS facial recognition*, Axios (Jan. 27, 2022), https://www.axios.com/idme-ceo-apologizes-misstatements-irs-facial-recognition-88ce2ee2-9ae9-426c-b69e-c0b42ad82f61.html.
[36] IRS PIA, *supra* note 8 at 8.
[37] *EPIC v. United States Dep't of Com.*, 928 F.3d 95 (D.C. Cir. 2019); EPIC *v. Presidential Advisory Comm'n on Election Integrity*, 878 F.3d 371 (D.C. Cir. 2017).

central authority on privacy in the federal government, with the expertise necessary to guide agencies as they conduct PIAs.

B. Private Sector Data Collection and Use Governed by Sectoral Laws

There is no comprehensive law in the United States governing the collection and use of personal data. Instead, some types and uses of data are regulated by sector-specific laws such as the Health Insurance Portability and Accounting Act (HIPAA), the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA), and others, while many types of data are not protected at all.[38] In addition to leaving huge gaps in coverage that have allowed the expansion of data collection and abuse across many different sectors, most notably online services, this also leads to confusion by the public about what types of personal data are protected and how and increased compliance costs for businesses. The US needs a comprehensive, coherent approach to privacy and data protection.

C. Comprehensive State Privacy Laws

In recent years, largely in response to Congressional inaction, some states have enacted their own privacy laws. In 2018, the California State Legislature enacted the California Consumer Privacy Act of 2018 ("CCPA"), the first comprehensive consumer privacy law enacted in the United States. The CCPA established the right of residents of California to know what personal information about them is being collected; to know whether their information is sold or disclosed and to whom; to limit the sale of personal information to others; and to access their information held by others. The CCPA gives individuals a right to delete their data and prohibits businesses from selling the personal information of CA residents under the age of 16 without their opt-in consent. The CCPA was further updated by a ballot question approved by voters in 2021, creating the California Privacy Protection Agency.

In the past year, Virginia and Colorado have also passed broad consumer privacy laws, though of at varying levels of effectiveness when it comes to protecting privacy. And this year, state legislatures in Massachusetts, Washington, Alaska, Oklahoma, New York, Ohio, Indiana, Florida, and elsewhere are considering comprehensive privacy legislation.

III. Solutions: Congress Should Enact Comprehensive Privacy Legislation and Establish a Data Protection Agency

The basic structure of information privacy law is to place responsibilities on organizations that collect personal data and to give rights to the individuals whose data is collected. This is sensible for many reasons, including the fact that it is the entity in possession of the data that controls its subsequent use and is in the best position to limit access and protect against abuse or breach. Information privacy law also promotes transparency by making data

[38] *See* Cong. Research Service, R45631, *Data Protection Law: An Overview* (2019), *available at* https://crsreports.congress.gov/product/pdf/R/R45631.

practices more open to scrutiny and encourages the development of innovative technical approaches.

EPIC, joined by ten other privacy, consumer, and civil rights groups, has set forth a framework for Congress to use when developing a privacy law that: (1) limits the collection and use of personal data; (2) prohibits discriminatory uses of data; (3) requires algorithmic fairness and accountability; (4) bans manipulative design and unfair marketing practices; (5) limits government access to personal data; (6) provides for a private right of action; (6) preserves states' rights to enact stronger provisions; and (7) establishes a federal data protection agency to enforce these new rules.[39] I detail each of these principles below.

A. Limit the Collection and Use of Personal Data

Federal legislation should not take a "notice and choice" approach or rely on industry self-regulation to protect data privacy. Instead, the law should place strict limits on the collection, use, storage, and transfer of personal data. Legislation should build on the U.S. Code of Fair Information Practices and OECD Privacy Guidelines, which are widely followed and form the basis of other data protection regimes. These frameworks create obligations for companies that collect personal data and establish individual data rights. Core principles include:

- Strict data collection and use limitations
- Data minimization and deletion requirements
- Transparency about business practices
- Purpose specification
- Access, correction, and deletion rights
- Data accuracy
- Confidentiality and security requirements
- Compliance and accountability

The adoption of "data minimization" techniques is essential to data protection across the board. A company implementing data minimization measures should collect only the data necessary to provide a good or service, and not more.[40] Companies complying with their data minimization requirements must also delete personal information when it is no longer needed.

The landmark privacy law passed by Congress, the Privacy Act of 1974, which applies to government agencies, requires data minimization. Each agency that collects personal data shall "maintain in its records only such information about an individual as is relevant and necessary to

[39] Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Justice in the United States* (2021), https://epic.org/wp-content/uploads/2022/01/Privacy-and-Digital-Rights-For-All-Framework.pdf.

