Comments from

THE FUTURE OF PRIVACY FORUM

to

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, DC 20230

Docket Number: 180821780-8780-01

Developing the Administration's Approach to Consumer Privacy

John Verdi, Vice President of Policy
Stacey Gray, Policy Counsel
Michelle Bae, Elise Berkower Memorial Fellow
Amy Oliver, Policy Advisor

THE FUTURE OF PRIVACY FORUM*†
1400 I St. NW Ste. 450
Washington, DC 20005

www.fpf.org

November 9, 2018

* The Future of Privacy Forum (FPF) is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.
† The views herein do not necessarily reflect those of our supporters or our Advisory Board.

Table of Contents

Executive Summary

On September 26, 2018, the U.S. Department of Commerce, the National Telecommunications and Information Administration (hereinafter Department) published a request for public comments on ways to advance consumer privacy while protecting prosperity and innovation.[1] We thank the Department for the opportunity to provide feedback, and commend its efforts to engage all stakeholders on the critical issue of consumer privacy and security in the United States.

The Department has requested input on the best approach to strengthen existing consumer data protections in the United States while promoting the administration's high-level goals, including: enhancing legal clarity; reducing legal fragmentation; and increasing national and global interoperability.

In FPF's view, the best approach would be for Congress to draft and pass a baseline, non-sectoral federal information privacy law. The current U.S. sectoral approach to consumer privacy and security has resulted in incomplete legal protections, and a significant amount of commercial data, even sensitive data, that should be better protected. State legislatures have begun to address these concerns in recent years with a growing patchwork of state and local laws on topics such as data breaches, biometrics, geo-location, and education technology, as well as state and local attempts to regulate the broad range of all commercial data, which can lead to inconsistent and sometimes conflicting requirements. A federal law could reduce confusion, establish legal protections for users across the country, and provide companies with clarity regarding their data protection obligations.

In substance, a federal privacy law should seek to address nuances in what is definable as covered information (personally identifiable information), increase interoperability and decrease conflict with existing international frameworks, promote defaults and controls that are tailored to the sensitivity of data and context of transactions, and establish incentives for regulated entities to build robust internal accountability programs and to engage in socially beneficial uses of data.

Overall, we recommend that the Department:

- Support the drafting and passage of a baseline, non-sectoral federal information privacy law;
- Consider issues of interoperability with existing federal sectoral laws as well as global privacy frameworks, and avoid creating conflicting requirements with existing national and international frameworks in order to promote beneficial cross-border data flows;
- Address a range of important substantive considerations, including: treating covered data with nuance in crafting legislative definitions; promoting internal accountability, oversight, and training; recognizing distinctions between sensitive and non-sensitive data; and creating incentives for socially beneficial uses of data and for technical solutions that can resolve privacy issues while supporting data utility.

[1] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (Sept. 26, 2018), https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy.

I. Federal Legislation

The Request for Comments (RFC) seeks input on the best approach to strengthen existing consumer data protections in the United States while promoting the administration's high-level goals, including: enhancing legal clarity; reducing legal fragmentation; and increasing national and global interoperability.[2] The best way to strengthen consumer data protections and promote these goals is by drafting and passing a baseline, non-sectoral federal information privacy law.

We encourage the Department to support federal legislation rather than encourage states to pursue a non-federal approach or urge stakeholders to create purely non-statutory frameworks. The current federal sectoral approach to consumer data privacy and security in the United States is incomplete, and should be bolstered by the creation of baseline legal protections. A federal law has the potential to provide clear, consistent privacy and security protections that are preferable to the development of a patchwork of inconsistent or conflicting state privacy laws.

A. Current incomplete legal protections

In comparison to the European Union and other governments with comprehensive data privacy laws,[3] the United States does not currently have a baseline set of legal protections that apply to all commercial data about individuals, regardless of the particular industry, technology, or user base. Instead, the United States has taken a sectoral approach that has led to the creation of federal laws that provide strong protections only in certain industries such as surveillance,[4] healthcare,[5] video rentals,[6] education records,[7] or children's privacy.[8]

As a result, U.S. federal laws currently provide strong privacy and security protection for information, which is often particularly sensitive, about individuals collected in certain contexts, while leaving other data largely unregulated aside from the FTC's generally applicable Section 5 authority to enforce *ex post* against deceptive or unfair business practices.[9] For example: health records held by hospitals and covered by the Health Insurance Portability and Accountability Act (HIPAA)[10] are subject to strong privacy and security rules, whereas health-related or fitness data held by app developers or online advertising companies and not covered by HIPAA are largely unregulated; student data held by schools and covered by the Family Educational Rights and Privacy Act (FERPA)[11] are subject to federal privacy safeguards,

[2] *Id*.

