Statement of Jessica J. González

Vice President of Strategy & Senior Counsel
Free Press & Free Press Action

Before the

City of Long Beach
Technology and Innovation Commission

Regarding

Data Privacy and Surveillance

Delivered on

June 26, 2019

Thank you for inviting me to present Free Press Action's policy analyses on data privacy and surveillance.[1] I am Jessica González, Vice President of Strategy and Senior Counsel at Free Press Action, a non-partisan, non-profit organization with 1.4 million members across the U.S., and approximately 10,000 members in Long Beach. I live just a bit north of Long Beach, but my brother, sister-in-law and best friend are Long Beach residents and I love spending time in this city.

[1] I'd like to thank my Free Press Action colleagues Sandra Fulton and Matthew F. Wood for helping me prepare these remarks.

For those who are not familiar with Free Press Action, we are a national organization based in Washington, D.C. but we have five California-based staff members, and four of us are in the greater Los Angeles area. To ensure our independence, we take no money from corporations and governments.

Free Press Action believes that media and technology are essential to our democracy, and we fight to ensure that they are used for justice. We also strive to ensure that people have a voice in the decisions that shape our rights to connect and communicate.

These values drive our positions on data privacy and surveillance.

I understand that Long Beach collects data from sensors on the cities' vehicle fleet; body cameras worn by police; smart water meters; an array of mobile apps used by the public; license plate readers; social media monitoring; and countless other ways.

I also understand that in light of this trend, the Long Beach Department of Innovation has asked this Commission to draft a data privacy policy or, at least, to develop privacy principles. I applaud this wise step.

And I also know that Long Beach is a sanctuary city. While I certainly commend the city for stepping up protections for undocumented people, I'd suggest that Long Beach must expand its data privacy policies, and make sure they are enforceable too if it is serious about protecting its residents from the atrocities coming out of Washington. I'm afraid that principles alone will not suffice to protect undocumented people and others who are often unjustly targeted by federal, state and local law enforcement.

Too often, technology that on its face seems benign, or even useful, has been abused by state and private actors to the extreme detriment of people of color and immigrants. State use of some technologies is infringing on our privacy, civil liberties and civil rights right now.

So next I will go through a few popular surveillance technologies, describe some of the abuses we see happening with those technologies, and outline a set of solutions that the Technology and Innovation Commission may use to guide what I hope will be strong policy proposals to the mayor's office and the Long Beach City Council.

Police Body Cams

Many people initially supported body-worn cameras in hopes that they would provide transparency into some police interactions with community members, and help protect peoples' rights, especially in heavily policed communities of color.

But as Leadership Conference on Civil and Human Rights and Upturn documented in their 2017 scorecard, "accountability is not automatic. Whether these cameras make police more accountable — or simply intensify police surveillance of communities — depends on how the cameras and footage are used."

This scorecard evaluates the body-worn camera policies currently in place in major police departments across the country, and it measures Long Beach's performance against eight standards laid out in the Civil Rights Principles of Body Worn Cameras, to which Free Press is a signatory. It found that Long Beach meets one of its principles, to make department policy publicly and readily available; and partially meets two others, one for limiting officer discretion on when to record, and another for addressing personal privacy concerns. But the scorecard found that Long Beach falls short or is not clear enough with regard to the other five principles, which suggest prohibiting officer pre-report viewing, limiting retention of footage, protecting footage against tampering and misuse, making footage available to individuals filing complaints, and limiting biometric searching of footage.

The scorecard provides a much more detailed analysis of Long Beach's policies and I believe that you all have a copy, so I won't take your time reading it aloud here. But I would recommend a thorough read, and that this Commission recommend enforceable policies that hold local law enforcement accountable in all eight areas identified in the Civil Rights Principles of Body Worn Cameras. I'd highlight especially the need to adopt policies that compel footage to be released to the public, and that prevent police abuse and tampering.

Body worn cameras are a prime example of how the adoption of strong safeguards with a new technology can increase public accountability, but how without strong rules the technology can be weaponized and used against already over-surveilled populations.

Automated License Plate Readers ("ALPRs")

Several months ago an ACLU FOIA request revealed that ICE "is tracking and targeting immigrants through a massive [automated] license plate reader database [called Vigilant] supplied with data from local police departments — in some cases violating sanctuary laws." According to ACLU of Northern California, "[e]mails show local police handing driver information over to ICE informally, violating local law and ICE policies."

Vigilant draws this information from the fifty most populous places in the country, including the Los Angeles-Long Beach-Santa Ana metropolitan area. As of November 2018, it does not appear that Long Beach is handing over detection data to ICE, however Long Beach is sharing data with hundreds of other law enforcement agencies, which may in turn be sharing that information with ICE and other federal authorities. This practice is ill advised.

Indeed ICE notoriously employs "methods for circumventing both internal privacy rules and attempts by local law enforcement agencies to lock down their information."