[40] *See* EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (January 2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/; *see also* Access Now, *Data minimization: Key to protecting privacy and reducing harm* (May 2021), https://www.accessnow.org/data-minimization-guide/.

accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[41]

The recently passed update to the California Consumer Privacy Act also includes provisions requiring data minimization.[42] The European Union General Data Protection Regulation (GDPR) requires companies, among other things, to minimize collection of consumer data to what is "[a]dequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."[43]

Personal data that is not collected cannot be at risk of a data breach. Recognizing the need to limit private data collection, the National Telecommunications and Information Administration ("NTIA") has identified "reasonable minimization" as a "critical Privacy Outcome."[44]

Some types of data, and some uses of data, are especially sensitive and deserve even stricter regulation. For instance, biometric and genetic data are inherently sensitive, but even information about the products people buy and the services they search for can be used to make inferences about their health, religious beliefs, economic situations, and other characteristics that are sensitive in nature. In these situations, prohibiting certain data collection and use may be necessary.

B. Prohibit Discriminatory Uses of Data

Privacy legislation should protect against discriminatory uses of data and extend civil rights protections online.[45] Processing that leads to disparate treatment or adverse disparate impacts should be prohibited. The law should also prohibit predatory data collection practices and uses that target economically disadvantaged or marginalized communities.[46]

C. Require Algorithmic Fairness and Accountability

Automated systems that use artificial intelligence or other big data tools to make decisions about individuals pose significant risks to fundamental rights. Public and private actors are increasingly using AI systems to make decisions about eligibility for jobs, education, housing, parole and bail, credit, insurance, healthcare, and government services.[47] The error,

---

[41] 5 U.S.C. § 552a (e)(1).
[42] Cal. Civ. Code § 1798.100(c).
[43] Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).
[44] Nat'l Telecomms. & Info. Admin., U.S. Dep't. Commerce, *Developing the Administration's Approach to Consumer Privacy*, Request for Comments, Docket No. 180821780-8780-01 (Oct. 11, 2018), https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrationsapproach-to-consumer-privacy.
[45] *See* Kristen Clarke and David Brody, *It's time for an online Civil Rights Act*, The Hill (Aug. 3, 2018), https://thehill.com/opinion/civil-rights/400310-its-time-for-an-online-civil-rights-act.
[46] *See generally* Leadership Conf. on Civil and Human Rights, *Civil Rights Principles for the Era of Big Data*, https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/.
[47] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

bias, and discrimination embedded in these systems perpetuate systemic inequities,[48] yet public agencies and private companies are not currently required to evaluate the potential impacts and biases of these systems before they use them.

Indeed, many AI systems have been deployed by both government agencies and private companies with little to no oversight and with questions regarding their effectiveness.[49] A 2019 National Institute of Standards and Technology ("NIST") study of facial recognition tools—which are typically "AI-based"[50]—found that the systems were up to 100 times more likely to return a false positive for a non-white person than for a white person.[51] Specifically, NIST found that "for one-to-many matching, the team saw higher rates of false positives for African American females," a finding that is "particularly important because the consequences could include false accusations."[52] A separate study by Stanford University and MIT, which looked at three widely deployed commercial facial recognition tools, found an error rate of 34.7% for dark-skinned women compared to an error rate of 0.8% for light-skinned men.[53] A review of Rekognition—an Amazon-owned facial recognition system marketed to law enforcement—revealed indications of racial bias and found that the system misidentified 28 members of U.S. Congress as convicted criminals.[54]

Legislation should require meaningful transparency, enable oversight of these AI systems by developing standards for and requiring independent assessments of algorithmic impact, conducting routine and randomized screening of new systems, and requiring publication of system details and audit results.[55] The law should also require a right to human review of automated decisions. Uses of AI that subvert human and civil rights should be prohibited, such as many uses in the criminal justice system, for mass surveillance, and emotion detection.

Unless express, binding limits on the use of AI are established *now*, the technology will quickly outpace our collective ability to regulate it. Congress should not make the same self-regulatory mistakes with AI that it made with data collection and use.

