Statement of Michelle Richardson, Director, Privacy & Data
Center for Democracy & Technology

before the
United States Senate Committee on Commerce, Science and Technology
Examining Legislative Proposals to Protect Consumer Data Privacy
December 4, 2019

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to testify about comprehensive federal privacy legislation. CDT is a nonpartisan, nonprofit 501(c)(3) charitable organization dedicated to advancing the rights of the individual in the digital world. CDT is committed to protecting privacy as a fundamental human and civil right and as a necessity for securing other rights such as access to justice, equal protection, and freedom of expression. CDT has offices in Washington, D.C., and Brussels, and has a diverse funding portfolio from foundation grants, corporate donations, and individual donations.[1]

The Need for Comprehensive Federal Legislation

The U.S. privacy regime today does not efficiently or seamlessly protect and secure Americans' personal information. Instead of one comprehensive set of rules to protect data throughout the digital ecosystem, we have a patchwork of sectoral laws with varying protections depending on the type of data or the entity that processes the information. While this approach may have made sense decades ago, it now leaves a significant amount of our personal information - including some highly sensitive or intimate data and data inferences - unprotected.

Our current legal structure on personal data simply does not reflect the reality that the internet and connected services and devices have been integrated into every facet of our society. Our

[1] All donations over $1,000 are disclosed in our annual report and are available online at: https://cdt.org/financials/.

schools, workplaces, homes, automobiles, and personal devices regularly create and collect, and, increasingly, infer, intimate information about us. Everywhere we go, in the real world or online, we leave a trail of digital breadcrumbs that reveal who we know, what we believe, and how we behave. Overwhelmingly, this data falls in the gaps between regulated sectors.

The lack of an overarching privacy law has resulted in the regular collection and use of data in ways that are unavoidable, have surprised users, and resulted in real-world harm. A constant stream of discoveries shows how this data can be repurposed for wholly unrelated uses or used in discriminatory ways.

While the Federal Trade Commission's ability to police unfair and deceptive practices provide a backstop, large policy gaps around access, security, and privacy exist, which confuse both individual consumers and businesses. Because the FTC is prohibited from using traditional rulemaking processes, the agency has developed a "common law" of privacy and security through its enforcement actions.[2] Creating proactive privacy rights through an episodic approach will not be able to keep up with advances in technology and the explosion of device and app manufacturers.

Privacy and Data Security Legislation Pending in December 2019

Despite repeated criticism that Congress had not moved on privacy legislation, this Committee as well as other committees of jurisdiction have held meaningful hearings over the last year. The chair, ranking member, and several other Commerce committee members have introduced legislation on comprehensive privacy legislation or some piece of the bigger picture. Below are a number of key issues and discussion of how they can be addressed in legislation.[3]

Scope of legislation

Covered entities. It's crucial that any comprehensive privacy law cover all private sector entities that collect, use, and share personal information.[4] This includes not only the prominent tech

[2] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 606–27 (2014).

[3] CDT focuses here on proposals authored by Chairman Wicker and Ranking Member Cantwell. CDT will have additional analysis on issues not addressed here, time permitting. Legislation by Committee members Thune, Blunt, Fischer, Blackburn, Blumenthal, Schatz, Markey, Klobuchar, and Peters all include important principles or language that can contribute to the final bill.

[4] We do not have a final recommendation as to whether HIPAA, Gramm-Leach-Bliley, FCRA or other existing consumer privacy laws should be reformed and made consistent with comprehensive proposals. CDT generally supports updating those laws, but Congress should move forward in the currently unregulated space if addressing financial services, health care and other sectors becomes an impasse.

companies that have captured our attention recently, but also not-for-profit entities and the communication providers that are currently under FCC jurisdiction for privacy and security enforcement. Creating a single federal standard will ensure that individuals can rely on the same baseline rights as they move across the digital ecosystem. To that end, Chairman Wicker's staff discussion draft[5] is one of the more comprehensive proposals.

