LOCAL POLICE SURVEILLANCE TECHNOLOGY

THE PROBLEM

As the capabilities of surveillance technologies continue to advance, so does law enforcement's ability to monitor civilians' movements, communications, and ideas. Today, these technologies enable local police to trick a cell phone into providing them with the user's location. They can monitor where drivers and pedestrians travel in public using license plate readers and close circuit television cameras. They can intercept text messages unbeknownst to their senders or recipients. They can even be alerted when somebody posts a hashtag like #BlackLivesMatter on Twitter or Facebook. These measures, some of which are of questionable legality, are happening with far too little public knowledge or governmental oversight.

This growing surveillance impacts everybody, but has disproportionate impact on people of color, certain religions (particularly Muslims), and people who are politically active.[1] How do we know this? Despite the efforts of police to keep the use of surveillance technologies a secret, when advocates have periodically been able to peer behind that veil of secrecy, they have discovered these technologies are frequently deployed in a discriminatory manner. This proved to be the case in cities like **Baltimore, MD, Lansing, MI, Milwaukee, WI, Oakland, CA,** and **Tallahassee, FL**, where various surveillance technologies were overwhelmingly focused on communities of color.

The policies of the Trump Administration have exacerbated the threat presented by the local use of surveillance technologies.[2] President Trump has made it very clear, in both words and deeds, that his administration is hostile towards undocumented immigrants, Muslims, and other vulnerable communities. Because federal law enforcement does not have enough personnel to monitor the millions of persons belonging to these groups, the Trump Administration needs the help of local law enforcement to fully pursue his agenda. While some local police forces have refused to help federal law enforcement agencies, even in those cities, that may not be enough to stymie the Trump Administration's efforts. By continuing the Obama Administration's expansion of programs that fund local police purchases of surveillance technologies, and making those grants contingent on local police sharing their data directly with the federal government or other government entities that share data with the feds, the current Administration can gain the passive assistance it needs from local law enforcement to more effectively target those communities. This is precisely the loophole U.S. Immigration and Customs Enforcement (ICE) used to obtain Oakland, California's automatic license plate reader data even though Oakland is a sanctuary city. As long as local police continue to have the authority to approve such agreements in secret, they are likely to do so.

The problem, in short, is that local police are increasingly using surveillance technologies to invade privacy, undermine civil rights and civil liberties, and target vulnerable communities. Because in most cities, decisions about funding, acquiring, and using surveillance technologies are exclusively made by local law enforcement in secret, the public and their elected officials neither know what surveillance technologies are being used nor have the ability to restrict or prohibit their use. That must change.

THE SOLUTION

In the fall of 2016, a coalition of sixteen politically diverse organizations, including the ACLU and the Center for Popular Democracy, launched the Community Control Over Police Surveillance (CCOPS) effort. The effort is based upon eight guiding principles:

- Surveillance technologies should not be funded, acquired, or used without express city council approval;
- Local communities should play a significant and meaningful role in determining if and how surveillance technologies are funded, acquired, or used;
- The process for considering the use of surveillance technologies should be transparent and well-informed;
- The use of surveillance technologies should not be approved generally – approvals, if provided, should be for specific technologies and specific, limited uses;
- Surveillance technologies should not be funded, acquired, or used without addressing their potential impact on civil rights and civil liberties;
- Surveillance technologies should not be funded, acquired, or used without considering their financial impact;
- To verify legal compliance, surveillance technology use and deployment data should be reported publically on an annual basis; and
- City council approval should be required for all surveillance technologies and uses – there should be no "grandfathering" for technologies currently in use.

To achieve these objectives, the CCOPS effort is promoting the adoption of model legislation[3] by city councils across the nation. As of summer 2017, CCOPS-type laws have already been adopted in **Seattle**[4], **Nashville**[5], and **Santa Clara County**[6], California (home of Silicon Valley). Bills have been introduced, or on the verge of being introduced by an identified sponsor, in 16 additional cities[7] (plus two states[8]). Grassroots efforts to identify a sponsor who will introduce a CCOPS bill are underway in more than 40 additional cities. If adopted, CCOPS laws will create an open, transparent process for the approval – or rejection – of local surveillance technologies. Moreover, as part of the process of seeking approval, law enforcement will need to provide the public and their elected officials with detailed information regarding how the surveillance technology works, how it will be deployed and for what purposes, what the potential adverse impacts on civil rights and liberties are, and how those potential adverse impacts will be avoided.

Where CCOPS bills become law, local law enforcement will no longer be able to acquire surveillance technologies without an open, public hearing and city council approval. Likewise, police departments will not be able to use that technology in a manner that has not been approved by the city council, nor will they be able to share access to or data from those technologies with the federal government or any other entity without city council approval. Given these objectives, it is fair to say CCOPS is as much about promoting government transparency as it is about empowering the public and their elected officials to make informed decisions about the use of surveillance technologies.

Elected officials and organizations wishing to start or join a CCOPS effort in their city should visit the CCOPS website (see details below). They can also contact the ACLU for further information and assistance at CCOPS@ACLU.org.

ADDITIONAL RESOURCES

To learn more about the CCOPS effort, and to access CCOPS advocacy resources, visit the CCOPS website at www.CommunityCTRL.com.

To download a version of the CCOPS model city council legislation, see "An Act to Promote Transparency and Protect Civil Rights and Civil Liberties with Respect to Surveillance Technology". ACLU. January 2017.

To download the fourteen-organization CCOPS' Guiding Principles document, see "Community Control Over Police Surveillance – Guiding Principles." ACLU.

For a primer on the various surveillance technologies being used by local police, "Community Control Over Police Surveillance: Technology 101." ACLU.

Co-authored by the American Civil Liberties Union