---

[48] *See* Richardson, Rashida, *Racial Segregation and the Data-Driven Society: How Our Failure to Reckon with Root Causes Perpetuates Separate and Unequal Realities*, 36 Berkeley Tech. L.J. 3 (2022).
[49] David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, & Mariano-Florentino Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* 6 (Feb. 2020) https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.
[50] Nat'l Inst. Standards & Tech., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 14 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[51] Nat'l Inst. Standards & Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
[52] *Id.*
[53] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Proceedings of Machine Learning Research 81:1–15 (2018), https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/.
[54] Russell Brandom, *Amazon's facial recognition matched 28 members of Congress to criminal mugshots*, The Verge (July 26, 2018), https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.
[55] *See e.g.* H.R.6580, 117th Cong. (2022) (Algorithmic Accountability Act requires transparency and accountability for automated decision making systems).

D. Ban Manipulative Design and Unfair Marketing Practices

Legislation should prohibit dark patterns designed to manipulate individuals into making choices that are in the businesses' interests rather than their own.[56] Pay-for-privacy provisions or take-it-or-leave-it terms of service, which discriminate against those with less means, should be illegal.

E. Limit Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government is able to collect personal data in bulk from companies, a form of "mass surveillance" enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.[57]

Federal agencies are using data collected by private companies for law enforcement, immigration, and other purposes. This undermines legal mechanisms intended to limit such government access, such as the 4th Amendment. A detailed report in *The Wall Street Journal* in early 2020 revealed that federal agencies are accessing cell phone location data without warrants or judicial oversight.[58] These agencies are engaging in warrantless location surveillance despite the Supreme Court's ruling in *Carpenter v. United States*[59] that officers must obtain a warrant in order to collect cell phone location data. The sale of location data by data brokers, which made this warrantless tracking possible, is a threat to the privacy and security of all Americans. Congress should close the loopholes that have allowed warrantless location tracking to take place.

Federal privacy legislation should require that any government collection of personal data should have a lawful basis, be performed in accordance with applicable data protection laws, be limited in time and scope to the original purpose of collection, and be subject to independent oversight. With few exceptions, it should be conducted only with the consent of those whose personal data is collected. Personal data should not be collected in bulk, from third-party data brokers without a warrant, or through warrantless surveillance. Legislation should require agencies to appoint a Chief Privacy Officer at the leadership level with the authority to oversee and address privacy issues across the agency.

---

[56] *See generally* Rohit Chopra, *Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc.*, FTC File No. 1723186 (Sep. 2, 2020), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf; *See, e.g.*, Complaint of EPIC, *In re In the Matter of Amazon.com, Inc.* (Feb. 23, 2021), https://epic.org/wp-content/uploads/privacy/dccppa/amazon/EPIC-Complaint-In-Re-Amazon.pdf.

[57] *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

[58] Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone- location-data-for-immigration-enforcement-11581078600.

[59] 138 S. Ct. 2206 (2018).

F. Provide for a Private Right of Action

Robust enforcement is critical to effective privacy protection. The inclusion of a private right of action with statutory damages is a crucial tool to supplement government enforcement, particularly for marginalized communities. If a company violates federal privacy law, individuals and groups of individuals, or their agents, should be able to pursue a private right of action that provides meaningful redress without a showing of additional harm. While government enforcement is essential, the scope of data collection online is simply too vast for one entity to regulate. Individuals and groups of individuals who use these online services are in a good position to identify privacy issues and bring actions to vindicate their interests.

The inclusion of a private right of action is the most important tool Congress can give to Americans to protect their privacy.

Many privacy laws include a private right of action, and these provisions have historically made it possible to hold companies accountable for their privacy violations. In crafting liability provisions in privacy statutes, Congress has frequently included a liquidated damages provision to avoid protracted disputes over quantifying privacy damages. This is necessary because it is often difficult to assign a specific economic value to the harm caused by a privacy violation.

For example, when Congress passed the Cable Communications Privacy Act in 1984, they established privacy rights for cable subscribers and created a private right of action for recovery of actual damages not less than liquidated damages of $100 per for violation or $1,000, whichever is higher.[60] The Video Privacy Protection Act specifies liquidated damages of $2,500.[61] The Fair Credit Reporting Act affords individuals a private right of action that can be pursued in federal or state court against credit reporting agencies, users of credit reports, and furnishers.[62] In certain circumstances, individuals can also recover attorney's fees, court costs, and punitive damages. The Drivers Privacy Protection Act similarly includes a private right of action.[63] The Telephone Consumer Protection Act allows individuals who receive unsolicited telemarketing calls to recover actual monetary loss or up to $500 in damages per violation.[64]

The statutory damages set in privacy laws are not large in an individual case, but they can provide a powerful incentive in large cases and are necessary to ensure that privacy rights will be taken seriously and violations not tolerated. In the absence of a private right of action, there is a very real risk that companies will not comply with the law because they think it is unlikely that they would get caught or fined. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations.

