Testimony and Statement for the Record
Jules Polonetsky
CEO, Future of Privacy Forum

Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework
Senate Committee on Commerce, Science, and Transportation

May 1, 2019

Thank you for inviting me to speak today. The Future of Privacy Forum is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. We are supported by leading foundations, as well as by more than 150 companies, with an advisory board representing academics, industry, and civil society.[1] We bring together privacy officers, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

I speak to you today with a sense of urgency. Congress should advance a baseline, comprehensive federal privacy law because the impact of data-intensive technologies on individuals and vulnerable communities is increasing every day as the pace of innovation accelerates. Each day's news brings reports of a new intrusion, new risk, new harm, another boundary crossed. Sometimes it's a company doing something that consumers or critics regard as "creepy;" sometimes it is a practice that raises serious risks to our human rights, or civil liberties, or our sense of autonomy. There is a growing public awareness of how data-driven systems can reflect or reinforce discrimination and bias, even inadvertently.[2]

For many people, personal privacy is a deeply emotional issue, and a real or perceived absence of privacy may leave them feeling vulnerable, exposed, or deprived of control. For others, concrete financial or other harm may occur; a loss of autonomy, a stifling of creativity due to feeling surveilled, or the public disclosure of highly sensitive information like individuals' financial data or disability status are just some potential consequences of technology misuse, poor data security policies, or insufficient privacy controls.[3]

At the same time, individuals and society are benefitting from new technologies and novel uses of data. Companies reinventing mobility are making transportation safer and more accessible; healthcare providers are using real-world evidence to advance research; and education technology providers can empower students and teachers to enhance and personalize learning.[4] In much the same way that electricity faded from novelty to background during the industrialization of modern life 100 years ago, we see artificial intelligence and machine learning becoming the foundation of commonly available products and services, like voice-activated digital assistants, traffic routing, and accurate healthcare diagnoses.[5]

---

[1] The views herein do not necessarily reflect those of our supporters or our Advisory Board. See Future of Privacy Forum, Advisory Board, https://fpf.org/about/advisory-board/; Supporters, https://fpf.org/about/supporters/.
[2] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018).
[3] Lauren Smith, Unfairness By Algorithm: Distilling the Harms of Automated Decision-Making (Dec 11, 2017), Future of Privacy Forum, https://fpf.org/2017/12/11/unfairness-by-algorithm-distilling-the-harms-of-automated-decision-making/.
[4] Future of Privacy Forum, Policymaker's Guide to Student Data Privacy, (April 4, 2019), FERPA|Sherpa, https://ferpasherpa.org/policymakersguide/.
[5] Brenda Leong & Maria Navin, *Artificial Intelligence: Privacy Promise or Peril?* (February 20, 2019), Future of Privacy Forum, https://fpf.org/2019/02/20/artificial-intelligence-privacy-promise-or-peril.

Each of these examples holds the promise of improving our lives but each one also poses the risk of new and sometimes unforeseen harms. It is in the best interests of individuals and organizations for national lawmakers speak in a united, bipartisan voice to create uniform protections that help rebuild trust. Congress has the opportunity now to pass a law that will shape these developments to maximize the benefits of data for society while mitigating risks. Delaying Congressional action means that businesses will inevitably continue to develop new models, build infrastructure, and deploy technologies, without the guidance and clear limits that only Congress can set forth.

This is a global challenge, and other countries have responded. The European Union (EU) has substantially updated its data protection framework, the General Data Protection Regulation (GDPR),[6] and Japan has made substantial updates to its data protection law, the Act on Protection of Personal Information (APPI).[7] The EU and Japan have also announced a trade agreement that includes a reciprocal data adequacy determination, creating the world's largest exchange of safe data flows and boosting digital trade between the two zones.[8] Other nations, from India[9] to Brazil,[10] are passing privacy laws or updating existing data protection regimes.[11]

Current business practices along with new technologies are being shaped by laws around the world, while the U.S. approach to data protection remains outdated and insufficient. The continuation of cross-border data flows, which are crucial to the United States' leadership role in the global digital economy, are under stress. This may put U.S. companies, from financial institutions to cloud providers, at a disadvantage due to the perception that our laws are inadequate. Congress must ensure that the U.S. is not left behind as the rest of the world establishes trade and privacy frameworks that will de facto define the terms of international information and technology transfers for decades to come.

The United States currently does not have a baseline set of legal protections that apply to all commercial data about individuals regardless of the particular industry, technology, or user base. For the past decades, we have taken a sectoral approach to privacy that has led to the creation of federal laws that provide strong protections only in certain sectors such as surveillance,[12] healthcare,[13] video rentals,[14] education records,[15] and children's privacy.[16] As a result, U.S. federal laws currently provide strong privacy and security protection for information that is often particularly sensitive about individuals but it leaves other – sometimes similar – data largely unregulated aside from the FTC's Section 5 authority to enforce against deceptive or unfair business practices.[17] For example, health records held by hospitals and covered by the Health Insurance Portability and Accountability Act (HIPAA)[18] are subject to strong privacy and security rules, but health-related or fitness data held by app developers or online advertising companies

---

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj
[7] Japanese Act on Protection of Personal Information (Act No. 57/2003).
[8] Press Release: European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, European Commission (Jan. 23 2019), http://europa.eu/rapid/press-release_IP-19-421_en.htm
[9] Mayuran Palanisamy and Ravin Nandle, *Understanding India's Draft Data Protection Bill* (Sep 13, 2018), IAPP Privacy Tracker, https://iapp.org/news/a/understanding-indias-draft-data-protection-bill.
[10] Lei 13.709/18, Lei Geral de Proteção de Dados Pessoais (Brazil General Data Protection Law).
[11] *Data Privacy Law: The Top Global Developments in 2018 and What 2019 May Bring*, DLA Piper (Feb. 23 2019), https://www.dlapiper.com/en/us/insights/publications/2019/02/data-privacy-law-2018-2019/
[12] Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510–22.
[13] Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. No. 104-191, 110 Stat. 1938 (1996).
[14] Video Privacy Protection Act of 1988 (VPPA), 18 U.S.C. § 2710.
[15] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.
[16] Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506.
[17] Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a).
[18] Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR § 164.524.

is not covered by HIPAA and is largely unregulated. Student data held by schools and covered by the Family Educational Rights and Privacy Act (FERPA)[19] is subject to federal privacy safeguards, but similar data held by educational apps unaffiliated with schools is not subject to special protections. The Fair Credit Reporting Act (FCRA)[20] helps ensure the accuracy of third-party information used to grant or deny loans, but FCRA's accuracy requirements do not apply to similar third-party reviews used to generate user reputation scores on online services.

