CENTER FOR DEMOCRACY & TECHNOLOGY

9 November 2018

Submitted via email to privacyrfc2018@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

RE: Docket No. 180821780-8780-01

The Center for Democracy and Technology (CDT) is a non-profit advocacy organization working to promote democratic values online and in new, existing, and emerging technologies. CDT pursues this mission by supporting laws, policies, and technical tools which empower users, protect privacy, and preserve individual rights online. CDT respectfully submits these comments in response to the request for public comment from the National Telecommunications and Information Administration (NTIA) on how to advance consumer privacy.

CDT advocates for a strong federal baseline privacy law and believes that any administration proposal must have a legislative component at its foundation. Meaningful commercial privacy protection requires common standards and protections across industries, limits on the use of sensitive data, and rigorous enforcement. Importantly, a federal solution must be carefully scoped to provide one national standard for data protection without undermining state action that does not directly address consumer privacy in the digital ecosystem. We appreciate the NTIA's recognition that companies should embrace longstanding Fair Information Practice Principles (FIPPs), as well as internal accountability and risk management efforts, but the administration must advance a legislative proposal that additionally prohibits intrusive and unfair data collection and use.

I. Under (A) and (B), the Department seeks feedback on both the core privacy outcomes consumers should expect from organizations and the proposed high-level goals for an end-state for U.S. consumer-privacy protections.

1. *Voluntary accountability measures are insufficient to protect an individual's privacy; a federal approach should seize on the current moment to enshrine privacy protections in law.*

The NTIA endorses seven general privacy outcomes that are represented in longstanding U.S. and international policy. These outcomes echo aspects of the Fair Information Practice Principles (FIPPs) and draw on international data protection frameworks like the EU General Data Protection Regulation (GDPR). Specifically, the administration embraces (1) transparency, (2) control, (3) reasonable minimization, (4) security, and (5) access and correction, which are operationalized via a (1) risk management framework and (2) accountability principles. In isolation, CDT does not disagree that each

1401 K Street NW, Suite 200 Washington, DC 20005

of these outcomes is important, but we believe there are serious limitations to an approach that emphasizes voluntary actions by corporate actors. It does not seize on the current opportunity to enshrine a national law that resolves our state-by-state patchwork of legal protections *and* aligns with global privacy norms.

Absent a mandatory baseline and a clear set of prohibitions and restrictions on data collection and use, the NTIA's outcomes will require individuals to place their trust in companies to protect privacy through voluntary measures. As the NTIA has acknowledged, individuals do not trust companies to protect their data online,[1] and 68% of Americans believe current laws are insufficient to protect their privacy.[2] We agree in many respects with the recent assessment of the UK Information Commissioner's Office that "the time for self-regulation is over."[3]

As the UK ICO also notes, internal accountability measures are not without merit. The intended outcome of accountability is to shift privacy management[4] away from overburdened users toward the companies invading user privacy. Corporate accountability measures include internal staffing, "privacy by design," and review processes as fundamental elements for protecting individuals' privacy.[5] However, none of these mechanisms ensure that the privacy interests of consumers are aligned with a company's ultimate bottomline. For example, privacy professionals are often viewed as the privacy voice for individuals within companies, but the issue of ultimate allegiance cannot be dismissed.[6] The GDPR attempts to address this challenge by establishing independent data protection officers that are insulated from corporate management and have their responsibilities and qualifications spelled out by statute.[7] While

[1] Nat'l Telecommunications & Info. Admin., Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds (Aug. 20, 2018), https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds.

[2] *E.g.*, Pew Research Ctr., The State of Privacy in Post-Snowden America (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (finding a "majority of the U.S. public believes changes in law could make a difference in protecting privacy – especially when it comes to policies on retention of their data."). A more recent survey found that 68% of respondents supported the enactment of a GDPR-type law in the United States. Janrain Research: Consumer Attitudes Toward Data Privacy Survey (2018), https://www.janrain.com/resources/industry-research/consumer-attitudes-toward-data-privacy-survey-2018.

[3] Jessica Haworth, The time for self-regulation is over, UK information commissioner tells tech firms, Daily Swig (Nov. 6, 2018), https://portswigger.net/daily-swig/the-time-for-self-regulation-is-over-uk-information-commissioner-tells-tech-firms.

[4] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880, 1881 (2013) (noting that "even well-informed and rational individuals cannot appropriately self-manage their privacy").

[5] Intel Privacy Legislation Discussion Draft, Section 4 (Nov. 5, 2018), *available at* https://usprivacybill.intel.com/legislation/.

[6] Angelique Carson, Should the privacy profession adopt a code of ethics?, IAPP Privacy Advisor (Feb. 28, 2017), https://iapp.org/news/a/should-the-privacy-profession-adopt-a-code-of-ethics/ ("Basically, doctors have their allegiance related to their patients . . . . The problem in the privacy profession is: Where is your allegiance?").

