Oakland Poised to Lead in Protecting Privacy

The city council is on the verge of implementing significant citywide reforms aimed at protecting the privacy of its residents, including a first-of-its-kind surveillance equipment ordinance.

By Brian Hofer and the Oakland Privacy Working Group

On February 10, the Oakland City Council's Public Safety Committee is poised to vote on a handful of recommendations that, if implemented later by the full council, will significantly protect the right to privacy for city residents in this age of Big Data. Councilmembers will consider a privacy and data retention policy for the scaled-back Port Domain Awareness Center (DAC), drafted by a council-appointed citizens' committee.

The citizens' committee is also asking the council to establish a new permanent committee to advise the council on broad privacy-and data-related matters, including a citywide privacy policy, modifications to an existing whistleblower ordinance, and a first-of-its-kind surveillance equipment ordinance. If adopted, the recommendations would ensure that there is a public debate on privacy issues before the council approves future surveillance projects. In addition, the citizens' committee has built requirements into the proposed policy that mandate that the effectiveness of surveillance tools be reported publicly and undergo independent audits. The policy also requires ongoing oversight and penalties for abuse in order to ensure that the tools are used properly.

The lengthy and boisterous city council meetings in February and March 2014 led to the beginning of a meaningful discussion between the city and community regarding surveillance and the impact to privacy caused by use of new law enforcement tools. The remarkable willingness by elected officials and project proponents to sit down with opponents and discuss issues in a good-faith substantive manner is a silver lining to this controversial topic.

Taken as a whole, the implementation of the committee's recommendations would make Oakland the national leader in protecting the privacy rights of its citizens. Other cities are pursuing a similar path. Seattle has created a permanent privacy committee and also adopted a surveillance equipment ordinance. Seattle adopted the ordinance after citizens discovered — three years after the fact — that their police department had purchased drones.

Menlo Park recently adopted an ordinance that regulates the use of automated license plate readers. San Francisco Supervisor John Avalos and Santa Clara County Supervisor Joe Simitian are working with the ACLU to introduce in their jurisdictions the same type of surveillance equipment ordinance we hope to introduce here. On November 23, 2014, the editorial board of the *Los Angeles Times* endorsed the ACLU's ordinance, stating: "The ACLU's approach to vetting new technologies is so pragmatic that cities, counties, and law enforcement agencies throughout California would be foolish not to embrace it."

Here in Oakland, we have no citywide privacy policy; no privacy or data-retention policies for the use of automated license plate readers; and no policy concerning the Oakland Police Department's cellphone tower-mimicking Stingray devices, a system so controversial that police agencies across the nation actively conceal its use from courts and defense attorneys, going so far as to dismiss charges at trial rather than reveal the technology (see "Judge threatens detective with contempt," *Baltimore Sun*, November 17, 2014).

A Stingray tricks all cellphones within range into thinking it's a cell tower, intercepting call information, phone contact logs, and text messages. When OPD activates a Stingray at 14th and Broadway during a political protest, hundreds of attorney-client privileged communications around City Center are at risk of being intercepted because a Stingray can only operate in a dragnet fashion — it sucks up every cellphone's data, penetrating law firm walls and the halls of City Hall in the process. Stated simply, it cannot operate without violating the Fourth Amendment rights of all cellphone users because it cannot be targeted to the one phone number for which OPD might have obtained a warrant.

In addition, the "chilling effect" of mass surveillance is already taking a toll. In 2014, the PEN American Center surveyed writers in fifty nations, finding that many writers living in so-called free countries say they sometimes avoid controversial topics out of fear of government surveillance, and are self-censoring at levels near those in repressed nations. This is the harm — not that bad guys are caught using new shiny gadgets — but that lawful activities are reduced because of surveillance.

The use of Oakland's surveillance equipment is not independently audited, and neither the purchase of the Stingrays nor their use has ever been knowingly approved by the council. In addition, information about the cost effectiveness, success, and ramifications of misuse of these tools is rarely, if ever, publicly presented to the council and public to judge the appropriateness of continued use. It is this lack of process that led to the DAC protests earlier this year and that we hope to correct now by installing the same framework in both the DAC privacy policy and the surveillance equipment ordinance. This is the Oakland success story — that we are now having these conversations.

In November, Menlo Park presented its first transparency report on automated license plate readers, and it concluded that only one stolen vehicle had been recovered even though police had tracked the license plates of 263,430 vehicles. Similarly, our city auditor's February 2014 report revealed that Oakland's ShotSpotter surveillance audio recordings had resulted in only 0.09 percent of total arrests in calendar year 2013. In this era of budget cuts, there is an argument to be made as to the lack of efficacy regarding these surveillance tools and whether they are worth the infringement on peoples' right to privacy. In fact, cities throughout the nation have decided to not renew surveillance contracts with private companies after examining hard data about their lack of effectiveness. What is most important is that the public should also get to decide on the appropriateness of these tools. The Oakland citizens' committee's recommendations will achieve that goal.

Last week, the city administrator's report regarding the citizens' committee's work was posted online and it contained an unexpected revelation: The Port of Oakland will not be paying its share, and has decided to redirect the grant funds that were to finance the first two years of operating costs at the DAC and use them instead for other port projects. I cautioned the council at the March 4, 2014 meeting that this could happen — comments echoed by

Councilmember Rebecca Kaplan. Former Councilmember Wilson Riles Jr. made it even more pointed, sharing his experiences from his days in office when this so-called free technology, via grants, ends up on the Oakland taxpayer's tab. Regardless of whether this revelation keeps the DAC permanently dark or not, the privacy conversation with the city must continue.

With the adoption of these recommendations as written, the Oakland City Council can show that it's earnest about protecting its citizens' privacy rights. By supporting their full implementation, city staff members and law enforcement officials can demonstrate that they intend to earn the community's trust by operating within the rules. As the *Los Angeles Times* editorialized, "trust us is not enough."

Contact the author of this piece, send a letter to the editor, like us on Facebook, or follow us on Twitter.

« How Fracking Changes Everythin… The Case for Banning Monsanto'… »