[3] 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; Japanese Act on Protection of Personal Information (Act No. 57/2003); Lei 13.709/18, Lei Geral de Proteção de Dados Pessoais (Brazil General Data Protection Law).

[4] Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510–22.

[5] Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. No. 104-191, 110 Stat. 1938 (1996).

[6] Video Privacy Protection Act of 1988 (VPPA), 18 U.S.C. § 2710.

[7] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

[8] Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506.

[9] Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

[10] Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR § 164.524.

[11] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

while data held by educational apps unaffiliated with schools is not subject to special protections; the Fair Credit Reporting Act (FCRA)[12] helps ensure the accuracy of third-party information used to grant or deny loans, while FCRA's accuracy requirements do not apply to third-party reviews used to generate user reputation scores on online services.

Increasingly, states and local political actors are recognizing the inadequacy of this sectoral framework, and responding by passing general privacy laws such as the California Consumer Privacy Act of 2018,[13] as well as legislating in specific areas such as biometrics,[14] geo-location data,[15] data brokers,[16] and education technology.[17]

B. Preference to a non-legislative approach

A baseline federal privacy law would offer strong consumer protections that are not well incentivized by market forces, which in turn helps create consumer trust in privacy and security practices. 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 with respect to data security;[18] the typical length and substance of modern privacy notices;[19] research suggesting that most individuals do not adequately value future risks;[20] the design of user interfaces to encourage decisions that are not aligned with users' best interests;[21] and a lack of sufficient protections for privacy as an economic externality or "public good."[22]

Self-regulatory efforts can sometimes be effective to address rapidly evolving technology or build trust in a new sector where privacy law does not exist or is ambiguous.[23] In particular, industry best practices are most effective when given the force of law.[24] Without such a legal underpinning, even well-intentioned self-regulatory efforts with a strong base of technical and policy support, such as efforts to adopt a

[12] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681.

[13] California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.198(a) (2018).

[14] Biometric Information Privacy Act (BIPA), 740 ILCS/14.

[15] Proposed Illinois Geolocation Privacy Protection Act (815 ILCS 505/2Z) (vetoed by Gov. Bruce Rauner on Sept. 21, 2018).

[16] Vermont Data Broker Law, 9 V.S.A. §§ 2446-2447 (effective January 1, 2019).

[17] State Student Privacy Laws, FERPA SHERPA (July 20, 2018), https://ferpasherpa.org/state-laws/ (last accessed Nov. 9, 2018).

[18] *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).

[19] *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).

[20] *See e.g.*, Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest L. Rev. 261, 303-05 (2014).

[21] *See* Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (2018).

[22] Joshua A. T. Fairfield and Christoph Engel, *Privacy As A Public Good*, 65 Duke L.J. 385, 423–25 (2015).

[23] *See e.g.*, Student Privacy Pledge, https://studentprivacypledge.org/ (last accessed Nov. 9, 2018).

[24] Today, most companies can make voluntary public commitments that are enforceable by the Federal Trade Commission. In limited circumstances, companies can develop or join statutorily recognized safe harbors. *See, e.g.,* Federal Trade Commission, *COPPA Safe Harbor Program*, https://www.ftc.gov/safe-harbor-program (last accessed Nov. 9, 2018).

universally recognized browser-based Do Not Track flag,[25] can fail due to a lack of underlying consensus on appropriate business norms.[26]

C. Avoiding inconsistent or conflicting state laws

Many state and local government responsibilities involve traditionally local issues, such as administering public education systems or regulating businesses with a physical presence or activities within the state. In contrast, data-driven businesses operate largely without geographic borders, insofar as they may collect and share information about individuals across the country or the world without regard to where those individuals are physically located.