[7] Regulation (EU) 679/2016 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

laudable, this approach can outsource regulatory action to companies and incentivize a cottage industry of consultants and lawyers more engaged in compliance than privacy protection.[8]

2. *Shortcomings in existing approaches to privacy by design underscore the limitations of privacy protection via internal corporate processes and procedures.*

Privacy by design also presents shortcomings as the sole substantive solution to existing privacy challenges.[9] According to the Federal Trade Commission, privacy by design requires companies to promote privacy throughout their organization and throughout the entire lifecycle of products and services, which includes data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.[10] While it is laudable that privacy by design seeks to shift the responsibility for protecting data away from individuals and proactively onto companies, it is very flexible and its impact relies on the internal privacy values of businesses. A company could consider privacy controls and reject most or all of them without much consequence. For example, debates this fall between Ann Cavoukian, one of the architects of modern privacy by design, and Sidewalk Labs, which is engaged in developing a prototype smart city in Toronto, have revealed some of the limitations of addressing major policy issues via simply "doing more" privacy by design.[11]

The reality is that major companies have long committed to embedding privacy into their development processes, but assessing the practical benefit of that process for consumers is challenging.[12] Moreover,

---

movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, articles 37-39 [hereinafter GDPR].

[8] Salvador Rodriguez, Business booms for privacy experts as landmark data law looms, Reuters (Jan. 22, 2018), https://www.reuters.com/article/us-cyber-gdpr-consultants/business-booms-for-privacy-experts-as-landmark-data-law-looms-idUSKBN1FB1GP ("The cottage industry that's developed around GDPR includes lawyers who advise on compliance, cyber security consultants, and software developers that help firms conduct painstaking inventories of vast amounts of data to identify and index information.").

[9] *See* Daniel Castro, The FTC Report on Consumer Privacy Misses the Mark, Innovation Files (Apr. 2, 2012), https://www.innovationfiles.org/the-ftc-report-on-consumer-privacy-misses-the-mark/ (cautioning that the term "has devolved into little more than a hot buzzword").

[10] Federal Trade Comm'n, Protecting Consumer Privacy in an Era or Rapid Change 13 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacyera-rapid-change-recommendations/120326privacyreport.pdf.

[11] Nick Summers, Google's smart city dream is turning into a privacy nightmare, Engadget (Oct. 26, 2018), https://live.engadget.com/2018/10/26/sidewalk-labs-ann-cavoukian-smart-city/ (noting that "Sidewalk Labs has committed to implement, as a company, the principles of privacy by design.").

[12] Privacy commitments undertaken by Uber illustrate this problem. Compare Jen King, Privacy by Design and the Uber Settlement, Stanford Center for Internet & Society (Oct. 15, 2018), https://cyberlaw.stanford.edu/blog/2018/10/privacy-design-and-uber-settlement ("evaluating whether a company is incorporating privacy into their design processes is more difficult than evaluating a comprehensive privacy program focused on legal compliance") with Hogan Lovells, Review and Assessment of Uber's Privacy Program (Jan. 2015), https://newsroom.uber.com/wp-content/uploads/2015/01/Full-Report-Review-and-Assessment-of-Ubers-Privacy-Program-01.30.15.pdf (noting that "Uber has policies in place that require employees to address Consumer Data privacy issues as they arise during development of the Uber app").

a narrow construction of privacy by design will not account for more nuanced violations of individuals' privacy expectations and perceptions.[13] In 2013 Ira Rubinstein and Nathan Good recommended regulators convene workshops, identify best practices, and fund more research in privacy engineering and usability studies -- these types of activities are still needed.

3. *A risk management approach requires clarifications that a broad range of privacy risk exists from corporate data processing.*

A risk management approach comes with many of the same challenges of privacy by design. Some point to the success of risk management in cybersecurity as a model for privacy regulation, but harms and the corresponding controls that can mitigate them are much less controversial in the cybersecurity field. There is less consensus among industry as to what constitutes a risk of privacy harm,[14] and as industry representatives acknowledge, "[c]larification of privacy risks is needed as part of new national privacy laws."[15] In addition to this diversity of opinions within corporate America, recent events have confirmed there is a significant disagreement about the value of privacy between users and industry in general.