We also recommend that legislation not categorically exempt small businesses.[6] They may collect, use, and share data in many of the same ways as larger entities.From the perspective of an individual consumer, the harms they experience are not mitigated because a company has fewer customers or makes less money. A privacy law that is clear and reasonable need not put an undue compliance burden on smaller entities, and many of the provisions in the bills authored by Chairman Wicker and Ranking Member already meet that test.

If the Committee feels that some procedural requirements are too much for a small business to comply with, legislation should adopt the Wicker staff discussion draft approach and exempt smaller entities from specific requirements. For example, it is more important that small businesses meet data security requirements, offer opt-ins, avoid discimination, and provide access, correction, and deletion rights. It is less important that they conduct broader risk assessments, have certain staff members, or provide in depth reporting on their data practices.

Covered data. It is also important that legislation cover all personal data even if the Committee decides that there may be tiers of sensitivity that warrant different substantive requirements. We strongly recommend that the committee define covered personal information consistent with current FTC guidance which is best reflected in Ranking Member Cantwell's draft bill as "information that identifies, or is linked or reasonably linkable to an individual or consumer device, including derived data."[7] The additional qualifier that this data "can be used on its own or in combination with other information held by, or readily accessible to, the covered entity"[8] as proposed in the Wicker staff draft may be overly restrictive. Distinguishing between data that is linkable and that which is not serves two purposes. First, to discourage first parties from unnecessarily associating information with real people, but second, to offer down stream protections when information is shared with affiliates, third parties, or even in the instance of a data breach. These additional reasons for storing and using data in de-identified format will be frustrated by a definition that so heavily focuses on first party linkability.

---

[5] STAFF OF S. COMMERCE COMM. CHAIRMAN WICKER, STAFF DISCUSSION DRAFT (2019) *available at:* https://aboutblaw.com/NaZ (hereinafter WICKER DISCUSSION DRAFT).

[6] Pending proposals that define small businesses as those with a small number of users are more meaningful than previous iterations that focused solely on income or number of employees. These latter two metrics do not have a bearing on whether certain data harms will be deeply or widely felt by users. Ideally, a bill will borrow from the FTC's current guidance that focuses on number of users (5,000) and minimal data processing practices. FED. TRADE COMM. REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 15–16 (2012).

[7] Consumer Online Privacy Rights Act, S. ____, 116th Cong. § 2(8) (2019) (hereinafter COPRA).

[8] WICKER DISCUSSION DRAFT, § 2(7).

Corporate Responsibility

The core of any privacy and security law must be corporate responsibility. While we should respect the rights of individuals to control their data, any systemic change will have to come from the entities that collect, use, and share data themselves. While a new law will have to regulate businesses of varying sizes, business models and data uses, there are some requirements that can be imposed across the board to ensure individuals receive digital civil rights that do not require them to micromanage the relationships they have with companies. All of the components of corporate responsibility are contained in the bills introduced in the Senate to date and only need to be stitched together to provide meaningful consumer protection.

Data use. Both Chairman Wicker and Ranking Member Cantwells' bills begin to address the exceptionally hard question of whether and how to regulate the use of data beyond any opt-in requirement. The FTC continues to develop a body of common law to prohibit certain data uses on a case by case basis, but a federal privacy law can and should go one step further to categorically prohibit some of the riskiest data uses.

Data use limitations exist to some extent in Chairman Wicker's minimization section[9] and Ranking Member Cantwell's loyalty section.[10] The committee could also borrow from legislation sponsored by Senators Blunt and Schatz on facial recognition technology[11] and Senator Markey's comprehensive privacy bill.[12] Ultimately, data use limitations must go beyond limiting data use to what a company *says* it will do with data, to creating an objective limitation regardless of what any one privacy policy entails. While there are a number of ways to craft this, a clear purpose limitation on sensitive data will make great strides towards aligning consumer knowledge and expectations with corporate behavior. To the extent that some provisions peg data use to what a company believes is a "reasonable" consumer expectation, they may be subject to bad faith arguments or protracted litigation about what exactly a "reasonable consumer" is.