As much as possible, data-driven businesses should not be subject to compliance requirements that vary across the country or -- worse -- requirements that conflict. For example, all 50 U.S. states, the District of Columbia, Guam, and the Virgin Islands have passed data breach notification laws.[27] Because many of these laws contain different, at times directly conflicting, requirements, they have led to high compliance costs for businesses.[28]

Similarly, most users of smartphone apps, websites, and technology platforms understand that they are interacting with companies spanning geographical boundaries, and do not expect to have fewer privacy rights -- such as the right to access, correct, or delete information, or to exercise meaningful control over whether that information is used for unexpected purposes, shared with others, or sold -- simply because they live in one state rather than another. Instead, a baseline national privacy law would provide clear, consistent consumer protections and build trust in modern data practices.

II. Interaction with Existing Legal Frameworks

A federal 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 in existing federal sectoral laws. While recognizing the United States' unique global privacy leadership, a U.S. privacy law should also consider notable privacy provisions of the European Union's General Data Protection Regulation (GDPR), and address issues of interoperability where feasible. 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.

[25] World Wide Web Consortium (W3C), *Tracking Protection Working Group*, https://www.w3.org/2011/tracking-protection/ (last accessed Nov. 9, 2018).

[26] *See* Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 Minn. J. L. Sci. & Tech. 281 (2012); Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, Gizmodo (Oct. 15, 2018), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324 (last accessed Nov. 9, 2018).

[27] National Conference of State Legislatures, *Security Breach Notification Laws* (Sep. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last accessed Nov. 9, 2018).

[28] A 2018 Ponemon Institute study of information provided by 477 companies showed an average cost of $3.86 million per breach. The study included legal services, communications with regulators, and determination of regulatory requirements as potentially included in a company's post breach cost calculation. Ponemon Institute, *2018 Cost of a Data Breach Study: Global Overview* (Jul. 2018), https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

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. Pursuant to the Supremacy Clause of the U.S. Constitution,[29] state common law, and even state constitutions, are subordinate to federal regulation where they contain conflicting provisions. In this way, a comprehensive federal privacy law could provide some degree of helpful clarity and certainty, such as by establishing uniform definitions of covered types of information, or the types of data that should be subject to an individual right to access, correct, or delete their data.

Congress may, to the extent it wishes, take further steps to preempt local regulation, and prevent states or local governments from drafting further new, different, or more protective laws within the field of information privacy (through express or implied "field preemption").[30] Although most other federal privacy laws have declined to preempt stronger state protections,[31] a comprehensive, or broadly applicable federal privacy law would be likely to preempt a significant amount of parallel state efforts.

As the Administration 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.[32] State enforcement authorities have increasingly applied UDAP laws to data-driven business practices such as mobile apps and platform providers.[33] In general, states should maintain the freedom to enforce broadly applicable commercial fairness principles in a technology-neutral manner.

- **The Role of State Attorneys General.** There has also been a growing recognition of the important role of state attorneys general in the development of evolving privacy norms.[34] State attorneys general have brought enforcement actions that meaningfully push forward legal protections in areas such as nonconsensual pornography.[35] As officials with a broad scope of

[29] Supremacy Clause, U.S. Const. art. VI, cl. 2.

[30] Within this range, there is great flexibility in the extent to which a federal privacy law could have preemptive effect. See generally, Paul Schwartz, *Preemption and Privacy*, 118 Yale L.J. 902, 922–47 (2008) (exploring the strengths and weaknesses of a federal omnibus privacy law).

[31] *See id* at 916–21.

[32] 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.

[33] *See e.g.*, *Attorney General Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities*, Attorney General of Massachusetts (Apr. 4, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html (last accessed Nov. 9, 2018); *A.G. Schneiderman Announces Results of "Operation Child Tracker," Ending Illegal Online Tracking Of Children At Some of Nation's Most Popular Kids' Websites*, NYS Attorney General (Sept. 13, 2016), https://ag.ny.gov/press-release/ag-schneiderman-announces-results-operation-child-tracker-ending-illegal-online (last accessed Nov. 9, 2018).

[34] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 785–91 (2016).

[35] *See id*.

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.

- **State Constitutions**. Eleven states have enumerated constitutional rights to privacy, most of which were created through constitutional amendments in the last fifty years.[36] Many have been construed to create protections against government searches and seizures that exceed the rights expressed in the Fourth Amendment to the U.S. Constitution.[37] In addition to governing law enforcement access to information, some states have chosen to express a free-standing fundamental or inalienable right to privacy.[38] 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. Thus, while a federal baseline privacy law should seek to meet the important goals of clarity and consistency for businesses and consumers, it should also aspire to respect differences of underlying beliefs in the United States regarding privacy as a fundamental right at the state and local level.