To the extent that risk management becomes part of the administration's proposal, CDT recommends an explicit adoption of the risks compiled by the National Institute for Standards & Technology (NIST). NIST acknowledges that privacy risks exist beyond economic loss and include diminished capacity for autonomy and self-determination, discrimination (legal or otherwise), and a generalized loss of trust.[16] An extensive framing of risk is present in a legislative discussion draft from Intel which includes (1) psychological harm, (2) significant inconvenience and loss of time, (3) adverse eligibility determinations, (4) stigmatization and reputational harm, (5) unwanted commercial communications, (6) price discrimination, and (7) other effects that alter experiences, limit choices, or influence individuals in addition to expected financial or physical harms.[17]

Identifying a list of risks, however, does not provide clear direction to companies as to what they must do to mitigate or avoid them altogether. Absent a firm set of legislative rules, the NTIA's calls for risk management would give businesses considerable discretion to determine what risks individuals may assume. Industry, for example, highlights the benefits of price discrimination and frequently minimizes the reality that the data-driven ecosystem presents reputational impacts for individuals.

---

[13] Ira S. Rubenstein & Nathaniel Good, Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, 28 Berkeley Tech. L.J. 1333, 1352 (2013).
[14] *See* FTC Informational Injury Workshop: BE and BCP Staff Perspective (Oct. 2018), *available at* https://www.ftc.gov/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective.
[15] Mark MacCarthy, What exactly is a privacy risk?, CIO (Sept. 18, 2018), https://www.cio.com/article/3306760/privacy/what-exactly-is-a-privacy-risk.html.
[16] Sean Brooks et al., NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems 10 (Jan. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. NIST's framework is itself an adaptation of Daniel Solove's detailed taxonomy of privacy invasions. Daniel Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006).
[17] Intel Privacy Legislation Discussion Draft, Section 3 (Nov. 5, 2018), *available at* https://usprivacybill.intel.com/legislation/.

4. *Considerations of context and user expectation require careful interrogation of how industry shapes expectations and design user experiences.*

The NTIA has acknowledged the definitional challenges around key privacy terms. As we discuss below in Section III, even once the NTIA answers the threshold question of what types of personal information should be covered, identifying what requirements or expectations go along with that information will be key. For example, the NTIA proposal emphasizes the role of "context," which considers factors such as user expectations and the sensitivity of the information. These concepts need additional clarification.

While context was highlighted in the prior administration's Consumer Privacy Bill of Rights,[18] it has proven difficult to operationalize. Policymakers have been unable to answer how exactly a company's privacy obligations should be tied either to the context of a transaction or consumer relationship or individual user expectations. An individual's contextual expectations rest on a number of subjective variables such as an individual's level of trust in an organization and her perception of the value she might receive from the use of her information.[19] When the concept of respect for context is only embraced in principle and not practice, it becomes susceptible to a number of competing determinations.[20] Unfortunately, companies and industry privacy practices have deemed consumer expectations to be sufficiently shaped by disclosing information in a privacy policy.[21] Respect for context should go beyond the four corners of a privacy policy. Contextual cues call for embracing for what Woodrow Hartzog terms a design agenda in privacy law.[22]

CDT has previously called for further exploration of and enforcement against unfair design, including unfair default settings and aggressive notifications that manipulate users.[23] Ultimately, these are issues

[18] White House, Press Release, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

[19] Carolyn Nguyen, Director, Microsoft Technology Policy Group, Contextual Privacy, Address at the FTC Internet of Things Workshop (Nov. 19, 2013), *available at*: http://www.ftc.gov/sites/default/files/documents/public_events/internet-thingsprivacy-security-connectedworld/final_transcript.pdf.

[20] See Helen Nissenbaum, Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't, Berkeley Law (May 24, 2013, 9:31 PM), http://privacylaw.berkeleylawblogs.org/2013/05/24/helen-nissenbaum-respect-for-context-as-abenchmark-for-privacy-online-what-it-isand-isnt-2/.

[21] E.g., Consumer Privacy Protection Principles, Alliance of Automobile Manufacturers 9 (Nov. 12, 2014): "When Participating Members present clear, meaningful notices about how Covered Information will be used and shared, that use and sharing is consistent with the context of collection."

[22] *See* Woodrow Hartzog, Privacy's Blueprint (2018).

[23] Comments of the Center for Democracy & Technology re: FTC Hearings on Competition and Consumer Protection in the 21st Century 4-6 (Aug. 20, 2018), https://cdt.org/files/2018/08/CDT-FTC-comments-5-8-20-18.pdf.

1401 K Street NW, Suite 200 Washington, DC 20005

that extend out of the realm of law and policy to considerations about user experience and user interface, backend design, and how to cabin so-called "dark patterns."

5. *The impacts of algorithms and automated decision making are emerging privacy challenges that must be considered by the NTIA.*

Finally, CDT notes that the NTIA request for comment does not address the risks from opaque and discriminatory algorithms and we recommend that any proposal from the administration explicitly account for this quickly growing risk. As Ryan Calo has noted, machine learning permits organizations "to derive the intimate from the available."[24] As a result, privacy discussions have rapidly evolved from a debate that emphasizes individual control to a focus on the information and power asymmetries facing individuals.[25] This raises serious issues for data-driven practices ranging from eligibility determinations to targeted marketing. Studying these practices has been challenging because individual users don't know what offers they're excluded from seeing, and companies seldom, if ever, release the precise targeting parameters.[26] Applications of artificial intelligence and machine learning have been termed the "ultimate test for privacy" and have been an extensive focus of the GDPR,[27] yet are largely missing from the NTIA's current framework.

