Slate

The Fragmented Surveillance State

Andrew Guthrie Ferguson

November 10, 2017

In Chicago, **every person arrested** over the past four years has received an algorithmically generated “threat” score (from 1-500) to determine his or her risk of being a perpetrator or victim of a future crime. Those individuals with the highest scores on the Chicago Police Department “**heat list**” get extra attention in the form of home visits or increased community surveillance.

In Baltimore, for months **Cessna planes equipped with wide-angle video cameras** capable of filming entire segments of the city flew overhead. A private security company—**Persistent Surveillance Systems**—connected its aerial video with ongoing police reports and handed the footage over to the Baltimore Police Department to assist in investigating past crimes. Using the surveillance video, one could literally map the comings and goings of everyone—criminals and innocents alike. The only problem was that **no one had informed** the Baltimore City Council or the mayor of this arrangement.

The Los Angeles Police Department—**in partnership** with the private technology firm Palantir—is currently mapping criminal associates and gangs using new **social network technologies**. Data about targets and their associates, families, and friends are fed into a growing police investigative database. These social network systems, which target “chronic offenders,” **also include information about innocent associates**, family members, and friends, creating extensive human maps of connections and patterns of contacts.

Big data policing means that new privacy-invading technologies are now a local problem. Instead of one frightening big brother surveillance state, the reality is really more like thousands of little sisters and brothers (and cousins) all reporting fragmentary bits of bad behavior. The result may be no less oppressive, but the solutions to challenge this growing privacy threat are far more difficult. After all, there are almost **17,000 different law enforcement agencies** in the United States, including federal, state, and municipal police departments.

From one perspective, these new surveillance technologies offer breakthrough policing capabilities. Predictive analytics promises new measures of efficiency, allowing police departments to do more with less and target only those most worthy of police attention. If you really could predict the most violent members of your community and effectively intervene, it would offer a proactive **public health** approach to violence reduction. Similarly, automated and extensive surveillance systems give police a proverbial **time machine**, allowing them to go back in time to watch and investigate any crime that takes place in public.

At the same time, these technologies challenge traditional conceptions of privacy and raise issues of racial bias. Mass surveillance systems capture not just crimes, but the privacies of life: Where you go, whom you associate with, and the patterns of your daily interactions can be recorded and mapped. Predictive targeting affects individuals based on educated guesses of future criminal involvement, not current proof of criminal activity. If the **inputs** that go into this prediction model include data that can be subject to human bias (like **police discretion in arrests**), then the **outputs will reflect that biased data**. This noise can both distort the accuracy of the forecasts and undermine the fairness of a legal system based on such data.

Faced with a choice between security and privacy, society may choose to adopt new big data policing technologies. Or, like in Baltimore when citizens found out about the aerial Persistent Surveillance Systems, they rejected the technology as too intrusive.

But, right now society is not even having that debate. Ask yourself two very basic questions: What police surveillance technologies are currently being used in your home town? If you are unsure of the answer, where would you go to find out? Both turn out to be remarkably hard to answer, which reveals the democracy deficit at the heart of big data policing.

Unless you live in the few localities that require civilian oversight over new police technologies like **Somerville, Massachusetts**, or **Santa Clara, California**, you don’t know which surveillance technologies police are using in your community. Unless you are engaged with organizations like the **American Civil Liberties Union**, the **Electronic Frontier Foundation**, the **Center for Democracy and Technology**, Impact Justice’s **Justice Data Accountability Project**, the **Policing Project**, or the **Cato Institute**—organizations that advocate around this issue—you don’t even have a place to take a stand against local surveillance.

This is a democracy problem, and one compounded by the fragmented nature of localized policing. In **New York City**, **Oakland**, **Seattle**, and other big cities, local governments have begun debating similar oversight systems. But it is a debate that everyone must join. Critical liberty and accountability issues are at stake in big data policing, and the conversation needs to be had before, not after, these technologies are implemented in your neighborhood. It may be the case that citizens *are* comfortable with their activities being surveilled, but the question should be put them in an open and transparent forum.

So how do we even begin to reclaim local control over police surveillance in a fragmented world? First, we need people to ask the most basic of questions about what surveillance technologies are being purchased with tax dollars and why. Questions of public safety require public comment and oversight. Second, we need to create a space to demand accountability from local leaders. At some point in the fiscal year, local officials should have to explain their technology purchases and policies to the community. Even scheduling the accountability moment will force elected leaders to think through the policies and potential risks of new surveillance technologies. Third, citizens have to invite outside experts, technologists, civil libertarians, data scientists, lawyers, academic institutions, and the larger community into the conversation. To understand a “black box technology” may require experts skilled in decoding complex algorithms and advocates informed about the intricacies of legal code. This is exactly the type of effort led by the ACLU’s **Community Control Over Police Surveillance** project and can be replicated city by city, state by state.

Though that’s a pretty simple how-to guide—implementing it, of course, is much harder. But we have to start somewhere, so why not in your town?