The U.S. has not always lagged behind its major trade partners in privacy and data protection policymaking. In fact, the central universal tenets of data protection have U.S. roots. In 1972, the Department of Health, Education, and Welfare formed an Advisory Committee on Automated Data Systems, which released a report setting forth a code of Fair Information Practices.[21] These principles, widely known as the Fair Information Practice Principles (FIPPs), are the foundation of not only existing U.S. laws but also many international frameworks and laws, including GDPR.[22] And while GDPR is the most recent major international legislative effort, the U.S. should look for interoperability with and insights from the OECD Privacy Guidelines[23] and the Asia-Pacific Economic Cooperation (APEC) framework and Cross-Border Privacy Rules (CBPRs).[24]

As privacy concerns continue to escalate, states around the U.S. are charging ahead, proposing, passing, or updating consumer privacy laws.[25] Many of these laws are serious, nuanced efforts to provide individuals with meaningful privacy rights and give companies clarity regarding their compliance obligations. At the same time, multiple, inconsistent state law requirements risk creating a conflicting patchwork of laws that create uncertainty for organizations that handle personal information. Individuals deserve consistent privacy protections regardless of the state they happen to reside in.

The U.S. has a shrinking window of opportunity to regain momentum at both the national and international level. If we wait too long, more countries and states will act, which will have an immediate impact on new technologies and business initiatives and ultimately reduce the impact of any federal law.

There are key points that need to be addressed with particular care in any federal consumer privacy law. A baseline federal privacy law should offer strong protections.[26] This, in turn, will

---

[19] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.
[20] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681.
[21] Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health & Human Services (1973), https://aspe.hhs.gov/report/records- computers-and-rights-citizens.
[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[23] Organization for Economic Co-operation and Development, Privacy Guidelines, https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm
[24] APEC has 21 members comprising nearly all of the Asian-Pacific economies, including the United States, China and Russia. The CBPR system—endorsed by APEC member economies in 2011 and updated in 2015 attempts to create a regional solution across 21 member economies, whose governments are at different stages of compliance with the APEC Privacy Framework. In the United States, the Federal Trade Commission has agreed to enforce the CBPRs. Eight APEC countries have formally joined the CBPR system—United States, Canada, Mexico, Japan, Singapore, Taiwan, Australia and the Republic of Korea. In the recent United States-Mexico-Canada Agreement (USMCA), which Congress is reviewing as it considers ratification, the three countries promote cross-border data flows by recognizing the CBPR system as a valid data privacy compliance mechanism for data-transfers between the countries. *See* Cross-Border Privacy Rules System, http://cbprs.org/ (last visited Apr. 28, 2019). Also relevant for the Committee's reference is Convention 108 of the Council of Europe, an international data protection treaty that has been signed by 54 countries to date, not including the United States.
[25] See Mitchell Noordyke, U.S. State Comprehensive Privacy Law Comparison, IAPP (April 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/.
[26] Leading scholars and advocates have expressed skepticism about market-based responses to privacy and security concerns. Common criticisms of a purely market-driven approach include: consumers' lack of technical sophistication

bolster trust in privacy and security practices. The law will regulate a substantial share of the U.S. economy, and must therefore be drafted with careful attention to its effects on every sector as well as a wide range of communities, stakeholders, and individuals.

Eighteen years ago, I left my job as the New York City Consumer Affairs Commissioner to become one of the first company chief privacy officers (CPO) in the U.S. Working for eight years in privacy and consumer protection roles at major tech companies helped me understand that it takes people, systems, and tools to manage data protection compliance. I have also served as a state legislator and a Congressional staffer, and today at FPF work with companies, foundations, academics, regulators, and civil society to seek practical solutions to privacy problems. With this perspective, gained from my experience with key stakeholder groups and ongoing focus on the protection of privacy of individuals and consumers, I offer the following views.

1. Covered Data and Personal Information Under a Federal Privacy Law

In drafting baseline federal privacy legislation, the most important decision is one of scope: how should the law define the "personal information" that is to be protected? Laws that adopt an overly broad standard are forced to include numerous exceptions in order to accommodate necessary or routine business activities, such as fraud detection, security, or compliance with legal obligations; or to anticipate future uses of data, such as scientific research or machine learning. Conversely, laws that define personal information too narrowly risk creating gaps that allow risky uses of data to go unregulated.

Leading government and industry guidelines recognize that data has a range of linkability where it can potentially be used to identify or contact an individual or to customize content to an individual person or device.[27] A federal privacy law should avoid classifying covered data in a binary manner as either "personal" or "anonymous." Instead, it should draw distinctions between different states of data given their materially different privacy risks. Context matters. Personal data that is intended to be made public should be regulated differently than personal data that will be kept confidential by an organization.[28] Similarly, data that is out in the wild should not be

---

with respect to data security (See, e.g., Aaron Smith, *What the Public Knows About Cybersecurity*, Pew Research Center (Mar. 22, 2017), http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/ (last accessed on Nov. 9, 2018); the typical length and substance of modern privacy notices (*See e.g.*, Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society, at 8-10, (2008)); research suggesting that most individuals do not adequately value future risks (*See e.g.*, Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest L. Rev. 261, 303-05 (2014)); the design of user interfaces to encourage decisions that are not aligned with users' best interests (*See* Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (2018)); and a lack of sufficient protections for privacy as an economic externality or "public good" (Joshua A. T. Fairfield and Christoph Engel, *Privacy As A Public Good*, 65 Duke L.J. 385, 423–25 (2015)).