II. Under (C), the Department also seeks comments that describe what the next steps and measures the administration should take to effectuate its privacy outcomes high-level goals.

1. *Concrete guidance is needed to operationalize the FIPPs, and a federal privacy law should offer four key protections for consumers.*

Opaque data processes that lead to information asymmetries and power disparities, particularly among marginalized and vulnerable consumers, demonstrate the fundamental problem with basing a privacy regime on voluntary implementation of the Fair Information Practice Principles (FIPPs). CDT has long reiterated its belief that a commercial data privacy framework should incorporate all of the FIPPs,[28] and this is a common demand of privacy and consumer advocates.[29] Operationalizing the FIPPs has proven

[24] Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. Davis L. Rev. 399, 421 (2017).
[25] *Id.* at 423; *see also* Privacy International & Article 19, Privacy and Freedom of Expression In the Age of Artificial Intelligence (2018), https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence.
[26] Upturn, Leveling the Platform: Real Transparency for Paid Messages on Facebook at 16 (May 2018), https://www.teamupturn.org/static/reports/2018/facebook-ads/files/Upturn-Facebook-Ads-2018-05-08.pdf.
[27] Eduardo Ustaran, Is Artificial Intelligence the Ultimate Test for Privacy?, Hogan Lovells (Mar. 2, 2018), https://www.hldataprotection.com/2018/03/articles/consumer-privacy/is-artificial-intelligence-the-ultimate-test-for-privacy/.
[28] Ctr. for Democracy & Tech., Recommendations for a Comprehensive Privacy Protection Framework (Feb. 4, 2011), https://cdt.org/insight/recommendations-for-a-comprehensive-privacy-protection-framework/.
[29] Public Interest Privacy Legislation Principles 1 (forthcoming Nov. 13, 2018).

1401 K Street NW, Suite 200 Washington, DC 20005

challenging, however, as their precise formulations have been disputed and debated.[30] Industry stakeholders often speak of the need to recalibrate the FIPPs in light of new technological developments and increased data collection, and the NTIA appears to recognize that general principle of data minimization is under strain. Additional clarity is needed from the NTIA to detail how companies must concretely operationalize the FIPPs, provide affirmative individual rights to data, and address broader equity and fairness concerns.

CDT proposes a federal privacy law that (1) builds on the FIPPs to grant affirmative access, correction, deletion, and portability rights to individuals, (2) requires reasonable security practices and transparency from companies, (3) prevents advertising discrimination against protected classes, and (4) presumptively prohibits certain collection and use of sensitive data for secondary purposes. Individuals must have access to and, in some instances, the ability to correct their personal data held by companies. They should have the ability to delete and remove their data from services. The public should have detailed information about what data companies are collecting and with whom they share it. Many of these types of overarching privacy rights should be noncontroversial. What is more challenging is the question of what rights individuals should have with respect to data that is observed or inferred about them. Inferences can be more sensitive and relevant than the data individuals directly provide to a company, are often invisible to individuals and the public, and can be the basis for decisions that have significant effects on people's lives.[31]

The policy challenge posed by such inferential information and its incorporation into automated systems highlights a fundamental limitation of the FIPPs to ensure that data collection, use, and sharing is truly "fair" to individuals. The FIPPs often cannot directly address the effect of how systems, platforms, and products are today designed, or the resulting transaction costs that undermine trust, individual obscurity, and personal autonomy.[32] The FIPPs do not, as Woodrow Hartzog details, "focus on how technology actually *affects* people."[33]

2. *Presumptive prohibitions on unfair, secondary uses of sensitive information acknowledge that consumers lack informed choice.*

Many existing data processing practices undermine individuals' capacity to make informed choices. The FTC has noted that unfair practices exist online where activities prey on vulnerable consumers, involve coercive conduct, and create significant information deficits, or involve third parties with whom

[30] Sean Brooks et al., NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems 10 (Jan. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[31] *See* Office of Oversight & Investigations, Majority Staff, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Senate Commerce Committee (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a/D5E458CDB663175E9D73231DF42EC040.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.
[32] Woodrow Hartzog, Privacy's Blueprint 124 (2018).
[33] *Id.* at 61.

individuals have no relationship like data brokers.[34] This is a systemic failure of today's data ecosystem; as a result, a policy response that emphasizes "more transparency" or corporate accountability simply creates more institutional processes without addressing this underlying challenge.

