Statement of Joseph Jerome, Policy Counsel, Privacy & Data Project
Center for Democracy & Technology

before the
New York Senate Senate Standing Committee on Consumer Protection
New York Senate Standing Committee on Internet and Technology
hearing on Online Privacy and Role of Legislature

June 4, 2019

Dear Chairpersons Thomas and Savino, and Members of the Committee:

Thank you for the opportunity to testify today. I speak on behalf of the Center for Democracy & Technology, a non-profit, non-partisan technology advocacy organization based in Washington, D.C. CDT has long worked to promote laws that protect individuals' privacy and security online.

The goal of my testimony today is to explain to you why privacy is important and the urgent need for laws that limit companies' ability to use and abuse our data. Unregulated data processing has real world impacts that extend far beyond headlines about Facebook or generalized concerns about online ad tracking. I would like to highlight a few areas where privacy law could help to curtail unfair and discriminatory corporate behaviors.

- **First, "take-it-or-leave-it" privacy policies disadvantage low-income Americans.** The irony of so-called "notice-and-choice" is that it gives people very little choice in how they share personal information. Not using an app or service is not a real option. This lack of choice is especially stark for low-income Americans, who rely on mobile technologies and cannot shop around for devices or services that provide better privacy protections.[1] Low-income customers are least able to pass up on incentive programs like grocery store loyalty cards, which feed into data brokers that profile and score people based on incomplete information that affects people's opportunities in

[1] Pew Research Ctr., Mobile Fact Sheet (Feb. 5, 2018), https://www.pewinternet.org/fact-sheet/mobile/.

ways no one understands. Dozens of different data brokers operate different opt-outs.[2] Any restriction on data flows can help protect these communities.

- **Second, commercial surveillance technologies take advantage of power imbalances.** New technologies, including face tracking, make spying on New Yorkers easier than ever before. Without appropriate safeguards, the design and proliferation of these products can facilitate abuse. For example, smart lock company Latch allowed landlords to track their tenants.[3] Residents in a New York City apartment building found themselves needing a smartphone app just to get into the building's lobby, elevator, or mail room. Five tenants had to go to court just to enter their apartments using good-old-fashioned keys.[4] New privacy laws compensate for these power imbalances by creating costs to cavalier data practices.
- **Third, location data sharing is exploitative and raises legitimate safety considerations.** I want to stop and emphasize location data for a moment -- the reality is that companies have been careless in how they collect, share, and sell our location information. *The New York Times* recently revealed that many of the apps that collect location information repurpose or share that information with third parties.[5] In early 2019, mobile phone carriers were again caught sharing location data with third-party aggregators -- data that has ended up in the hands of bounty hunters.[6] Stalkers, aggressive debt collectors, and the watchful eyes of law enforcement use this data to harass people. Their recourse is limited. The National Network to End Domestic Violence (NNEDV) advises survivors who are concerned they may be tracked to simply turn their phones off.[7] No one should have to make the choice between using a cell phone and being safe from stalking.

The burden of protecting privacy cannot fall on consumers. Companies can promise to be more transparent, to provide more clarity in how they collect and use our information, but no amount of

---

[2] Steven Melendez & Alex Pasternack, *Here are the data brokers quietly buying and selling your personal information*, Fast Company (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[3] Sage Lazzaro, *America's Favorite Door-Locking App Has a Data Privacy Problem*, OneZero (Apr. 29, 2019), https://onezero.medium.com/tagged/latch.

[4] Priscilla DeGregory, *Hell's Kitchen tenants win battle to use keys instead of high-tech entry system*, N.Y. Post (May 7, 2019), https://nypost.com/2019/05/07/hells-kitchen-tenants-win-battle-to-use-keys-instead-of-high-tech-entry-system/.

[5] Jennifer Valentino-DeVries et al, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[6] Zack Whittaker, *Despite promises to stop, US cell carriers are still selling your real-time phone location data*, TechCrunch (Jan. 9, 2019), https://techcrunch.com/2019/01/09/us-cell-carriers-still-selling-your-location-data/; Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8, 2019), https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

[7] National Network to End Domestic Violence, Data Privacy Day 2019: Location Data & Survivor Safety (Jan. 28, 2019), https://www.techsafety.org/blog/2019/1/30/data-privacy-day-2019-location-data-amp-survivor-safety.

notice will help the average New Yorker grapple with the dozens and dozens of businesses that collect and share their information.[8] We need clear rules for what companies can and cannot do with data.

My organization, CDT, supports a federal solution to these problems,[9] but as Congress delays and delays, states must step into the breach. The California Consumer Privacy Act (CCPA) is not an outlier -- it joins state laws in Illinois, Vermont, and Massachusetts.[10] New York has an opportunity to shape that national conversation about what companies can do with our personal data.

Any meaningful privacy regulation will have five key components. **First**, it must provide for individual rights to access, correct, delete, and port personal information. **Second**, it should require reasonable data security measures and make companies responsible for how they handle information. **Third**, it should include explicit use limitations, particularly the repurposing or secondary use of sensitive data like geolocation information. **Fourth**, it should help address data-driven discrimination and civil rights abuses. **Finally**, it must provide for strong enforcement.