In addition, massive databases like those created by ALPRs are simply ripe for abuse. In 2016, the AP uncovered that "police officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work."

Long Beach should give the public meaningful notice of the city's use of this technology and invite comment thereon, and then evaluate whether the benefits of using this technology truly outweigh the serious privacy threats. The city may want to consider banning license plate readers altogether once it studies the impacts on privacy and conducts a racial impact assessment, or, at a minimum, it should consider adopting strong data retention policies to significantly reduce the amount of time the city holds this data in its possession.

Facial Recognition Technologies

Facial recognition technology has been quickly adopted by law enforcement despite damning reports of inaccuracies and racial bias. A 2016 report by Georgetown Law Center found that facial recognition technology is racially biased,

especially against Black people. As my colleague Sandra Fulton explains, the "system is a network of various state and federal databases that are generally built of drivers' licenses and mug shots. These databases sweep up millions of innocent Americans without their knowledge and put them into what Georgetown calls the 'perpetual lineup.' It's the first time in our nation's history that the FBI has maintained a biometric database made up primarily of innocent people."

Even in the trusted hands, tracking people and retaining this information is dangerous. In the wrong hands, it could be deadly.

For instance, a 2018 analysis by the ACLU of Northern California found that Amazon's facial recognition software, which is called Rekognition, "incorrectly matched 28 members of Congress, identifying them as other people who have been arrested for a crime." Those members were Republican and Democratic, men and women, and all ages; but, critically, they were disproportionately people of color, including six members of the Congressional Black Caucus. In fact, "nearly 40% of Rekognition's false matchers … were of people of color even though they make up only 20% of Congress."

In a time where Democrats and Republicans agree on very little in Washington, recent Congressional hearings have shown bi-partisan support for a moratorium on the use of facial recognition technology until we have a better grasp on the privacy implications.

With this host of ethical issues in play, it's no wonder that San Francisco voted to ban facial recognition technology by local law enforcement, and that the California Assembly recently passed AB 1215, the Body Camera Accountability Act.

In 2017 the Office of the Chief of Police for the Long Beach Police Department, in response to a FOIA request, stated that Long Beach did not use facial recognition technologies at that time, yet somehow six people had been identified using such technologies.

We'd suggest a moratorium on adoption of facial recognition technologies unless the city can show that they will not disproportionately harm people of color and immigrants, and that they will not violate people's privacy rights.

Solutions and Policy Proposals

Beyond the solutions and policy proposals I mentioned earlier in covering the types of privacy vulnerabilities that we've studied most, Free Press Action also has nine general recommendations on best practices for governments that want to respect the privacy rights of their residents. One guiding principle for all of them is that communities should pass ordinances to require transparency, oversight, and approval whenever a police department considers purchasing surveillance technology.

The first recommendation is transparency. Be as transparent and accessible as possible when describing technologies and privacy policies the city has already adopted and that it is considering.

The second is to allow the public to comment both on policies and technologies already adopted and being considered. Make sure that comment process is truly accessible to all, and that the public has enough time and a meaningful opportunity to participate.

The third is that the city must conduct outreach to the most impacted communities to ensure their perspectives are heard.

The fourth is to conduct privacy impact assessments and racial impact assessments before adopting any new surveillance technologies or data privacy practices and policies. The city should take a good look at who is the most surveilled, and why. It may want to create a local board with community members and people from the most impacted communities to assist in the privacy impact assessment.

The fifth is that Long Beach should abandon any efforts at predictive policing. The impacts of algorithmic bias in this space are too severe, and cannot be overcome with any quick fixes.

The sixth is that Long Beach should minimize the amount of data it keeps on its residents and community, and retain as little of this data as it possibly can. The less data you hold onto about your community, the safer it will be from ICE and outside law enforcement agencies that could use the data for purposes that go against Long Beach's values.

Seventh, the city should exercise strong oversight of its law enforcement personnel.

Eighth, when in doubt, require a warrant for local law enforcement to collect data about people in the Long Beach community.

Finally, the city should place a moratorium on adopting new technologies unless it can show that use of such technologies would not violate peoples' privacy rights and would not have a disparate impact on people of color and immigrants.

Lastly, I'd be remiss not to mention the Community Control Over Police Surveillance – Guiding Principles that ACLU put forth in coalition with Council on Islamic Relations, Million Hoodies Movement for Justice, NAACP and over a dozen other civil rights organizations. They provide model legislation that is being considered in cities across the U.S. Six California cities and the BART system have adopted that model already, and it is moving through the California legislature. The principles considered an array of technologies, including stingrays, automatic license plate readers, electronic toll readers (or EZ Pass), closed circuit TV, biometric surveillance technology, gunshot detection and location hardware and services, X-ray vans, surveillance-enabled light bulbs, hacking software and hardware, social media monitoring software, through the wall censors and radar, body cams, and predictive policing software.

Thanks again for inviting me here today, and I welcome your questions.