[27] According to the Federal Trade Commission (FTC), data are not "reasonably linkable" to individual identity to the extent that a company: (1) takes reasonable measures to ensure that the data are deidentified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data (the "Three-Part Test"). Federal Trade Commission, Protection Consumer Privacy In An Era of Rapid Change (2012), at 21, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumerprivacy-era-rapid-change-recommendations/120326privacyreport.pdf. According to the National Institute of Sciences and Technology (NIST), "all data exist on an identifiability spectrum. At one end (the left) are data that are not related to individuals (for example, historical weather records) and therefore pose no privacy risk. At the other end (the right) are data that are linked directly to specific individuals. Between these two endpoints are data that can be linked with effort, that can only be linked to groups of people, and that are based on individuals but cannot be linked back." Simson L. Garfinkel, NISTIR 8053, *De-Identification of Personal Information* (Oct. 2015), at 5, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf. Leading industry associations provide similar guidelines. *See, e.g.*, Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data (Nov 2011), at 8, *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf (considering data to be deidentified "when an entity has taken reasonable steps to ensure that the data cannot reasonably be re-associated or connected to an individual or connected to or be associated with a particular computer or device.").

[28] *See, e.g.*, *Netflix Prize*, Netflix, https://www.netflixprize.com/ (last accessed April 28, 2019) (releasing data publicly as part of a contest to improve user recommendations); Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization*

treated the same as data that is subject to technical deidentification controls (such as redacting identifiers, adding random noise, or aggregating records) as well as to effective legal and administrative safeguards (such as commitments not to attempt to re-identify individuals or institutional access limitations).

FPF has crafted modular draft statutory language that attempts to capture these distinctions.[29] We believe, in broad terms, that categories of data that are exposed to individual privacy and security risks, yet materially different in their potential uses and impact, include:[30]

- *Identified data*: information explicitly linked to a known individual.
- *Identifiable data*: information that is not explicitly linked to a known individual but can practicably be linked by the data holder or others who may lawfully access the information.
- *Pseudonymous data*: information that cannot be linked to a known individual without additional information kept separately.
- *deidentified data*: (i) data from which direct and indirect identifiers[31] have been permanently removed; (ii) data that has been perturbed to the degree that the risk of re-identification is small, given the context of the data set; or (iii) data that an expert has confirmed poses a very small risk that information can be used by an anticipated recipient to identify an individual.

By recognizing such distinctions, federal privacy legislation would craft tiers of safeguards that are commensurate to privacy risks while at the same time allowing for greater flexibility where it is warranted. For example, on the one hand, appropriate regulatory requirements for deidentified data might mandate that companies cannot make such data public or share it with third parties without technical, administrative, and/or legal controls that reasonably prevent re-identification. But it may be appropriate to exempt deidentified data from other requirements, such as providing users with access or portability rights or the right to object to or opt-out of a company's use of deidentified data, since by definition it is not technically feasible to link deidentified data to a particular, verifiable individual. On the other hand, for pseudonymous or identifiable data that can be reasonably linked to a known individual, it may be more fitting to provide individuals with access and portability rights, or the ability to opt-in or opt-out of certain uses of that data, as appropriate.

In many cases, the ability to reduce the identifiability of personal data through technical, legal, and administrative measures will allow a company to retain some utility of data (e.g., for research, as we discuss below),[32] while significantly reducing privacy risks. New advances in deidentification and related privacy-enhancing technologies (PETs) (discussed below at number 5) are continuing to emerge.[33] As a result, it is wise for lawmakers to take account of the many states of data and to provide incentives for companies to use technical measures and effective controls reduce the identifiability of personal data wherever appropriate.

---

of Large Sparse Datasets (2018), https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (re-identifying records of known Netflix users).

[29] See Appendix D.

[30] *See generally*, Jules Polonetsky, Omer Tene, & Kelsey Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, Santa Clara L. Rev. (2016); A Visual Guide to Practical De-identification, Future of Privacy Forum, https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/.

[31] Direct identifiers are data that directly identifies a single individual, for example names, social security numbers, and email addresses. Indirect identifiers are data that by themselves do not identify a specific individual but that can be aggregated and "linked" with other information to identify data subjects, for example birth dates, ZIP codes, and demographic information. Simson L. Garfinkel, NISTIR 8053, *De-Identification of Personal Information* (Oct. 2015), at 15, 19, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

[32] See section 3 below.

[33] See section 5 below.

2. Sensitive Data

The term sensitive data is used to refer to certain categories of personal data that require additional protections due to the greater risks for harm posed by processing or disclosing this data. While individuals should generally be able to exercise reasonable control over their personal information, those controls should be stronger with respect to sensitive data. Thus, a federal privacy law should provide heightened protections for the collection, use, storage, and disclosure of users' sensitive personal information or personal information used in sensitive contexts. FPF has crafted modular draft statutory language that proposes a practical approach to regulating sensitive data that is consistent with current norms and best practices.[34]

The Federal Trade Commission has defined sensitive data to include, at a minimum, data about children, financial and health information, Social Security numbers, and precise geolocation data.[35] The GDPR defines sensitive data more broadly by recognizing special categories of personal data as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[36] Under GDPR, the legal grounds for processing these special categories of data are more restricted.[37]

In addition to opt-in controls, federal legislation should include additional requirements – such as purpose limitation and respect for context – for certain sensitive categories of data. For example, if information such as a user's precise geolocation or health information is collected with affirmative consent for one purpose (such as providing a location-based ridesharing service, or a fitness tracking app), a law should restrict sharing that sensitive, identifiable information with third parties for materially different purposes without user consent. This is consistent with the choice principle in the FTC's 2012 Report, which urged companies to offer the choice at the point in time, and in a context, in which a consumer is making a decision about his or her data.[38] There may be instances where sensitive data will require consent, and where such consent will be impossible to obtain.[39] The law should provide for the creation of a transparent, independent ethical review process that can assess such cases and provide a basis for a decision that a use of data is beneficial and will not result in harm.