Artificial intelligence and civil rights. Both bills recognize the importance of providing oversight of artificial intelligence programs and reinforcing longstanding discrimination laws that may be undercut by current data practices. Despite their differences, we hope this signals a commitment to addressing these issues in any final privacy and security legislation. CDT prefers the breadth and depth of Ranking Member Cantwell's approach and looks forward to working with the committee on refining these requirements as necessary as the legislation moves forward.

[9] WICKER DISCUSSION DRAFT, § 105.
[10] COPRA, § 101.
[11] Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. § 3 (2019).
[12] Privacy Bill of Rights Act, S. 1214, 116th Cong. § 3 (2019).

Data security. CDT commends Chairman Wicker and Ranking Member Cantwell for including data security requirements in their draft bills. Close to half of US states do not have a general purpose data security law, and FTC enforcement under its Section 5 authority will always be limited to what its resources allow. We recommend combining the two and adding one additional provision.

First, the committee should adopt Chairman Wicker's base text in section 204 regarding the requirements of a reasonable data security program. Second, the committee should adopt Ranking Member Cantwell's scoping of data to be covered. Her draft protects not only sensitive information, but all personal information. Because both bills impose a reasonableness standard that will peg to the size and complexity of the organization and the sensitivity and use of the data, it is unnecessary to exempt certain data sets from the overall security requirement. Third, this section should provide overall rulemaking for the FTC. Right now, the Wicker and Cantwell bills require guidance or limited rulemaking, but it is time for the longstanding guidance of the FTC to be written into regulation. To the extent that some in the corporate sector have criticized the FTC's data security requirements as too vague despite long-standing guidance in this space, they will benefit from having regulations on the books to better describe requirements.

Individual rights

Both the Wicker and Cantwell drafts offer meaningful individual controls to individuals and we commend the comprehensive approach contained in them.

Opt in requirements for sensitive data. Both bills include a comprehensive list of sensitive data that is subject to affirmative, express consent. The differences are minimal but the definitions should be amended in a few key ways. First, the committee should adopt an expansive definition of health information, and we recommend borrowing from CDT's model legislation[13] which incorporates not only data that reflects a person's mental and physical status, but data that is processed for health or wellness purposes. As Senator Klobuchar and Murkowski recognize in their Protecting Personal Health Data Act,[14] apps, wearables, and devices are creating and collecting intensely personal information that can be used in ways that greatly affect a person's mental and physical well-being. Any definition should ensure that these resulting data sets receive heightened protection.

Second, sensitive data should include Ranking Member Cantwell's formulation of "information revealing online activities over time and across third-party website[s] or online services."[15] This formulation is meaningfully different from the type of data that will be regulated by "Do Not

[13] CTR. DEMOCRACY & TECH., CDT FEDERAL BASELINE PRIVACY LEGISLATION DISCUSSION DRAFT, § 1(2) (2018). https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.
[14] Protecting Personal Health Data Act, S. 1842, 116th Cong. § 2 (2019).
[15] COPRA, § 2(20(J).

Track" functions the FTC would facilitate under either proposal.[16] We understand this to mean data collection that is more pervasive and intrusive than first party tracking or one-off identification of an individual which arguably deserve less protection. This formulation is also consistent with Senator Blackburn's BROWSER Act[17] which has long recognized the unique place at which edge providers sit in the ecosystem. While all entities should play by the same set of rules, recognizing that long term tracking of this data is particularly risky for privacy and security is consistent with the overall approach of the bills.

Product development exception. In general, the list of exceptions to the opt-in right contains reasonable data use that is core to offering the product an individual signs up for. They fairly recognize that some data processing is absolutely necessary to offer safe and effective products and cannot be opted out of either individually or at scale. However product development as listed in Chairman Wicker's staff discussion draft is meaningfully different from the rest of the data uses. It permits companies to collect data without someone's consent even if they have no understanding of how it will be used or whether they will benefit from the use at some point in the future. Since product development is solely for the benefits of the companies who collect the data - unlike everything else on this list of exceptions-- it should not be done without an individual's consent. To the extent the Committee does not want to inhibit innovation, it should further explore why the de-identification carve out is insufficient for product development, and whether some middle ground should be created for processing data this way.