CDT believes that some types of information present inherent risks that individuals cannot assess and that unnecessary collection and secondary uses of this information should be curtailed. The processing of precise geolocation information is one such example. Location information provides, as the Supreme Court held, an intimate window into a person's life, revealing not just an individual's particular movements but also their political, professional, religious, and sexual associations.[35]

Despite the FTC's efforts to classify precise geolocation as information warranting "affirmative express consent", companies have been found to sell precise geolocation data[36] and surreptitiously collect this information,[37] as justified via their privacy policies. Instead, the processing of precise geolocation information should only happen when an individual has purposely opted into a service that requires this information, and there should be a strong legal presumption that location data will not be further shared or used for other purposes. These types of guardrails should exist for other sensitive practices like identification using biometrics, the collection of information on children and individual health, and targeting based on protected classes like race or religion.

3. *Privacy protections are critical protections for marginalized and vulnerable consumers, and the NTIA should seek further feedback from a wide range of civil rights organizations often missing from privacy debates.*

Identifying sensitive practices and suitable guardrails calls for a broad conversation among communities that are often not part of existing privacy debates. To that end, the NTIA should solicit the views of additional perspectives across civil rights organizations, as well as consumer and privacy advocacy groups. CDT does not believe further multistakeholder work to create another set of voluntary best practices on the issue of consumer privacy would be productive, but privacy rules, both in terms of protecting consumers and advancing economic opportunity, may have unanticipated impacts for different socioeconomic groups. Far too often, debates about privacy are dominated by large industry

[34] Thomas B. Leary, Fed. Trade Comm'n, Unfairness and the Internet (Apr. 13, 2000), https://www.ftc.gov/public-statements/2000/04/unfairness-and-internet.
[35] Carpenter v. United States, No. 16-402, at 12, 585 U.S. ____ (2018) (citing United States v. Jones, 565 U.S. 400, 415 (2012)).
[36] Zack Whittaker, US cell carriers are selling access to your real-time phone location data, ZDNet (May 14, 2018), https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/. These companies pointed to privacy policies to justify this practice, but ultimately changed this practice after public criticism.
[37] Dieter Holger, How 'free' Wi-Fi hotspots can track your location even when you aren't connected, PCWorld (Nov. 1, 2018), https://www.pcworld.com/article/3315197/privacy/free-wi-fi-hotspots-can-track-your-location-even-when-you-arent-connected.html.

1401 K Street NW, Suite 200 Washington, DC 20005

voices and privacy organizations that can lack a diversity of backgrounds and views.[38] CDT believes that consumer privacy protections are especially critical for marginalized and vulnerable communities, and that the negative impacts of unfair data processing practices involving geolocation data, biometrics, and consumer scoring disproportionately fall on those groups.

4. *Government procurement processes can improve cybersecurity, data privacy, and algorithmic accountability practices.*

Beyond endorsing baseline privacy legislation, the federal government should use its procurement power to ensure that the products and services it purchases include privacy and security controls. This will not only protect government systems, but also likely send more privacy and security-friendly products into the consumer market.

While the federal government has long set contracting standards on privacy and security, it has issued extensive data and product management guidance over the last several years which could improve the next generation of government purchases. Documents drafted or updated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) now clearly delineate agency obligations and provide technical advice on how to incorporate privacy controls into products.[39] The executive and legislative branches could do more to speed the adoption of such products either through legislative or executive mandates[40] or better funding current IT modernization efforts.[41] Procurement processes could be used to drive more meaningful public transparency into algorithmic processes that produce legal effect. For instance, CDT and other leading organizations provided recommendations for how procurement contracts could be used to assess bias and fairness issues in automated decision-making systems.[42]

III. Under (D), the Department acknowledges that that some of the most important work in establishing privacy protections lies within the definitions of key terms, and seeks comments on the definitions.

1. *A broad definition of personal information is needed to protect consumers and capture evolving business practices that undermine privacy.*

[38] *See generally* Erin Murphy, The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions, 111 Mich. L. Rev. 485, 505 (2013).
[39] OMB Circular A-130 (2016), NISTIR 8062 (2017), NIST 800-63, Rev. 5, (2018).
[40] *See, e.g.*, S. 1691, The Internet of Things (IoT) Cybersecurity Improvement Act of 2017, introduced by Senator Mark Warner.
[41] The Technology Modernization Fund was created by Congress in 2018 and controls $100 million dedicated to updating government systems under a more streamlined contracting process. An estimated $85 billion was spent last fiscal year on information technology, which overwhelming is used to maintain legacy systems. See https://itdashboard.gov/.
[42] Advocacy Letter Re: New York City's Automated Decision Systems Task Force 3 (Aug. 17, 2018), http://assets.ctfassets.net/8wprhhvnpfc0/1T0KpNv3U0EKAcQKseIsqA/52fee9a932837948e3698a658d6a8d50/NYC_ADS_Task_Force_Recs_Letter.pdf.