[60] 47 USC § 551(f).
[61] 18 USC § 2710(c)(2).
[62] 15 U.S.C. §§ 1681n-1681o.
[63] 18 U.S.C. § 2724.
[64] 47 USC § 227(c)(5).

G. Preserve States' Rights to Enact Stronger Protections

A well-established principle in the United States is that federal privacy law should operate as a floor and not a ceiling. That means that Congress often passes privacy legislation that sets a minimum standard, or "baseline," for the country and allows individual states to develop new and innovative approaches to privacy protection. Historically, federal privacy laws have not preempted stronger state protections or enforcement efforts. Federal consumer protection and privacy laws, as a general matter, operate as regulatory baselines and do not prevent states from enacting and enforcing stronger state statutes.

The Fair Credit Reporting Act, The Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Driver's Privacy Protection Act, and the Gramm-Leach-Bliley Act are just a few of the laws which allow states to craft protections that exceed federal law.

The consequences of federal preemption are potentially severe and could include both a reduction in privacy protection for many consumers, particularly as states continue to enact their own privacy laws, and also a prohibition on state legislatures addressing new challenges as they emerge. That could leave consumers and businesses exposed to increasing levels of data breach and identity theft from criminal hackers and foreign adversaries.

Today the states are on the front lines of consumer protection in the United States. They are updating privacy laws to address new challenges. They are bringing enforcement actions to safeguard American consumers. They are establishing the data protection standards that are safeguarding the personal data of Americans from attack by foreign adversaries.

It is absolutely essential to the development of privacy safeguards that Congress establish baseline standards that all states must follow, but leave states with the freedom to update their privacy laws as new technologies and business practices emerge. As Justice Brandeis famously explained, the states are the laboratories of democracy.[65] And these laboratories are all the more crucial in the area of technology policy, which is defined by persistent and rapid change.

H. Establish a U.S. Data Protection Agency

For more than two decades, EPIC has worked to support the Federal Trade Commission in its efforts to safeguard the privacy of American consumers. But it is our view that the consumer-centric, industry-by-industry approach to privacy regulation is unworkable. Congress should establish an independent Data Protection Agency in the United States to regulate, enforce, and coordinate data protection policies across all industries and governmental entities.

The United States has historically approached privacy with a consumer lens, but that view is outdated. The commercial surveillance systems that profile us and sort us into groups through a vast, opaque system of algorithms are perpetuating systemic inequities in our society.

[65] "It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory[.]" *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (Brandeis, J. dissenting).

The harms to individuals, groups of individuals, and society at large are real, and they require real solutions that do not fit neatly into the "consumer" box.

In order to move away from the commercial approach and tackle the very real threats Big Tech poses to civil rights, individual autonomy, and democracy, the United States must create a dedicated data protection agency ("DPA"). The United States is one of the few democracies in the world that does not have a federal data protection agency, even though the original proposal for such an institution emerged from the U.S. in the 1970s. The United States was once a global leader on privacy. The Fair Credit Reporting Act, passed in 1970, was viewed at the time as the first modern privacy law—a response to the growing automation of personal data in the United States. There is an urgent need for leadership from the United States on data protection. Virtually every other advanced economy has recognized the need for an independent agency to address the challenges of the digital age. Current law and regulatory oversight in the United States is woefully inadequate to meet the challenges. We also now face threats from foreign adversaries that target the personal data stored in U.S. companies and U.S. government agencies. The U.S. urgently needs a Data Protection Agency.

The DPA should be dedicated to privacy and data protection, oversight, and enforcement, with the authority and resources to address emerging privacy challenges. The DPA should examine the social, ethical, and economic impacts of data processing and oversee compliance and impact-assessment obligations. The DPA should work with the FTC and Department of Justice to address competition and growing concentration in the technology sector by reviewing and issuing guidance on the privacy and data protection implications of proposed mergers. Congress should empower a DPA with adequate resources, rulemaking authority, and effective investigatory and enforcement powers.[66]

Ideally, a DPA would be given the proper oversight and enforcement tools to ensure that companies innovate around and improve privacy, rather than simply pursuing penalties for privacy violations.[67] One mechanism for this has been proposed in Senator Gillibrand's Data Protection Act[68] – the DPA could require and oversee impact assessments of high-risk data practices, such as consumer scoring or the use of or AI or biometric data. As opposed to the FTC's unfair and deceptive acts and practices authority, which is backward looking and attempts to remedy harms that already occurred, the DPA's ability to regulate high-risk data practices could stop privacy harms *before* they happen and help technology companies innovate around privacy.