- **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, such as those regulating biometrics,[39] drones,[40] or education privacy. For example, in the field of educational technology ("ed tech"), more than 125 state laws have passed since 2013 regulating issues of data privacy and security for data-driven products and services used by students and teachers.[41] While in some ways, commercial uses of education-related data might be better regulated as part of a baseline consumer privacy law, it would depend on the scope of the bill and the extent of its substantive legal protections. Further complicating these matters, states retain a constitutional right to regulate the core behavior of their own governmental entities, including in the regulation of public schools and school districts.[42]

[36] *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 (last accessed Nov. 9, 2018); 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).

[37] *See e.g.*, State v. Hardaway, 36 P.3d 900, 910 (Mont. 2001) ("In light of the constitutional right to privacy to which Montanans are entitled, we have held that the range of warrantless searches which may be lawfully conducted under the Montana Constitution is narrower than the corresponding range of searches that may be lawfully conducted pursuant to the federal Fourth Amendment").

[38] *See e.g.*, Cal. Const., art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining . . . privacy."); Alaska Const., art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); Mont. Const. art. II, § 10 ("[t]he right of individual privacy is essential to the well-being of a free society and shall not be infringed . . . ").

[39] Biometric Information Privacy Act (BIPA), 740 ILCS/14 (2008).

[40] 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 (last accessed Nov. 9, 2018).

[41] State Student Privacy Laws, FERPA SHERPA (July 20, 2018), https://ferpasherpa.org/state-laws/ (last accessed Nov. 9, 2018).

[42] *See* U.S. Const. art. X.

B. Interaction with federal sectoral laws

In some cases, it may be appropriate for a federal privacy law to supersede and replace existing 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.

When considering how a baseline federal law ought to interact with existing sectoral laws, it's helpful to consider: (1) the extent to which the sectoral law addresses technology, business practices, or users who are uniquely situated; (2) the extent to which the sectoral law has created entrenched privacy and compliance practices for companies, or privacy tools or expectations for users; and (3) whether the sectoral law is currently enforced by a federal agency that has developed enforcement knowledge that would be difficult to replicate at the agency tasked with enforcing a baseline law. For example, if a sectoral law addresses a unique context of data use (e.g. children's information), it may be preferable to preserve the existing sectoral regime. Likewise, if a sectoral law has caused companies to make substantial investments in specific compliance frameworks, users to develop specialized privacy expectations, or oversight agencies to develop hard-won expertise, it may be best to avoid the disruption that would result from amending or repealing the existing sectoral structure.

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. For example, the EU's General Data Protection Regulation (GDPR) came into effect on May 25, 2018, and provides a comprehensive set of rules aimed at consumer control, data transparency, and fairness in data processing. The basic principles of the 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.

A federal baseline privacy law should also promote cross-border data flows[43] by avoiding the creation of obligations that directly conflict with other international laws. For example, an emergence of recent data

[43] *See generally,* McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows* (March 2016), 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 (last accessed Nov. 9, 2018).

localization laws have expressly prohibited data transfers or mandated highly-restrictive regulatory environments.[44] Countries that erect these barriers to data flows often cite concerns about cybersecurity, national security, and privacy. However, they often result in inefficient and burdensome requirements for activities such as data storage, management, processing, and analytics.[45] *See* Appendix A ("Financial Data Localization: Conflicts and Consequences"). 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.

III. Substantive Considerations

The Department should address a range of important substantive considerations, including: treating covered data with nuance in crafting legislative definitions; distinguishing between sensitive and non-sensitive data; promoting internal accountability of privacy and security programs; and creating incentives for socially beneficial uses of data.

A. Covered data and Personal Information

We urge the Department to support a federal baseline privacy law that treats covered data with nuance by recognizing that data exists within a range of identifiability. Leading government and industry guidelines with respect to de-identified data recognize that there is a range of linkability wherein data can be used to identify, contact, or customize content to an individual person or device.[46] A federal privacy law should avoid classifying covered data in a binary way as "personal" or "not personal," and instead build distinctions between categories of data that are materially different, such as data that is: explicitly identified; identifiable; pseudonymous; or de-identified. *See* Appendix B.