Personal information is an evolving concept. A privacy law is, in many respects, an exercise in drawing boundaries between the information that is and is not covered.[43] The challenge, as Professors Paul Schwartz and Daniel Solove have recognized, is that the "identifiability" of information rests on a spectrum.[44] State and federal privacy laws have addressed this in different ways, creating myriad legal definitions of personal information, and the result is that the scope of what might properly be deemed "personal information" is an unsettled question as a matter of law, policy, and technology.

The prevailing approach with respect to general commercial information is the framing offered by the Federal Trade Commission in 2012. The FTC takes the position that personal information is "linked or reasonably linkable to a consumer or a consumer's device," but it carves out from this information that is de-identified where a business "(1) takes reasonable measures to ensure that the data is 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."[45] De-identification is a valuable process for protecting privacy, but CDT would suggest it is worth reassessing what reasonable de-identification measures should entail and evaluating potential data misuse from aggregate and collective information.

Recent privacy incidents highlight the potential misuse of aggregated information. For instance, Strava, a fitness data platform, created an "aggregated" heat map that revealed information about the location and movements of military service members in conflict zones, including the alleged locations of secret U.S. military installations. This highlights some of the larger ethical issues that emerge with open data and public data sharing by default. Strava also argued that this information was anonymous, but researchers uncovered that it was possible to de-anonymize the data by uploading an altered GPS file, providing names, running speeds and routes, and heart rates of anyone who shared their fitness data.[46] Anonymization of historical geolocation data is incredibly challenging, if not impossible,[47] and this demonstrates the social implications of widespread sharing of collective information, especially for individuals or groups that are potential outliers.

The other approach is to sweep in as much information as possible into a data protection framework. CDT believes this is the better approach. In contrast to the U.S. approach, the GDPR broadly defines "personal data" to mean "any information relating to an identified or identifiable natural person"

---

[43] Peter Swire, Comments to the FCC on Broadband Consumer Privacy 12 (Apr. 28, 2015), https://transition.fcc.gov/cgb/outreach/FCC-testimony-CPNI-broadband.pdf.

[44] *E.g.*, Paul M. Schwartz & Daniel J. Solove, PII 2.0: Privacy and a New Approach to Personal Information, 11 PVLR 142 (Nov. 23, 2012), https://pdfs.semanticscholar.org/2c2a/b17010a276497b30ad22127d141884579e58.pdf.

[45] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change iv (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[46] Matt Burgess, Strava's data lets anyone see the names (and heart rates) of people exercising on military bases, Wired UK (Jan. 30, 2018), https://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military.

[47] Y. De Montjoye et al., Unique in the crowd: The privacy bounds of human mobility, 3 Scientific Reports 1376 (2013).

1401 K Street NW, Suite 200 Washington, DC 20005

including names, technical identifiers, and even factors specific to one's physical, physiological, genetic, mental, economic, cultural, or social identity.[48] The GDPR also attempts to recognize that identifiability of data rests on a spectrum, introducing the concept of psuedonymized data and excluding anonymous data from its reach.[49] These concepts have been introduced into U.S. law via the recently enacted California Consumer Privacy Act of 2018, demanding federal consideration, as well. All of these models point to the reality that de-identified and other types of anonymization may be subject to different standards but should not be removed from the protections of the bill altogether.

CDT believes a broad definition of personal information is appropriate in today's digital environment and endorses the linkability test that has been adopted by federal agencies. In addition to the FTC policy discussed above, the Office of Management and Budget has embraced a very similar formulation. OMB Circular A-130 definition of "PII" or personally-identifiable information as any data "that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual,"[50] including behavioral and transactional information.

2. *Sensitive information often is narrowly scoped and receives more formalistic than substantive protection.*

CDT also believes any framework should assess what types of information the NTIA believes are particularly sensitive. While CDT believes all personal information should be protected, there are some types of data and some processing practices that are so sensitive that they should be permitted only to provide a user the service they requested, and businesses be prohibited from entering the opaque and unaccountable market of secondary uses.

As the NTIA determines what constitutes personal information, sensitivity considerations will go hand-in-hand with this determination. Existing privacy frameworks call out specific types of information as being especially sensitive. The GDPR, for instance, refers to "special categories" of data that reveals "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."[51] The FTC's understanding of sensitive information is narrower and includes Social Security numbers and financial, health, children's, and precise geolocation data -- and potentially detailed data regarding

[48] GDPR, *supra* note 7, art. 4.
[49] *See* Opinion 05/2014 on Anonymisation Techniques, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 0829/14/EN, WP 216.
[50] Circular A-130, "Managing Federal Information as a Strategic Resource" (2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[51] GDPR, *supra* note 7, art. 9.

individual television viewing habits.[52] It is CDT's recommendation that secondary uses of sensitive information be sharply curtailed.