3. Research

It is vital that a national privacy law be crafted in a way that does not unduly restrict socially beneficial research, and that policymakers at the local, state, and federal levels continue to have the information they need to make evidence-based decisions. Today, in addition to the entities governed by the HIPAA Rule and legal mandates around human subject research,[40] many private

---

[34] See Appendix D.
[35] Federal Trade Commission, *Protection Consumer Privacy In An Era of Rapid Change* (2012), at 8, 58-60. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[36] GDPR, Article 9.
[37] GDPR, Article 9, Recital 51-52.
[38] Federal Trade Commission, *Protection Consumer Privacy In An Era of Rapid Change* (2012), at 60. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[39] For example, recruiting individuals for rare disease drug trials.
[40] 45 CFR 46 (amended 2018). Currently, 20 U.S. agencies and departments intend to follow the revised Common Rule and their CFR numbers. See U.S. Department of Health & Human Services, Federal Policy for the Protection of Human Subject ('Common Rule') https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html (last visited Mar. 8, 2019).

companies also conduct research, or work in partnerships with academic researchers, to gain important insights from the data they hold.

While obtaining individuals' informed consent may be feasible in controlled research settings, it is often impossible or impractical for researchers studying databases that contain the footprints of millions, or indeed billions, of data subjects. For example, when researchers are studying the effectiveness of personalized learning tools or evaluating disparate impacts of automated systems, they can benefit from access to large datasets. Legal mandates that require data holders to obtain continual permission from individuals for future uses of data – while appropriate in many commercial contexts – may create undue burdens for researchers who rely on datasets that contain information about individuals who cannot be contacted or who have been deidentified, particularly if researchers do not know, at the point of collection, what insights future studies may reveal.

This does not mean that data-based research should be exempted from a federal privacy law. The use of private commercial data for socially beneficial research should remain subject to strict standards for privacy, security, scientific validity, and ethical integrity.[41] However, we recommend that legal frameworks contain flexible provisions for research, such as enforceable voluntary compliance with federal Common Rule for human subject research; carefully tailored exceptions to the right of deletion for less readily identifiable information; or the creation of independent ethical review boards to oversee and approve beneficial research using personal information.

This balance between facilitating data research and evidence-based decision-making while maintaining privacy and ethical safeguards aligns with the 2017 report of the bipartisan Commission on Evidence-Based Policymaking and the 2018 Foundations for Evidence-Based Policymaking Act.[42] The Commission noted that increasing access to confidential data need not necessarily increase privacy risk. Rather, "steps that can be taken to improve data security and privacy protections beyond what exists today, while increasing the production of evidence."[43]

In short, companies that conduct research or partner with academic institutions must do so in a way that protects privacy, fairness, equity, and the integrity of the scientific process, and a federal privacy law should encourage, rather than place undue burdens on, legitimate research when appropriate ethical reviews take place.

4. Internal Accountability and Oversight

A federal baseline privacy law should incentivize companies to employ meaningful internal accountability mechanisms, including privacy and security programs, which are managed by a privacy workforce. Ultimately, to implement privacy principles on the ground, including not just legal compliance but also privacy by design and privacy engineering, organizations will need to devote qualified and adequately trained employees. Indeed, over the past two decades, a privacy workforce has developed that combines the fields of law, public policy, technology, and business management. This workforce's professional association, the International Association of

---

[41] In the words of danah boyd and Kate Crawford, "It may be unreasonable to ask researchers to obtain consent from every person who posts a tweet, but it is problematic for researchers to justify their actions as ethical simply because the data are accessible. Future of Privacy Forum, *Conference Proceedings: Beyond IRBS: Designing Ethical Review Processes for Big Data Research* (Dec. 20, 2016), page 4, https://fpf.org/wp-content/uploads/2017/01/Beyond-IRBs-Conference-Proceedings_12-20-16.pdf, *citing* danah boyd & Kate Crawford, Critical Questions for Big Data, 15(5) INFO. COMM. & SOC. 662 (2012).

[42] Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, 132 Stat. 5529 (2019).

[43] Report of the Commission on Evidence-Based Policymaking, 8 (September 2017) https://www.cep.gov/report/cep-final-report.pdf.

Privacy Professionals (IAPP), has doubled its membership in just the past 18 months.[44] The IAPP provides training and professional certification, demonstrating the heightened demand among organizations for professionals who manage data privacy risks.

In their book *Privacy on the Ground*, Kenneth Bamberger and Deirdre Mulligan stress "the importance of the professionalization of privacy officers as a force for transmission of consumer expectation notions of privacy from diverse external stakeholders, and related 'best practices,' between firms."[45]

Accordingly, today, data privacy management should no longer be regarded as a role that employees in legal or HR departments fulfill as a small piece of their larger job. Rather, it must be a new professional role with standards, best practices, and norms, which are widely agreed upon not only nationally but also across geographical borders. Responsible practices for personal data management are not common knowledge or intuitive, any more than accounting rules. They require training, continuous education, and verifiable methods for identifying and recognizing acceptable norms. Put simply, the digital economy needs privacy professionals. Encouraging organizations to implement internal governance programs that employ such professionals will ensure higher professional standards and more responsible data use, regardless of the specific rules ultimately chosen for data collection, processing, or use.

