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

New York State Senate
Standing Committee on Consumer Protection
Standing Committee on Internet and Technology

Protecting Consumer Data and Privacy on Online Platforms
November 22, 2019

The Center for Democracy and Technology commends Chairs Thomas and Savino and their committees for continuing their inquiry into modern data practices and how to draft a meaningful privacy law for New York citizens.

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 believes that new laws are the only way to clear the immense privacy and security debt we've accrued over the decades.

When we testified before this committee in June, we used location information as an example of how current law has failed to protect even the most sensitive information. We also flagged some of the trickier drafting challenges you would face like avoiding loopholes that may undercut an otherwise meaningful privacy law. We now submit this written statement as a roadmap to drafting the next iteration of the New York Privacy Act.[1]

[1] New York Privacy Act, S. 5642, 2019–20 Reg. Sess. (N.Y. 2019).

Overarching principles

First, the law must shift the burden of protecting privacy from individuals[2] back on to covered entities where it belongs. Any proposal that leaves individuals responsible for navigating controls for the hundreds of devices, accounts, apps and websites they interact with every day will not result in systemic change. While individual choice has a role in our digital ecosystem, it is not a substitute for requiring companies to meet a baseline of behavior that treats people and their data fairly.

Second, the law should apply to all entities that hold personal information. This includes not only the large tech companies that have captured our attention as of late, but telecommunication and internet service providers and not-for-profit organizations. Despite our different sizes, services, and business models, we can be governed by a single set of rules if they are clear and practical.

Third, the law should greenlight low-risk activities that are widely accepted as incidental to offering services and redlight the riskiest behavior. People and companies alike will benefit from this clarity and consistency across the ecosystem. While flexibility may allow a law to evolve with technology, too much of it can increase compliance costs and subject a law to constitutional challenges of vagueness. We know the behaviors that offend the average user or contribute to discrimination or exploitation. It's time to prohibit these practices.

Fourth, the law should provide for meaningful enforcement. Each state and the federal government will have to grapple with sweeping the data economy under new regulation. All of them will have to increase resources for this law to be meaningful, but New York should also consider whether a targeted private right of action can assist in cases that are a clear-cut violation of the most important consumer protections.

[2] We use people, individuals, consumers, users and communities interchangeably to represent the people whose information is collected and used. Some may not be "consumers" in the traditional sense because they lack a business relationship with the entity and some may not be "users" because they are not intentionally interacting with a company. We also use "company" in this statement as a generic reference to those entities that collect or use information outside of a completely individual and personal use.

Components of a statute

Translating these principles into legislation is complicated, but there is much that the New York Privacy Act (NYPA) already gets right. There is also plenty to borrow from new laws in California and Europe and text drafted by other legislative bodies and organizations like CDT.[3]

Corporate responsibilities. The New York Privacy Act's inclusion of "fiduciary duties" is a promising first step towards clearer obligations on corporate actors. In your next iteration, we strongly recommend converting some of this section into more explicit requirements and limitations. Clearer rules will ensure that individuals have meaningful rights on day one and shield the law from protracted litigation over what exactly it entails. Such rules may not be able to account for every possible use case, but they can meaningfully address many of them. Most important to this approach is imposing limitations on the collection, use, and sharing of personal information.

The committee should consider a more general minimization requirement that applies to all data. The US and international bodies have recognized this principle for decades,[4] and modern privacy laws like GDPR, and legislation pending at the state and federal level are starting to incorporate this as an affirmative obligation. GDPR talks of necessity, proportionality and purpose limitations- ideas that have and will continue to stand the test of time. Other possible language can be found in the pending ballot initiative in California to amend the CCPA.[5]

---

[3] General Data Protection Regulation 2016/679; California Consumer Privacy Act, ch. 55, 2018 Cal. Legis. Serv. 1809 (to be codified at Cal. Civ. Code § 1798.100); CTR. DEMOCRACY & TECH., *CDT FEDERAL BASELINE PRIVACY LEGISLATION DISCUSSION DRAFT (2018)* https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.

[4] ORG. ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK (2013) https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf; NAT'L INST. STANDARDS & TECH., STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS, FIPS PUB 199 (2004) https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf.

[5] "A business's collection of a consumer's personal information shall be limited to personal information that is reasonably necessary to achieve the purposes for which it is collected." The California Privacy Rights and Enforcement Act of 2020, Ballot Initiative 19-0019, (would amend Cal. Civ. Code Sec. 1798.100(c)) (Oct. 2, 2019) https://oag.ca.gov/system/files/initiatives/pdfs/19-0019%20%28Consumer%20Privacy%20-%20Version%202%29.pdf.

It's important to note that some formulations of this principle are still missing the mark in important ways. For example, the most recent version of the Washington Privacy Act[6] includes duties of purpose specification, minimization, and limits on secondary use. This is an excellent start, but those obligations are tied to what a company says it will do with the information. As a result, it is closer to a deception prohibition- requiring companies to follow through on their promises–than a substantive limitation on what data can be collected and used.

At the very least, you should prohibit the collection, use, and sharing of sensitive personal information that is not necessary for the delivery of a product, service, or feature a user requested. A clear bright line rule for data like precise geolocation information, biometrics, health data and other especially sensitive categories will deter some of the most offensive behavior in our current ecosystem. It will also relieve so much of the pressure on users to make granual decisions about many different actors, platforms and services which are beyond the capacity of any normal person. CDT's model legislation provides an example of this language.[7]

Individual rights. The New York Privacy Act already includes a comprehensive list of consumer rights in Section 1103, which we commend. Of particular note, this section avoids many of the pitfalls found in other proposals, such as overbroad exceptions or lack of clarity about the frequency or cost of exercising these rights.

If you are considering edits to this section, we recommend that you take extra care to preserve the following features. First, these rights should be available at a reasonable frequency and without cost to the consumer, assuming no manifestly excessive use. Data can be amassed so quickly that these rights could be meaningfully exercised twice a year as the bill allows. Second, there should be reasonable deadlines by which an entity must respond to consumers, and the proposed 30 days with an additional 60 day extension is fair to both companies and consumers alike. Third, controllers should be responsible for notifying third parties to which it sold a consumer's data when she

[6] Consumer Privacy DRAFT version 1, November 12, 2019, on file with Senator Reuven Carlyle.
[7] CTR. DEMOCRACY & TECH., CDT FEDERAL BASELINE PRIVACY LEGISLATION DISCUSSION DRAFT, 10–13 (2018) https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.

requests data deletion. This shifts the burden of tracking and notifying third parties who obtain an individual's data to the entity that chose to sell the data in the first place.

Finally, the NYPA borrows an important principle from GDPR that we recommend the committee refine going forward. Section 1103(k6) states that a person shall not be subject to profiling - defined as using automated decision making programs without human intervention - in high impact use cases like those that affect health or economic situation. This section could be clarified as some terms like "personal preferences" or "interests" are quite broad and sweep in information that may not need heightened protection.

Conclusion. Thank you for the opportunity to submit this statement. Crafting a meaningful privacy law is complicated and hearings like this are necessary to make informed decisions about how to proceed. We look forward to providing additional feedback as legislation moves forward.