For sensitive uses of information -- such as precise geolocation tracking, health and children's data, biometrics and audio and video content -- CDT proposes a relatively straightforward test: generally this information can be used if it is necessary to the product or service being offered and cannot be collected, used or shared for other purposes. Very limited exceptions may be possible if they benefit the consumer and have been approved by a regulator. It is important to note that this information would not be shared even with consumer consent. Just as we don't allow consumers to consent away core protections in other contexts - such as seatbelts in cars or sprinklers in office buildings - these should be core protections for the use of information. We believe the balance best serves consumers while still protecting innovation. It allows companies to still offer a broad array of services while giving consumers a clear idea of the uses of their personal information.

The alternative is recommitting to the current notice and consent model that relies on obtaining "affirmative express consent" prior to *collecting* sensitive data.[53] A myriad of settings and opt-outs only complicates any rational individual's ability to manage their privacy. This creates a default where once sensitive information is collected or obtained, it can then be used in privacy-invasive ways. For example, the FTC recently brought an enforcement action against the payment processing app Venmo for offering deceptive privacy settings where the bigger question was whether financial information, which everyone concurs is sensitive, was broadcast publicly by default.[54] Similarly, while precise geolocation information is incredibly revealing when collected and stored over time, it can also be *used* in real-time in ways that can be surprising at best and offensive at worst, as when one firm sent anti-abortion advertisements to women in the proximity of abortion clinics.[55]

E. One of the high-level end-state goals is for the FTC to continue as the federal consumer privacy enforcement agency, outside of sectoral exceptions beyond the FTC's jurisdiction. In order to achieve the goals laid out in this RFC, would changes need to be made with regard to the FTC's resources, processes, and/or statutory authority?

---

[52] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, *supra note* 45, at 15; *see also* Joseph Jerome, From Televisions to Telescreens: Video Viewing Habits Are Sensitive Information, Ctr. for Democracy & Tech. (Feb. 14, 2017), https://cdt.org/blog/from-televisions-to-telescreens-video-viewing-habits-are-sensitive-information/.

[53] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, *supra note* 45, at 58-60.

[54] Natasha Duarte, The FTC-Venmo Privacy Settlement is All About Design, Ctr. for Democracy & Tech. (Mar. 1, 2018), https://cdt.org/blog/the-ftc-venmo-privacy-settlement-is-all-about-design/.

[55] Curt Woodward & Hiawatha Bray, A company sent anti-abortion ads by phone. Massachusetts wasn't having it, Boston Globe (Apr. 4, 2017), https://www.bostonglobe.com/business/2017/04/04/healey-halts-digital-ads-targeted-women-reproductive-clinics/AoyPUG8u9hq9bJUAKC5gZN/story.html. This example also highlights the challenge of how "geolocation" and "health" data is properly understood. Outside of specific legal regimes, there is no baseline understanding among companies and consumers as to what these terms mean.

1. *In order to meaningfully policy industry data practices, the FTC needs additional resources and new statutory enforcement mechanisms.*

CDT has long supported the Federal Trade Commission as the country's "top privacy cop," but it is also clear that the FTC needs both more resources and authority.[56] In 2015, the FTC had only 57 full time staff working in the Division of Privacy and Identity Protection (DPIP), with additional staff working in enforcement and other areas that could touch on privacy. We note that recent legislative proposals like Sen. Ron Wyden's would greatly expand the personnel in DPIP, as well as elevate the Office of Technology Research and Investigation to its own bureau within the FTC.[57] These are positive first steps.

However, the FTC must also include new statutory enforcement mechanisms. CDT supports the Commission's continued requests for civil penalty authority.[58] We have long recommended that any reasonable response to addressing business use of personal information requires civil penalty authority. [59] Because much of the Commission's privacy and data security enforcement falls under Section 5 of the FTC Act, which does not provide for civil penalties, companies are functionally afforded one free "bite at the apple."[60] Before a company may be fined for violating individuals' privacy, it must first agree to and be placed under a consent decree and then subsequently violate that agreement.

This process has been inadequate either to protect user privacy or meaningfully punish companies for violations. The resulting penalties can be so miniscule as to ensure the penalties are simply the cost of doing business.[61] For instance, when Google agreed to pay a $22.5 million penalty for violating the terms of its consent order in 2012, this was approximately five hours worth of Google's revenue at the time.[62]

In some instances, no penalty is forthcoming or is levied after an unreasonably long period of time. Facebook has been under a consent decree throughout the entire duration of its dealing with Cambridge

---

[56] *Cf.* Megan Gray, https://twitter.com/megangrA/status/1059474790153703424.

[57] Sen. Ron Wyden, Press Release, Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy (Nov. 1, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.