In broad terms, categories of data that are both relevant to individual privacy and security risks, and materially different in their uses and impact, include[47]:

- *Identified data*: information explicitly linked to a known individual.
- *Identifiable data*: information that is not explicitly linked to a known individual, but that can practicably be linked by the data holder or others who may lawfully access the information.

[44] *See* U.S. Dept. of Commerce, *Measuring the Value of Cross-Border Data* (Sept. 30, 2016), at 4–5, https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows.pdf.

[45] *See* Financial Data Localization: Conflicts and Consequences, Future of Privacy Forum (2017), https://fpf.org/wp-content/uploads/2017/12/FPF_Bank-Regs_illo_01.pdf.

[46] 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 de-identified; (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. Leading industry associations provide similar guidelines. *See, e.g.*, Digital Advertising Alliance, Self-Regulatory Principles For Multi-site Data (Nov. 2011), at 8, http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf (describing data as de-identified "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.").

[47] *See* 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/.

- *Pseudonymous data*: information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact. This information is typically subject to a combination of technical, administrative, and legal controls. Under certain circumstances, pseudonymised data may qualify as de-identified.
- *De-identified data*: data that has been perturbed or otherwise altered using leading technical methods to make it difficult or impossible to re-identify individuals.[48] This information is typically subject to a combination of technical, administrative, and legal controls.

Notably, recognition of a spectrum of identifiable data provides regulators with the flexibility to adjust the substantive impact of regulatory requirements in line with policy objectives over time. For example, when data that is both pseudonymous and non-sensitive is shared and used by third parties for personalization, targeting, or profiling, a federal law could require that regulated companies provide users with a centralized, effective method of opting out of such collection and use.

In contrast, for data that is classified as de-identified, appropriate regulatory requirements might include legal, administrative, and technical controls, such as prohibiting releasing such datasets to the public in order to prevent risks of re-identification. In many instances, however, it may not be appropriate to require companies to provide users with access or portability rights regarding de-identified data.

B. Sensitive data

We agree with the Department that individuals should be able to exercise reasonable control over their personal information. A federal privacy law should provide heightened protections for the collection, use, storage, and disclosure of users' sensitive personal information or information used in sensitive contexts. 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 geo-location data.[49] The GDPR defines sensitive data more broadly by recognizing special categories of personal data, including "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."[50] Under the GDPR, processing of such sensitive data is prohibited, unless it falls under several exceptions.[51]

In addition to requiring opt-in controls in some circumstances, federal legislation could include additional requirements – such as purpose limitation, retention periods, and respect for context – for some sensitive categories of data. For example, if information such as a user's precise geo-location 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 could restrict sharing that sensitive, identifiable information with

[48] Simson L. Garfinkel, NISTIR 8053, *De-Identification of Personal Information* (Oct. 2015), at 2, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

[49] 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.

[50] GDPR, Art. 9.

[51] GDPR, Art. 9, Recital 51–52.

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 the consumer is making a decision about his or her data.[52]

C. Internal accountability and oversight

A federal baseline privacy law should find ways to incentivize companies to employ meaningful internal accountability mechanisms, including privacy and security programs. External certification processes can be useful, but it is important to recognize that privacy and security risks for technology-driven products and services tend to be ongoing and evolve rapidly. Thus, while external validators can help companies, particularly those with limited resources, navigate complex legal requirements, they will typically not be a substitute for ongoing in-house privacy and security expertise.

Federal legislation could require, or could provide safe harbor treatment or other incentives for: development, documentation, and implementation of comprehensive data security programs; execution of ongoing, documented privacy and security risk assessments, including for risks arising from automated processing; and implementation of robust accountability programs with internal staffing and oversight by senior management. For example, the GDPR requires companies to document their compliance steps,[53] appoint Data Protection Officers,[54] create data protection impact assessments,[55] implement privacy by design and by default,[56] and maintain records of processing activities.[57] Another way to increase expertise is to incentivize employee training through programs such as the International Association of Privacy Professionals (IAPP)'s Certified Information Privacy Professional (CIPP) program or other expert bodies.

D. Incentives for socially beneficial uses of data

Federal privacy legislation should support socially beneficial uses of data, promote the use of privacy-enhancing technologies (PETS), and support machine learning, artificial intelligence, and academic research.

Privacy-enhancing technologies include ongoing innovations in cryptography, data obfuscation, and other technical methods to protect the confidentiality of information.[58] As public interest-minded technologists increasingly focus on issues of individual privacy and data security, the field of PETS research and development has grown. For example, homomorphic encryption is an advanced technique that can enable

[52] 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.