Federal legislation could provide a safe harbor or other incentives for development, documentation, and implementation of comprehensive data privacy programs; execution of ongoing, documented privacy and security risk assessments, including for risks arising from automated decision-making; and implementation of robust accountability programs with internal staffing and oversight by senior management. For example, GDPR requires companies to document their compliance measures,[46] appoint Data Protection Officers,[47] and create data protection impact assessments,[48] among other requirements. Another way to increase internal expertise is to incentivize employee training through recognized programs.

External certification processes act as objective validators to help companies, particularly those with limited resources, navigate complex legal requirements. Similarly, incentivizing companies or industry sectors to create "red teams" to proactively identify privacy abuses or to cooperate with watchdog entities or independent monitors to support additional oversight, such as through safe harbors or other methods, would create an additional layer of privacy safeguards.

5. Incentives for Technical Solutions

Federal privacy legislation should promote the use of technical solutions, including privacy-enhancing technologies (PETS). The "holy grail" for data protection is utilizing technology that can achieve strong and provable privacy guarantees while still supporting beneficial uses. Legislation should create specific incentives for the use of existing privacy-enhancing technologies and for the development of new PETS. Following are ten PETS or technological trends that may become increasingly useful tools to manage privacy risks:

Advances in Cryptography

---

[44] See IAPP-EY Annual Governance Report (2018), https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf.
[45] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247, 252 (2010).
[46] GDPR, Art. 24, 40.
[47] GDPR, Art. 37-39.
[48] GDPR, Art. 35.

a. **Zero Knowledge Proofs** – Zero knowledge proof (ZKPs) are cryptographic methods by which one party can prove to another party that they know something to be true without conveying any additional information (like how or why the mathematical statement is true). ZKPs can be used in identity verification contexts, e.g. to prove that someone is over a certain age without revealing their exact date of birth. ZKPs help with data minimization and data protection and promote privacy by design and default.

b. **Homomorphic Encryption** – Homomorphic encryption is a process that enables privacy-preserving data analysis by allowing some types of analytical functions and computations to be performed on encrypted data without first needing to decrypt the data.[49] It is especially useful in applications that retain encrypted data in cloud storage for central access.

c. **Secure Multi-Party Computation** – Secure multi-party computation (SMPC) is a distributed computing system or technique that provides the ability to compute values of interest from multiple encrypted data sources without any party having to reveal their private data to the others. A common example is secret sharing, whereby data from each party is divided and distributed as random, encrypted "shares" among the parties, and when ultimately combined can provide the desired statistical result.[50] If any one share is compromised, the remaining data is still safe. SMPC holds particular promise for sharing or managing access to sensitive data such as health records.

d. **Differential Privacy** – Differential privacy (DP) is a rigorous mathematical definition of privacy that quantifies the risk that an individual is included in a data set. It leverages anonymization techniques that involves the addition of statistical "noise" to data sets before calculations are computed and results released. DP can be global or local.[51] Global DP is server-side anonymization or deidentification (where trust resides in the service provider); local DP is applied on the client or user's device. There are now differentially private versions of algorithms in machine learning, game theory and economic mechanism design, statistical estimation, and streaming. Differential privacy works better on larger databases because as the number of individuals in a database grows, the effect of any single individual on a given aggregate statistic diminishes.

Localization of Processing

e. **Edge computing and Local Processing** – For devices where speed is of the essence or connectivity is not constant, applications, data, and services are increasingly run away from centralized nodes at the end points of a network. Such local processing helps with data minimization by reducing the amount of data that must be collected (accessible) by the service provider, or retained on a centralized service or in cloud storage.

f. **Device-Level Machine Learning** – New machine learning focused semiconductor components and algorithms—along with the speedy, low-cost local storage and local processing capabilities of edge computing —are allowing tasks that use to require the computing horsepower of the cloud to be done in a more refined and more focused way on edge devices.

---

[49] *See* David Wu, University of Virginia Computer Science Department, *available at* https://www.cs.virginia.edu/dwu4/fhe-project.html.
[50] *See* Christopher Sadler, *Protecting Privacy with Secure Multi-Party Computation*, New America (Jan. 11, 2018), https://www.newamerica.org/oti/blog/protecting-privacy-secure-multi-party-computation/.
[51] Evaluation of Privacy-Preserving Technologies for Machine Learning, Outlier Ventures Research (Nov. 2018), https://outlierventures.io/research/evaluation-of-privacy-preserving-technologies-for-machine-learning/.

g. **Identity Management** – Many identity management solutions under consideration or development leverage a variety of platforms, including distributed ledger technology (described above), and local processing, that capitalize on device-level machine learning to provide the ability for individuals to verify and certify their identify. This enables people without internet access beyond smartphones or other simple devices to form secure connections, exchange identity-related credentials (such as transcripts or voting records) without going through a centralized intermediary. Verified personal data can be accessed from the user's device and shared via secure, encrypted channels to third parties, with data limited to the basic facts necessary for the relying party (e.g. that the individual is over 21, or does in fact qualify for a specific government service) on an as-needed basis. Depending on the implementation and standards, identity management can create privacy risks or can be deployed to support data minimization and privacy by design and default.