Access correction deletion portability. The individual controls are comprehensive. Our only suggestion is that the Committee include the timelines drafted into Wicker's staff discussion draft to ensure that rights are afforded on a reasonable timeframe.[18]

Data broker registry. We commend the Wicker staff draft for including a data broker registry housed at the FTC.[19] A registry will ensure that individuals can discover and exercise their rights against data brokers who have amassed incredible amounts of sensitive data on the average American. While many of the provisions in both the Cantwell and Wicker drafts may slim down the amount of information that eventually ends up in data broker databases, these entities are likely to continue collecting information and will still be holding data that has been accrued over decades of largely unregulated data use. That someone can exercise their access, correction, and deletion rights against these entities is the best protection against future data abuse.

[16] COPRA §, 105(b); WICKER DISCUSSION DRAFT, § 104(a–b).
[17] Balancing the Rights Of Web Surfers Equally and Responsibly Act of 2019, S. 1116, 116th Cong. § 2(12) (2019).
[18] WICKER DISCUSSION DRAFT, § 103.
[19] *Id.* § 203.

Enforcement

Both Chairman Wicker and Ranking Member Cantwell's drafts include meaningful enforcement mechanisms, but they differ in a few important ways.

First, Ranking Member Cantwell includes a private right of action ("PROA") for all violations of the law.[20] CDT believes a targeted private right of action is necessary for meaningful enforcement. This is not only because the number of entities that will be swept under new regulations will necessarily dwarf the resources of the FTC and state attorney generals, but because our history is full of instances where government actors simply did not have the wherewithal to be first movers on important social issues. Because private litigation has served such an important function in civil and consumer rights enforcement in the past, it should be reserved in some form in federal privacy legislation.

It is important to note that all 50 state unfair and deceptive practice laws include some form of a private right of action, even if substantially limited.[21] If a privacy bill seeks to categorically move privacy and data security out of these laws,[22] it should ensure that consumers are at least equally positioned to defend their rights as they are now.

The proper balance likely lies between the Cantwell and Wicker drafts in a specific delineation of what provisions can be enforced by PROA and under what conditions. State and federal laws are full of examples where PROAs are crafted to limit litigation to the most important harms. We recommend that the Committee consider this approach to find the right way to maximize accountability and minimize nuisance litigation. Such litigation controls could include opportunities to cure, harm requirements, reduced or nonexist damages or prior agency review, for example. We look forward to working with the Committee further on finding the right way forward on PROAs.

Second, legislation should allow state attorneys general to bring cases in state court and should not force consolidation of cases into the D.C. Circuit. Courts at every level are backlogged and funneling enforcement into too few courts will greatly delay meaningful defense of consumer rights.

---

[20] COPRA, § 301(c).
[21] CAROLYN CARTER, NAT'L CONSUMER LAW CENT., CONSUMER PROTECTION IN THE STATES: A 50-STATE EVALUATION OF UNFAIR AND DECEPTIVE PRACTICES LAWS 32–46 (2018).
[22] While California has a general purpose privacy law, and some states have targeted regulation like Illinois' Biometric Information Privacy Act, privacy law is overwhelming homed in state UDAP statutes at present. Similarly, roughly half of states do not have express data security requirements, so enforcement against unreasonable data security falls under UDAPs too. NAT'L CONFERENCE OF STATE LEGISLATURES, DATA SECURITY LAWS: PRIVATE SECTOR (May 29, 2019) http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

Conclusion

CDT thanks the Commerce Committee for the opportunity to testify about privacy legislation today. We are encouraged by the many thoughtful proposals already introduced in the Senate and believe that passing a single comprehensive privacy and security law should be a priority for committee action in 2020.