[53] GDPR, Art. 24, 40.

[54] GDPR, Art. 37–39.

[55] GDPR, Art. 35.

[56] GDPR, Art. 25.

[57] GDPR, Art. 30.

[58] Privacy Enhancing Technologies Symposium (PETS Symposium), https://petsymposium.org/2019/paperlist.php (last accessed Nov. 9, 2018).

the performance of basic functions on data that is encrypted – adding, matching, sorting – without revealing the underlying data.[59]

A federal privacy law should also promote beneficial uses of 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 and to ensure accuracy and avoid bias. These data uses can be undermined by data deletion requirements or legal requirements that restrict use of personal data beyond its specified purpose, even when it is de-identified. Although machine learning and AI should not be wholly unregulated by a comprehensive privacy law, a U.S. framework would be wise to ensure that uses of data for machine learning are supported when conducted responsibly.

Finally, a baseline federal privacy law should seek to support meritorious academic and private research. In addition to avoiding undue restrictions on existing research in fields such as medicine, public health, or environmental impact, a federal law might extend incentives to promote socially responsible research. For example, legal mandates that would require data processors to obtain continual permission from individuals for future uses might be appropriate in many commercial contexts. However, such mandates can impose real burdens on researchers who do not know what insights a future study might reveal, and who rely on datasets containing individuals that they cannot contact or who have been de-identified.

Conclusion

We commend the Department of Commerce and the National Telecommunications and Information Administration (NTIA) for their engagement with stakeholders on crafting a federal approach to consumer data privacy. In FPF's view, the best approach would be for Congress to draft and pass a baseline, non-sectoral federal information privacy law. Although we have flagged specific considerations related to such a law's content and its interaction with existing legal frameworks, we overall believe that a federal law remains the best approach to guaranteeing clear, consistent, and meaningful privacy and security protections in the United States.

[59] Andy Greenberg, *An MIT Magic Trick: Computing On Encrypted Databases Without Every Decrypting Them*, Forbes (Dec. 19, 2011), https://www.forbes.com/sites/andygreenberg/2011/12/19/an-mit-magic-trick-computing-on-encrypted-databases-without-ever-decrypting-them/#5918f1fb7fda. *See also* Jules Polonetsky, *Homomorphic Encryption Signals the Future for Socially Valuable Research on Private Data*, Future of Privacy Forum (May 26, 2017), https://fpf.org/2017/05/26/homomorphic-encryption-signals-future-socially-valuable-research-private-data/ (last accessed Nov. 9, 2018).

Appendix A. “Financial Data Localization: Conflicts and Consequences”

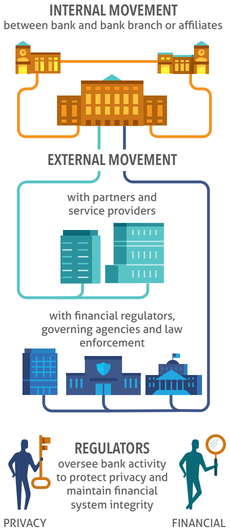
FINANCIAL DATA LOCALIZATION: CONFLICTS AND CONSEQUENCES

Produced by FUTURE OF PRIVACY FORUM
FPF.ORG

Modern banking customers are global, and expect on-demand, high-quality service from their financial institutions regardless of time or location, making 24/7 call centers and multi-national bank branches and service centers the norm. Similarly, regulators expect financial institutions to have a global understanding of their customers to assess and manage risk. Delivering on these expectations requires financial institutions to regularly move information between locations in support of business operations. Policy goals to ensure privacy and security are important and can coexist with the free flow of data. However, regulations that achieve these goals through localization cause conflict and complexity and can result in unintended consequences. Let's take a look:

HOW DATA FLOWS

Supporting business operations requires the regular movement of financial data between locations. Multi-national operations add complexity, as local governing regulations must be considered once a border is crossed.


