STATEMENT OF
ALBERT FOX CAHN, ESQ.
EXECUTIVE DIRECTOR
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, INC.

BEFORE THE
STANDING COMMITTEE ON CONSUMER PROTECTION
&
STANDING COMMITTEE ON INTERNET AND TECHNOLOGY
NEW YORK STATE SENATE

FOR A HEARING CONCERNING,
ONLINE PRIVACY & ROLE OF STATE LEGISLATURE SHOULD PLAY IN
OVERSEEING IT.

SUBMITTED
June 5, 2019
Thank you for the opportunity to submit written testimony. My name is Albert Fox Cahn, Executive Director of the Surveillance Technology Oversight Project (“STOP”). STOP advocates and litigates for New Yorker’s privacy rights, fighting discriminatory surveillance. I commend the committees, Chairs Thomas and Savino for today’s hearing; for bringing much-needed attention to issues of online privacy.

As data collection advances, so too should the privacy protections for New York residents. Corporations have increasingly unfettered access to our information, everything from purportedly “private” messages to our biometric data. But the corporate sector is not alone. Government agencies amassed Orwellian databases that vitiate our constitutional guarantees of privacy and autonomy. The threats are clear, and New York’s response must be equally concrete, ensuring that our privacy protections keep pace with developments in technology.

**Corporate data collection**

It is increasingly inconceivable for consumer to opt-out of corporate data collection without opting out from modern life. As the Supreme Court has repeatedly recognized, a cell phone is practically “a feature of human anatomy.” While the Court is vocal that Americans need not concede their privacy simply for engaging in the public sphere, its decisions have not kept pace with its rhetoric.

Today, data brokers can accumulate data from millions of unexpected New Yorkers, secretly rating our value as consumers, borrowers, and far more. Unlike traditional credit scores, New Yorkers currently lack any way to inspect and correct their ratings. New York must empower residents to understand and redress privacy violations.

Regrettably, our state has fallen behind more progressive states in ensuring personal privacy. California, for example, enacted the California Consumer Privacy Act (“CCPA”), giving consumers

---

1 JEFF DESJARDINS, *Here’s What the Big Tech Companies Know About You* (accessible online at: https://www.visualcapitalist.com/heres-what-the-big-tech-companies-know-about-you/).


6 *Id.*

7 *Id.*
the right to demand that businesses delete and/or export collected data. The CCPA also lets Californians opt-out from having their information resold to third parties.8

Overseas, the leading privacy protection is Europe’s Global Data Protection Regulation (GDPR) requires consumer consent for data processing, anonymization of collected data, the right to be forgotten, and data breach notification.9 Increasing numbers of jurisdictions are empowering individuals to control their information. It is high time that New York followed suit. There are no such informed consent regulations at the federal level. New York must fill in this gap to ensure that its residents understand what they sign. The average American would need almost 250 hours a year to read through all of their contracts.10 It should come as no surprise, therefore, that over 91% of Americans report consenting to legal terms without reading them.11 Yet even when consumers read these terms, they are written in a manner that vast majority of us could not decipher. Clearly, New York must do more to ensure that consent to data collection is not a legal fiction. Consumers need to clearly and easily understand how their data will be used and shared. New Yorkers’ must have the right to delete our data and ensure our information is never harvested without genuine consent.

**Government Surveillance**

The New York Privacy Act might revolutionize corporate data collection, but it fails to address the growing threat from local and state government surveillance. Ever cheaper, more powerful spy tools have enabled New York law enforcement agencies conduct warrantless, and even discriminatory, surveillance.12 While government surveillance is even more potent of a privacy threat than its commercial counterparts, the two are not wholly distinct. Police routinely turn to platforms like Facebook and Twitter to gather evidence, even turning Alexa and Google Home into their eyes and ears.

Some localities are fighting for reform, but statewide protections are needed. For example, the New York City Council is considering the Public Oversight of Surveillance Technology (“POST”) Act, requiring the New York Police Department (“NYPD”) to develop a public “Privacy and Use Policy” for every spy tool it deploys.13 The NYPD has built up an arsenal of cutting-edge, military-grade spy

---


10 DAVID BERREBY, *Click to agree with what? No one reads terms of service, studies confirm* (accessible online at: https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print).


tools without any public notice or debate. From x-ray vans that use ionizing radiation to see through walls, vehicles, and even clothing, to automated license plate readers that can monitor a vehicle’s location throughout the city, the NYPD’s Orwellian surveillance technology should disturb every New Yorkers.

The POST Act does not stop the NYPD from using these tools – no matter how problematic they might be – it merely creates an oversight mechanism against potential misuse. Far from being a way to undermine the NYPD, civilian surveillance oversight has enhanced trust in law enforcement in other cities.14 The New York City Council is particularly concerned with ensuring that New Yorkers’ private information is kept safe from federal agencies such as ICE. But there is only so much that any one locality can do. Statewide restrictions are needed if we are to ensure that New York’s police departments respect the fundamental privacy rights reaffirmed in the New York Privacy Act.

This hearing is a positive step towards ameliorating the privacy issues we face in New York. However, New York’s privacy reforms must not be delayed. Emerging technologies will only exacerbate the threats we already encounter on a daily basis. It is my hope that New York rises to the task at hand and curbs this problem before it is too late.

---

14 Oakland, California and Seattle, Washington have enacted similar police oversight laws without deteriorating public safety. See NEW YORK TIMES, San Francisco Banned Facial Recognition. New York Isn’t Even Close. (accessible online at: https://www.nytimes.com/2019/05/18/opinion/nypd-post-act-surveillance.html).