There is broad public support for the creating of a Data Protection Agency. A recent Data for Progress poll showed that 78% of Americans across the political spectrum support

[66] *See* EPIC, *The U.S. Urgently Needs a Data Protection Agency*, https://epic.org/dpa.
[67] *See* Julie Cohen, *How (Not) to Write a Privacy Law*, Knight First Amendment Institute (Mar. 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law ("An essential strategy for scaling enforcement authority involves leveraging gatekeeper power to demand and guarantee adherence to the design, operational, and monitoring requirements that public oversight processes have defined.")
[68] S. 2134, 117th Cong. § 3 (2021).

establishing a federal agency "specifically dedicated to creating and standardizing a regulatory framework aimed at protecting Americans' data privacy."[69]

The U.S. is one of the few advanced economies in the world without a data protection agency. The consequence is that the U.S consumers experience the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber-attack by criminals and foreign adversaries. Meanwhile companies collect vast amounts of personal data about Americans without their knowledge and without any meaningful data protection standards. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security. The need for an effective, independent data protection agency has never been greater.

IV. Congress Should Enact the Online Privacy Act

Congress can address these issues and strengthen data privacy protections in the United States by taking up a bill that incorporates many, if not all, of the suggestions outlined above. The Online Privacy Act filed by Chairwoman Lofgren and Representative Eshoo is a comprehensive framework that would place strict limits on the collection and use of personal data, extend civil rights protections online, and establish strong enforcement mechanisms via a private right of action and the creation of a U.S. Data Protection Agency.[70]

The Online Privacy Act would also make important updates to require the House of Representatives, Government Publishing Office, Library of Congress, and Smithsonian Institution to implement measures to prevent the disclosure of personal information by those entities and to minimize the risk of privacy harms in their operations.

One of the Online Privacy Act's strengths lies in its enforcement mechanisms. Without strong enforcement, many businesses will simply ignore privacy laws and accept the small risk of an enforcement action as a cost of business, as we have seen in Europe and in several states. Without independent oversight, privacy law simply becomes, as Professor Ari Ezra Waldman says, "compliance, rather than a substantive, task," or "privacy theater."[71] The inclusion of a private right of action and establishment of a Data Protection Agency avoid this fate by ensuring that the incentives to comply with privacy statutes are in place.

The Illinois Biometric Information Privacy Act (BIPA) has proven to be the most effective privacy law in the nation due to the inclusion of a private right of action.[72] Last November, Facebook announced that it was shutting down its face recognition system and deleting more than a billion people's facial recognition templates.[73] Many advocates believe

---

[69] Data for Progress, Poll, 10 (July 2021), https://www.filesforprogress.org/datasets/2021/7/dfp_DPA_202107_toplines.pdf.
[70] H.R.6027, 117th Cong. (2021).
[71] Ari Ezra Waldman, *Privacy Law's False Promise*, 97 Wash. U. L. Rev. 0773, 776 (2020); Ari Ezra Waldman, How Big Tech Turns Privacy Laws Into Privacy Theater, Forbes Future Tense (Dec. 2, 2021), https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html.
[72] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf.
[73] Facebook, *An Update On Our Use of Face Recognition* (Nov 2. 2021), https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/.

pending BIPA lawsuits against the use of facial recognition were a major factor in Facebook's decision. In 2020, Clearview AI ended all contracts with private companies and non-law enforcement entities nationwide and canceled all accounts belonging to any entity in Illinois in response to a BIPA suit it was facing.[74]

In addition to its strong enforcement mechanisms, the Online Privacy Act would also add prohibitions for discriminatory processing of data, mandate data minimization, require opt-in consent for the sale of personal information, ban dark patterns, grant data subject rights to users, and impose data security requirements on covered entities. Enactment of the Online Privacy Act would help restore the current power imbalance between the companies who collect data and individuals. EPIC recommends that Congress enact the Online Privacy Act this session.

V. Conclusion

The lack of a U.S. privacy law places not only our individual autonomy, but our democracy at risk. We have seen an increased interest among federal policymakers in recent years, but now we need action. We need comprehensive privacy legislation, robust enforcement, and resources and attention dedicated to making our online world more secure and preserving the privacy and fairness of new data systems.

Thank you for the opportunity to testify today.

[74] Nick Statt, *Clearview AI to stop selling controversial facial recognition app to private companies*, The Verge (May 2020), https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law.