Advances in Artificial Intelligence (AI) & Machine Learning (ML)

h. **"Small Data"** – Small data AI and machine learning systems use significantly less, or even no real data, via techniques such as data augmentation (manipulating existing data sets), transfer learning (importing learnings from a preexisting model), synthetic data sets (see below), and others.[52] With small data techniques, the future forms of AI might be able to operate without needing the tremendous amounts of training data currently required for many applications.[53] This capability can greatly reduce the complexity and privacy risks associated with AI and ML systems.

i. **Synthetic Data Sets** – Synthetic data sets are sets of artificial data created to replicate the patterns and analytic potential of real data about real individuals or events by replicating the important statistical properties of real data.[54] They can be created at a vast scale and reduce the need for large training or test data sets, particularly for AI and ML applications, and thus support reduced data sharing or secondary use concerns.

j. **Generative Adversarial Networks** – Generative Adversarial Networks (GANs) are a type of artificial intelligence, where algorithms are created in pairs (one to "learn," and the other to "judge"). Used in unsupervised machine learning, two neural networks contest with each other in a framework to produce better and better simulations of real data (creating faces of people, or handwriting). One valuable use: generating synthetic data sets.[55]

These tools and resources can potentially help mitigate data protection concerns posed by future technologies. Federal legislation could incentivize the growth and development of new PETS. The market for compliance tools for privacy and security professionals also continues to accelerate. Services that discover, map, and categorize data for organizations, wizards that help manage and complete privacy impact assessments, programs that handle data subject access requests and consent management, and deidentification services are already supporting privacy and security professionals at leading organizations as well as attracting investor interest.[56] Data protection resources entering the marketing are increasingly central to building systems that

---

[52] Harsha Angeri, *Small Data & Deep Learning (AI): A Data Reduction Framework*, Medium (Apr. 1, 2018), https://medium.com/datadriveninvestor/small-data-deep-learning-ai-a-data-reduction-framework-9772c7273992.
[53] H. James Wilson, Paul R. Daugherty, Chase Davenport, *The Future of AI Will Be About Less Data, Not More*, Harvard Business Review (Jan. 14, 2019), https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more.
[54] Applied AI, *Synthetic Data: An Introduction & 10 Tools*, (June 2018 update), https://blog.appliedai.com/synthetic-data/.
[55] Dan Yin and Qing Yang, *GANs Based Density Distribution Privacy-Preservation on Mobility Data*, Security and Communication Networks, vol. 2018, Article ID 9203076, (Dec. 2, 2018), https://doi.org/10.1155/2018/9203076.
[56] IAPP Privacy Tech Vendor Report (2018), https://iapp.org/resources/article/2018-privacy-tech-vendor-report/

allow professionals to manage the challenges that accompany the expanded data collection and the multiplying uses that shape modern business practices.

6. Machine Learning

A federal privacy law should also promote beneficial uses of artificial intelligence (AI) and machine learning. Many device manufacturers are making strides to minimize data collection by conducting data processing on-device (locally) rather than sending data back to a remote server. However, AI and machine learning technologies typically require large and representative data sets to power new models, to ensure accuracy, and to avoid bias. A U.S. framework would be wise to ensure that uses of data for machine learning are supported when conducted responsibly. To assess such responsible uses, we again recommend the development of a serious ethics review process. The academic IRB is well established as a necessary way for federally funded human subject research to be vetted.[57] Counterparts for corporate data will be important, if structured to provide expertise, confidentiality, independance, transparency of process, speed, and expertise.[58]

7. Interaction with Existing Legal Frameworks

A federal baseline privacy law should take into consideration existing legal frameworks, by preempting certain state laws where they create conflicting or inconsistent requirements, and superseding or filling gaps between existing federal sectoral laws. While recognizing the United States' unique global privacy leadership, a federal privacy law should also address issues of interoperability with GDPR and other global legal regimes. At a minimum, it is important for the U.S. to protect cross-border data flows by not creating obligations that directly conflict with other existing international frameworks.

A. Interaction with State Laws

The drafting of a federal privacy law in the United States will necessarily impact the range of state and local privacy laws that have been passed in recent decades or are currently being drafted. The question of preemption is at the forefront of many conversations regarding a federal privacy bill. Stakeholders from government, industry, civil society, and academia have expressed strong and sometimes conflicting views. At a minimum, we should seek to avoid a framework where web site operators are expected to comply with multiple inconsistent state mandates on the many day-to-day issues at the core of the digital economy, ranging from signing users up for email lists, implementing web site analytics, or conducting e-commerce. These concerns can reasonably be avoided with carefully crafted federal preemption, so long as the law also ensures a strong level of uniform privacy protections, certainly meeting and exceeding the core protections of the California Consumer Privacy Act (CCPA).

It is important to recognize that lawmakers' options are not binary. The choice is not between a preemptive federal law and a non-preemptive federal law. Rather, lawmakers must grapple with a range of state authorities and choose which to preempt and which to preserve.[59] I provide further context below. My core recommendations are that Congress: (1) preserve state Unfair and

---

[57] Protection of Human Subjects, 45 C.F.R. §§ 46.103, 46.108 (2012).
[58] See Future of Privacy Forum, *Conference Proceedings: Beyond IRBS: Designing Ethical Review Processes for Big Data Research* (Dec. 20, 2016), https://fpf.org/wp-content/uploads/2017/01/Beyond-IRBs-Conference-Proceedings_12-20-16.pdf.
[59] Peter Swire, US federal privacy preemption part 1: History of federal preemption of stricter state laws (Jan 9, 2019), IAPP Privacy Tracker, https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/.

Deceptive Acts and Practices (UDAP) laws, which regulate a wide range of commercial conduct, from fair pricing to honest advertising, when they do not specifically target privacy or security requirements; (2) preempt generally applicable consumer privacy laws, like the California Consumer Privacy Act (CCPA); and (3) be thoughtful about which state sectoral privacy laws to preempt or preserve.

For example, to the extent that a federal law contains provisions that conflict with state common law or statutes, the latter will be preempted by default.[60] Congress may, to the extent it wishes, take further steps to prevent states or local governments from drafting further new, different, or more protective laws, through express or implied "field preemption." Within this range, there is great flexibility in the extent to which a federal law can have preemptive effect.[61]

As this Committee considers the appropriate balance of federal and state intervention in the field of information privacy, it should carefully consider how a federal privacy law will impact certain key aspects of current state regulation:

- **State UDAP Laws**. Every state has broadly applicable Unfair and Deceptive Acts and Practices (UDAP) laws that prohibit deceptive commercial practices or unfair or unconscionable business practices.[62] State enforcement authorities have increasingly applied UDAP laws to data-driven business practices such as mobile apps and platform providers.[63] In general, states should maintain the freedom to enforce broadly applicable commercial fairness principles in a technology-neutral manner, to the extent that they do not specifically regulate the collection and processing of personal information addressed in the federal law.