INTERNAL MOVEMENT
between bank and bank branch or affiliates
EXTERNAL MOVEMENT
with partners and service providers
with financial regulators, governing agencies and law enforcement
REGULATORS
oversee bank activity to protect privacy and maintain financial system integrity
PRIVACY
FINANCIAL

UNINTENDED CONSEQUENCES OF LOCALIZATION

LEGAL TENSION

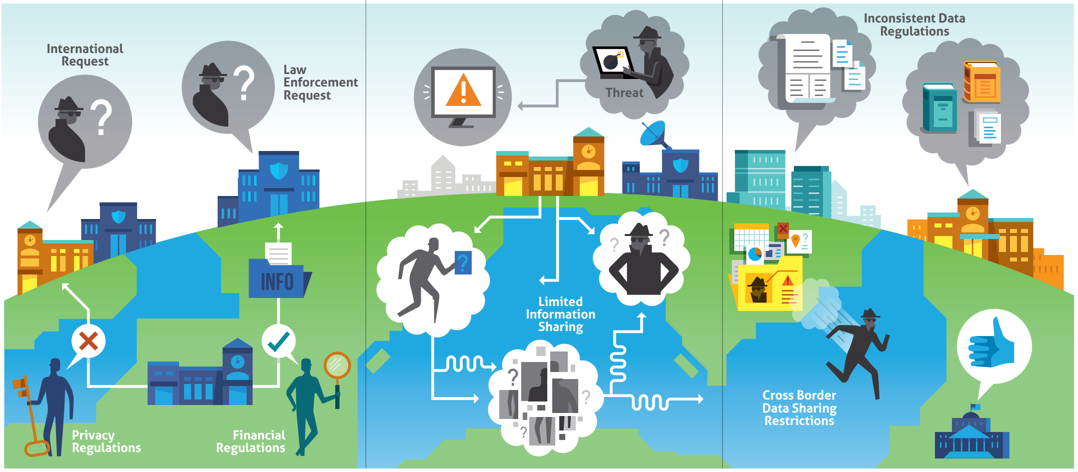
Banks have legal obligations to comply with both regulators and law enforcement agencies within their country. However, requests by law enforcement from other countries for access to data, even when narrowly tailored and proportionate, can often conflict with local regulations that seek to protect the privacy of citizens and the integrity of the financial system. These tensions are heightened by a lack of international, agreed upon principles or safe harbors.

HAMPERED THREAT RESPONSE

Data privacy and other cross border data transfer restrictions may limit the ability to share information from one country with peers and regulators in other countries so security threats may be slower to be identified. A legislative framework is needed for sharing threat information across borders while respecting local privacy and other rules.

COMPROMISED REPORTING CAPABILITIES

The inconsistency of data regulations across countries erodes the opportunity for holistic reporting. For example, when considering criminal activity, regulations require criminal reports to be made locally. In addition, cross border data sharing restrictions often apply to sharing with affiliates, which increases the risk that a criminal rejected in one country can open an account in another country.


International Request
Law Enforcement Request
INFO
Privacy Regulations
Financial Regulations
Threat
Limited Information Sharing
Inconsistent Data Regulations
Cross Border Data Sharing Restrictions

TYPES OF REGULATION

Many regulations exist to control access to information and protect privacy and security interests:

- ANTI MONEY LAUNDERING
- PRIVACY
- BANK SECRECY
- BLOCKING STATUTES
- CYBER SECURITY
- LOCALIZATION
- OUTSOURCING

PERCEIVED DRIVERS FOR LOCALIZATION

INFORMATION SECURITY

Perception: Localization provides better data security and protection.

Reality: Increased risk of cyber attacks as footprint grows and data becomes more diffuse.

PROTECTION OF PRIVACY VALUES

Perception: Localization protects data from over-broad law enforcement access abroad.

Reality: With narrowly tailored and proportionate laws we can accomplish better oversight and protect individual privacy.

TECHNOLOGY

Perception: Localization makes technology easier to manage.

Reality: It’s more difficult to update applications and ensure consistency with increased end-points.

EFFICIENCY

Perception: Localization increases efficiency.

Reality: Redundancy of data centers and personnel reduces bank efficiency and increases cost.

LOCAL JOBS

Perception: Localization creates jobs and stimulates the economy.