[58] Fed. Trade Comm'n, Press Release, FTC Testifies before House Energy and Commerce Subcommittee about Agency's Work to Protect Consumers, Promote Competition, and Maximize Resources (July 18, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/ftc-testifies-house-energy-commerce-subcommittee-about-agencys (noting that Section 5 does not provide for civil penalties, "reducing the Commission's deterrent capability" and seeking "civil penalties to effectively deter unlawful conduct").

[59] Ctr. for Democracy & Tech., Refocusing the FTC's Role in Privacy Protection (2009), https://www.cdt.org/files/privacy/20091105_ftc_priv_comments.pdf.

[60] Dissenting Statement of Commissioner J. Thomas Rosch, In the Matter of Google Inc., FTC Docket No. C-4336 (Aug. 9, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googleroschstatement.pdf.

[61] *Id.* Commissioner Rosch noted that a $22.5 million fine "represents a de minimis amount of Google's profit or revenues."

[62] Megha Rajagopalan, Is $22.5 Million a Big Enough Penalty for Google?, Business Ethics (Aug. 14, 2012), http://business-ethics.com/2012/08/14/10058-is-22-5-million-dollars-a-big-enough-penalty-for-google/.

1401 K Street NW, Suite 200 Washington, DC 20005

Analytica, as well as its merger of data between its Facebook platform and WhatsApp. Eight months ago the FTC announced that it was investigating Facebook,[63] and in that time, foreign regulators like the UK Information Commissioner's Office have managed to conclude its own investigation.[64]

At this point, it appears evident that the FTC consent decrees do not sufficiently restrain companies' irresponsible data practices.[65] U.S. policymakers and civil society have operated under the assumption that FTC investigations were adequate to drive business accountability, but absent adequate fining authority and the ability to mandate changes in corporate practice, consent decrees increasingly look like privacy paper tigers.

2. *Section 5 of the FTC Act's prohibition of unfair business practices must be extended to reach noneconomic informational injuries.*

Nearly twenty years of FTC privacy enforcement have revealed that the FTC's authority to proactively police privacy and require affirmative changes to business practices are curtailed by the Commission's powers under Section 5 of the FTC Act. This requires rulemaking authority, or more ambitiously, modifications of Section 5 to capture the unique consumer harms posed by data processing. We note that Sen. Ron Wyden's recent proposal also amends the statutory language of Section 5 to direct the FTC to consider privacy injuries that involve "noneconomic impacts and those creating a significant risk of unjustified exposure of personal information.''[66]

An alternative approach would be for the FTC to consider the role of established public policy when evaluating unfair data practices. Though frequently minimized by both commentators and the FTC, larger public policy considerations an important component of conversations around informational injuries.[67] Professor Dennis Hirsch recommends that constitutional doctrines of equal protection and due process, anti-discrimination laws, rules governing racial profiling, statutes such as the Genetic Information Nondiscrimination Act that limit secondary uses of personal data, state laws limiting

[63] Federal Trade Comm'n, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[64] UK Info. Commisioner's Office, Press Release, ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information (Oct. 25, 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/.

[65] *See also* Federal Trade Comm'n, Press Release, Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims (Apr. 12, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security.

[66] Wyden, *supra* note 57, sec. 3.

[67] *See* FTC Policy Statement on Unfairness (Dec. 17, 1980); *see also* Dennis D. Hirsch, That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority, 103 Ky. L.J. 345, 361 (2015) (arguing that "[o]ver time, FTC unfairness adjudications will produce a set of precedents, grounded in 'established public policies,' that will draw a line between appropriate uses of big data, and inappropriate uses; between fair practices, and unfair ones.").

employer access to and use of employee social media postings, and the FTC's own established policies should inform whether secondary uses of information are unfair.[68] He recommends that Congress instruct consumer protection agencies like the FTC to use its existing unfairness authorities "to prevent manipulative and biased big data business practices."[69]

--

CDT appreciates the NTIA's commitment to the project of advancing consumer privacy protection; we are also cognizant of the Department of Commerce's overarching goal of promoting innovation and U.S. leadership in emerging technologies. The NTIA's general outcomes are sound, but to the extent companies are currently seeking these ends, they have struggled to provide protections that are substantive and tangible for individuals. This is where the United States needs specific rights that are created through legislative action in Congress. The administration should champion this, and CDT looks forward to working with the NTIA as it proposes concrete language to this end.

Thank you,

Joseph Jerome
Policy Counsel
Center for Democracy & Technology

Michelle Richardson
Director, Privacy & Data Project
Center for Democracy & Technology

[68] Dennis Hirsch, To solve the Facebook problem, think big (data), The Hill (April 24, 2018), https://thehill.com/opinion/technology/384239-to-solve-the-facebook-problem-think-big-data.
[69] *Id.*