- **State Constitutions**. Eleven states have enumerated constitutional rights to privacy, most of which were created through constitutional amendments in the last 50 years.[64] In addition to governing law enforcement access to information, some states have chosen to express a free-standing fundamental right to privacy.[65] These amendments to state constitutions reflect the states' explicit intention to extend – or clarify – the fundamental rights of their own residents beyond the existing status quo of federal legal protections.

- **State Sector-Specific Laws.** Comprehensive state efforts to regulate consumer privacy and security, such as generally applicable data breach laws or the recent California Consumer Privacy Act, are likely to be partially or fully preempted by a federal law that meaningfully addresses the same issues and creates similar substantive legal protections. However, a federal law should also carefully anticipate its effect on sectoral state efforts,

---

[60] Supremacy Clause, U.S. CONST. art. VI, cl. 2.
[61] See generally, Paul M. Schwartz, Preemption and Privacy, 118 Yale L.J. 902 (2008), *available at* https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1071&context=facpubs.
[62] National Consumer Law Center, *Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws*, (Mar. 2018), http://www.nclc.org/images/pdf/udap/udap-report.pdf.
[63] *See* e.g. Federal Trade Commission, *Privacy & Data Security Update: 2017*, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf. (As one of the examples of state enforcement actions, the FTC and 32 State Attorneys General alleged that Lenovo engaged in an unfair and deceptive practice by selling consumer laptops with a preinstalled software program that accessed consumer's sensitive personal information transmitted over the Internet without the consumer's knowledge or consent.)
[64] *See* National Conference of State Legislatures, *Privacy Protections in State Constitutions* (Nov. 7, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.; Gerald B. Cope, Jr., *Toward a Right of Privacy as a Matter of State Constitutional Law*, 5 Fla. St. U. L. Rev. 631, 690-710 (2014).
[65] *See* e.g. Cal. Const., art. I, § 1; Haw. Const., art. I, §§ 6-7; Alaska Const., art. I, § 22.

such as those regulating biometrics,[66] drones/UAV,[67] or employer or school ability to ask for social media credentials.[68] For example, in the field of student privacy, more than 120 state laws have passed since 2013 regulating local and state education agencies and education technology companies,[69] and replacing those laws with a general consumer privacy law could eliminate important nuances that those laws incorporated; for example, a consumer privacy law would likely allow for users to delete their data, but, in the education context, students obviously should not have the ability to delete a homework assignment or test scores. Further complicating these matters, states retain a constitutional right to regulate the core behavior of their own governmental entities, including the regulation of school districts.[70]

B. Interaction with Federal Sectoral Laws

In some cases, it may be appropriate for a baseline, comprehensive federal privacy law to supersede and replace existing sectoral federal laws where a consistent baseline set of obligations would be beneficial. In other cases, the wide range of existing sectoral laws, including privacy laws and anti-discrimination laws, may be well suited to address concerns around automated decision-making or unfair uses of data.

C. Interaction with Global Privacy Frameworks

The U.S. has an opportunity to demonstrate leadership, protect consumers, and facilitate commerce by crafting a federal privacy law that ensures interoperability with international data protection laws. Just as the U.S. is currently confronting challenges posed by an assortment of privacy-focused state laws, disparate privacy regimes with varying degrees of privacy protections and controls are proliferating internationally. These laws and the corresponding multiplicity of compliance obligations adversely affect cross-border data flows and the multinational businesses that rely on such flows to remain competitive.

Legislation should consider and address, as much as possible, interoperability with other nations' privacy frameworks.[71] For example, legislation should promote interoperability with the most well-known example of a comprehensive privacy law, GDPR, which provides an extensive framework for the collection and use of personal data. The basic principles of GDPR should provide a reference for policymakers during the legislative process, with an understanding that the U.S. approach to privacy and other constitutional values may diverge in many areas, such as breadth of data subject rights, recognition of First Amendment rights, and the need for minimization requirements that may impact data use for AI and machine learning purposes. Also important for comparison are the OECD privacy guidelines and the APEC CBPS, particularly since the proposed United States-Mexico-Canada Agreement (USMCA), which Congress is reviewing as it

---

[66] Biometric Information Privacy Act (BIPA), 740 ILCS/14 (2008).
[67] National Council of State Legislatures, *Current Unmanned Aircraft State Law Landscape* (Sept. 10, 2018). http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.
[68] National Council of State Legislatures, *State Social Media Privacy Laws* (Nov. 6, 2018). http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx.
[69] State Student Privacy Laws, FERPA|Sherpa (April 23, 2019), https://ferpasherpa.org/state-laws.
[70] *See* U.S. CONST. art. X; Sonja Ralston Elder, *Enforcing Public Educational Rights Via a Private Right of Action*, 1 Duke Forum For L. & Soc. Change 137, 154 (2009).
[71] Per a McKinsey report, "Cross-border data flows are the hallmarks of 21st-century globalization. Not only do they transmit valuable streams of information and ideas in their own right, but they also enable other flows of goods, services, finance, and people." McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, (March 2016) at 30, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx.

considers ratification, recognizes the CBPR system as a valid data privacy compliance mechanism for data-transfers between the countries.