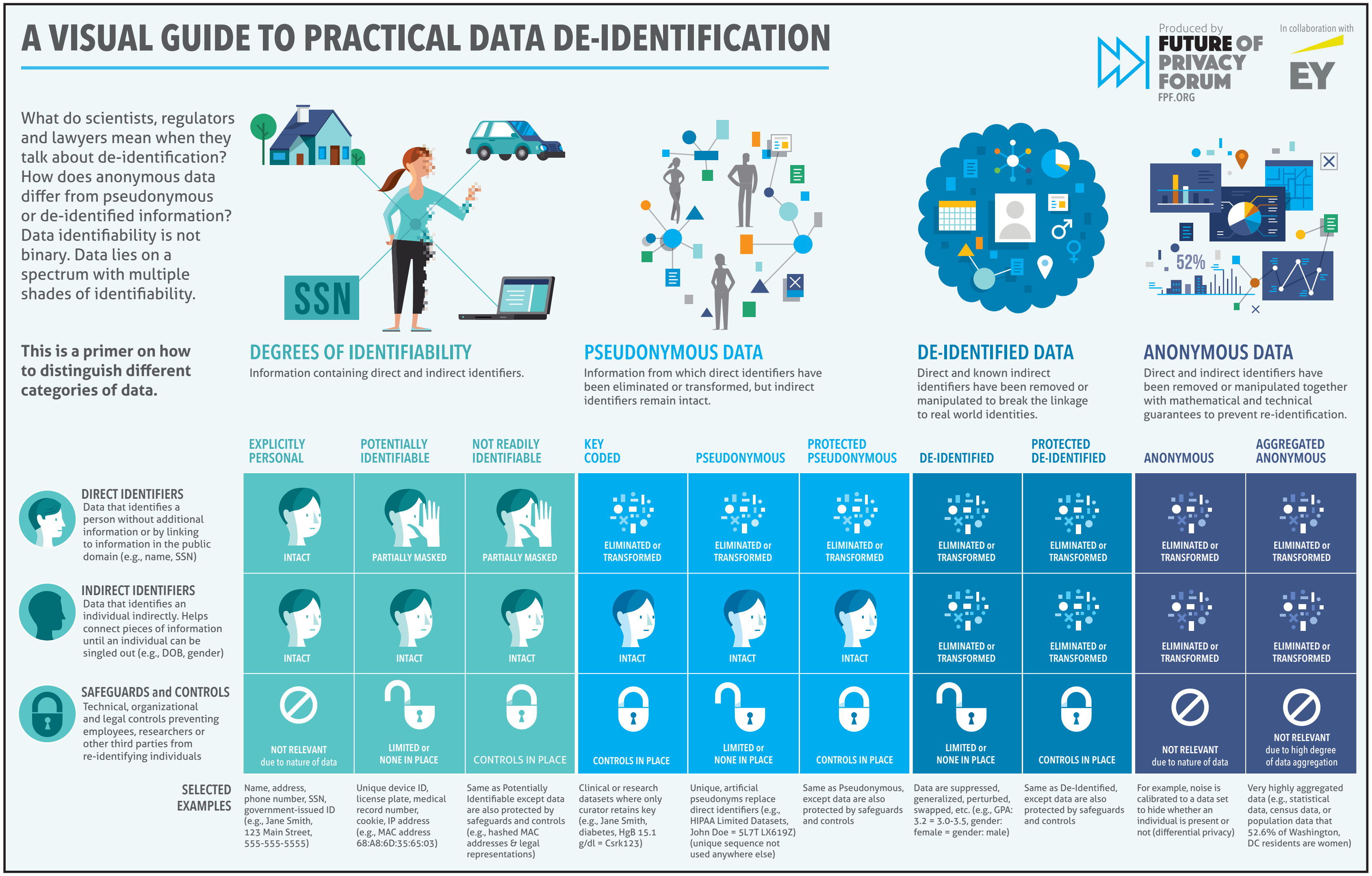
Reality: Job creation is minimal, and localization can cause global financial companies to reduce their presence, limiting services and opportunities.

ACCESS TO DATA

Perception: Localization is the only way to ensure access to data during a crisis.

Reality: Contractual access can be granted to data stored outside a local jurisdiction to ensure regulators can perform regulatory and supervisory roles, even during a crisis.

Appendix B. “A Visual Guide to Practical De-Identification”



A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

Produced by FUTURE OF PRIVACY FORUM
FPF.ORG

In collaboration with EY

What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.

This is a primer on how to distinguish different categories of data.

DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
DIRECT IDENTIFIERS Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
INDIRECT IDENTIFIERS Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
SAFEGUARDS and CONTROLS Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation
SELECTED EXAMPLES	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)	Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csrk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = 5L7T LX619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)	Same as De-Identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)