It is important that these components not be watered down by definitions or provisions that undermine the rule. Lack of clarity invites corporate malfeasance and exploitation, and overbroad exceptions create loopholes that swallow well-intended privacy protections.

For example, what "personal data" that is covered by the law is critical. A line must be drawn somewhere between personal and non-personal data, the argument goes, or else laws will capture all information even if it presents no risks to an individual's privacy. This oversimplifies how data is collected and processed, but it helps to explain why you will hear calls to both narrow the scope of "personal data" that is protected and broaden the definition of "de-identified data" that can be excluded from protection.[11] Unfortunately, companies have played fast-and-loose with how they define "personal data." They use opaque techniques to identify people. For example, retailers asked consumers their zip code and used this in combination with their name from credit card swipes to do reverse lookups with data brokers.[12]

Importantly, the New York Privacy Act includes a rigorous and meaningful de-identification exception.[13] While companies want an escape valve from having to give the same level of protection to all

---

[8] Center for Democracy & Tech., *Notice and Choice Are No Longer a Choice* (Mar. 1, 2019), https://cdt.org/blog/notice-and-choice-are-no-longer-a-choice/.

[9] *See* Center for Democracy & Tech., Federal Privacy Legislation, *available at* https://cdt.org/campaign/federal-privacy-legislation/.

[10] *See* Illinois' Biometric Information Privacy Act (740 ILCS 14/5), Vermont's Data Broker Law (9 V.S.A. §§ 2430, 2433, 2446 and 2447), and Massachusetts' Data Security Regulations (201 CMR 17.00).

[11] For additional discussion, see Center for Democracy & Tech., *The Washington Privacy Act Raises Important Considerations for Comprehensive Privacy Proposals* (2019), and accompanying letters, *available at* https://cdt.org/blog/the-washington-privacy-act-raises-important-considerations-for-comprehensive-privacy-proposals/.

[12] *See* Comments from Professor Chris Hoofnalge on Assembly Bill 375 (Mar. 8, 2019), *available at* https://hoofnagle.berkeley.edu/2019/03/08/comments-on-the-ccpa/#_ftn4 (citing Pineda v. Williams Sonoma, 51 Cal.4th 524, 2011 WL 446921).

[13] § 1100(6).

information at all times, companies can be quick to claim information is anonymous when it is not. Again, let me mention location data. De-identified location data can be re-identified with relative ease, and just a handful of location and time-stamped data points are needed to exploit anonymous location data.[14]

The fundamental problem, however, is that companies should not be put in the position of deciding what privacy risks to subject consumers to. For one, there is not a shared understanding of what risks to consider. When companies insist that only "concrete and tangible" privacy risk should be considered, this is code for limiting any consideration to financial harms. But privacy risks exist beyond economic loss and include diminished autonomy and self-determination, discrimination, and generalized loss of trust.[15] While the New York Privacy Act includes an expansive set of risks drawn from existing industry privacy proposals,[16] the reality is that companies have every incentive to take a narrow view of privacy risk that does not reflect either our shared values or the concerns of the most vulnerable among us.

Rather than giving businesses discretion to determine whether their data practices are risky, we need explicit limits on what companies can or cannot do with information. This is why my organization, CDT, has proposed privacy legislation that limits certain data processing activities where not required for a product, service, or function requested by an individual.[17]

Once more, location data serves as a perfect example for why such restrictions can be useful. As the executive director of Engine Advocacy, a non-profit network of startups, testified before Congress, flashlight apps have no "clear functional need to access a user's precise geolocation information to deliver its service",[18] and yet Goldenshores Technologies' Brightest Flashlight app did just that.[19] A risk assessment is not necessary to say in law that apps should not be collecting location data they do not need.

New Yorkers deserve stronger protections for their personal data, and the time has come to hold companies to account for failing to account for the privacy and security risks of their practices. CDT stands ready to serve as a resource to members of this committee as you grapple with the privacy

---

[14] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, & V. D. Blondel, Unique in the Crowd: The Privacy Bounds of Human Mobility, Scientific Reports 3: 1376 (2013).

[15] This framing is recognized by the National Institute of Standards and Technology. 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.

[16] § 1102(2); *see also* Intel U.S. Draft Privacy Legislation (2019), *available at* https://usprivacybill.intel.com/legislation/.

[17] *See* Center for Democracy & Tech., Federal Privacy Legislation, *available at* https://cdt.org/campaign/federal-privacy-legislation/.

[18] Testimony of Evan Engstrom, Executive Director, Engine Advocacy and Research Foundation, on "Small Business Perspectives on a Federal Data Privacy Framework" (Mar. 26, 2019), https://www.commerce.senate.gov/public/_cache/files/949f1fc8-dc28-4760-9f47-6cb925a1549e/0AE3566F5899E50A6C4D08C7142D8752.testimony-of-evan-engstrom-engine.pdf.

[19] Tom Warren, *Millions of Android users 'deceived' by flashlight app that shares location with advertisers*, Verge (Dec. 6, 2013), https://www.theverge.com/2013/12/6/5181472/brightest-flashlight-free-ftc-location-data-settlement.

challenges posed by today's online economy. The Senate's efforts to advance comprehensive privacy protections through the New York Privacy Act (S 5642) and to strengthen data security obligations through the SHIELD Act (S 5575) are a strong first step.

I look forward to any questions you may have.