A federal baseline privacy law should also promote cross-border data flows by avoiding the creation of obligations that directly conflict with other international laws. For example, an emergence of recent data localization laws have expressly prohibited data transfers or mandated highly-restrictive regulatory environments, resulting in inefficient and burdensome requirements for activities including: data storage, management, processing, and analytics. Countries that erect these barriers to data flows often cite concerns about cybersecurity, national security, and privacy.[72] Localization detrimentally impacts businesses,[73] consumers who benefit from free flows of data, and potentially data security. Thoughtful data governance and oversight policies with data subject rights and other protections can address data protection issues without resorting to a regulatory environment that employs localization as a solution.

8. Rulemaking, Civil Penalties, and Enforcement

No matter how well crafted, a privacy law will almost certainly require a well-resourced administrative mechanism to clarify certain terms and standards. In Europe, the GDPR contemplates that guidance from Data Protection Authorities will clarify key concepts and requirements. In California, the CCPA tasks the state attorney general with promulgating rules on complicated aspects of the statute. Under federal law, Congress provided for the FTC to issue regulations under the COPPA statute that have helped define key provisions and enable the law's safe-harbor program for the collection and use of children's data.

A comprehensive federal privacy law is no different. I urge the Committee to carefully consider what aspects of a federal law might benefit from regulatory clarity or guidance over time. And I urge legislative drafters to empower the FTC to provide such clarity, with specific parameters and considerations to take into account and subject to reasonable guardrails on the agency's authority. The Commission and other stakeholders have agreed, and noted that additional investigatory resources would be welcome.[74] The Commission receives many consumer complaints and would benefit from the ability to hire more technology and legal experts. Enhanced resources, and the deeper understanding of technology and business practices they bring to the Commission, can lead to fairer outcomes for both individuals and companies.

The authority to bring civil penalties is another key aspect of the FTC's current oversight of global technology firms. But today, the FTC can only fully exercise this oversight regarding companies with whom the Commission has entered into settlement agreements. Civil penalty authority in the

---

[72] The U.S. International Trade Commission and Department of Commerce have considered these concerns in a series of convenings and reports over the past several years. *See* e.g., U.S. Dept. of Commerce, *Measuring the Value of Cross-Border Data*, (Sept. 30, 2016), https://www.commerce.gov/news/fact-sheets/2016/09/measuring-value-cross-border-data-flows; U.S. Intl. Trade Comm'n, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, (Aug. 2017), https://www.usitc.gov/publications/332/pub4716_0.pdf.

[73] For example, a U.S. International Trade Commission report notes that there are cost, speed, and security advantages to cloud-based technologies. U.S. Intl. Trade Comm'n, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, (Aug. 2017) at 20, https://www.usitc.gov/publications/332/pub4716_0.pdf. A 2016 McKinsey report found a 10.1 percent rise in GDP over 10 years is attributable to cross-border flows. McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, (Mar. 2016) at 30, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx.

[74] FTC Staff, FTC Staff Comment to the NTIA: Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780–8780–01 (November 9, 2019) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

first instance would enable to FTC to bring its oversight to bear on all companies that handle personal data, protecting individuals and consumers and leveling the playing field.

It is also vital that technical assistance be provided if a new law is passed, particularly for small businesses. The FTC can help fulfill this role. A potential model for this is the U.S. Department of Education's Privacy Technical Assistance Center (PTAC), which has played a vital role in providing guidance, technical assistance, and best practices to states, districts, companies, and privacy advocates.[75]

Finally, there has also been a growing recognition of the important role of state attorneys general in the creation and protection of evolving privacy norms.[76] State attorneys general have brought enforcement actions that meaningfully push forward legal protections in many areas.[77] As officials with a broad scope of authority and the freedom to respond to rapidly evolving privacy challenges, they should remain key partners in the enforcement of a baseline federal information privacy law.

Conclusion

This is a critical juncture for U.S. policymaking. Privacy regulation is charging ahead in the EU and in the states. Now is the time for the United States as a nation to reassert its policy leadership, which stretches from Warren and Brandeis' 1890 treatise on *The Right to Privacy,* [78] through William Prosser's explication of the privacy torts in 1960,[79] to the Department of Health, Education, and Welfare's report first outlining the fair information practices in 1972,[80] which are the cornerstone for every data protection framework from OECD to GDPR.

Federal legislation should empower the FTC to rulemake and enforce and allow state AGs to retain enforcement powers. It should recognize broad spectrum of identifiability in definition of PII. It should provide heightened protection for sensitive data or contexts. It should not unduly restrict socially beneficial research find a way to enable crucial data-driven research. It should incentivize and recognize the privacy profession and PETs.

In my view, the best approach would be for Congress to draft and pass a baseline, non-sectoral federal information privacy law. Although I have flagged specific considerations related to such a law's content and its interaction with existing legal frameworks, I overall believe that a strong federal law remains the best approach to guaranteeing clear, consistent, and meaningful privacy and security protections in the United States.

APPENDED:

A. Future of Privacy Forum, Infographic, *Personal Data and the Organization: Stewardship and Strategy*
B. Future of Privacy Forum, Infographic, *A VIsual Guide to Practical De-Identification*

---

[75] U.S. Department of Education, Privacy Technical Assistance Center, https://studentprivacy.ed.gov.
[76] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 785-91 (2016), http://ndlawreview.org/wp-content/uploads/2017/02/NDL205.pdf.
[77] *Id*.
[78] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard L. Rev. 193 (1890), https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.
[79] William L. Prosser, Privacy, 48 Calif. L. Rev. 383 (1960), https://doi.org/10.15779/Z383J3C.
[80] Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health & Human Services (1973), https://aspe.hhs.gov/report/records- computers-and-rights-citizens.

C. Future of Privacy Forum Infographic, *Financial Data Localization: Conflicts and Consequences*
D. Future of Privacy Forum, Draft Legislative Language: “Covered Data”
E. Future of Privacy Forum, *Unfairness by Algorithm: Distilling the Harms of Automated Decision-making* (December 2017)
F. Future of Privacy Forum & Anti-Defamation League, *Big Data: A Tool for Fighting Discrimination and Empowering Groups*