DAY ONE PROJECT

Democratizing Police Adoption of Surveillance Technology

Catherine Crump

January 2021

Summary

The next administration should help local communities reassert control over police use of surveillance technology. It should support legislation requiring that the use of all federally-funded surveillance technology be approved by local elected representatives through a public process, and that this use be constrained by a formal policy delineating the situations in which it will be used, how the data it generates will be handled and secured, and how its effectiveness will be evaluated. If new legislation is not forthcoming, then the next administration should empower local initiatives through a pledge program in which leading local law enforcement authorities voluntarily agree to take these steps.

Today local law enforcement agencies obtain cutting edge—and potentially intrusive—surveillance equipment without the knowledge of elected leaders and the general public, sometimes leading to a rejection of the technology once the public discovers it. In Oakland, for example, following a council review that lasted only two minutes, the city created a data integration center that networked together all of its existing surveillance infrastructure. Once the public learned of the center, protests broke out and council meetings were flooded with angry residents. The backlash was so severe that the city ultimately largely gutted the center, even though millions in federal funding had already been spent on its development.[1]

Federal funding is a major driver of uninformed and undemocratic adoption of surveillance technology at the local level. The Federal Government funds billions of dollars in grants to local law enforcement agencies, money that can then be used to purchase surveillance equipment.[2] But the government does not take steps to ensure that local elected representatives and members of the public are involved in decisions about what technologies are acquired, or that protocols are developed to constrain how the technologies are used.

The Federal Government has a responsibility to intercede to make sure that local elected representatives are aware of and have control over how federally-funded surveillance equipment is used in their communities. Transparency is particularly important for surveillance technology because this equipment is often invisible. People cannot challenge deployment of surveillance technology in court or through public processes if they do not know about it. Moreover, surveillance technologies can be invasive, with potentially harmful effects on civil rights and liberties. Particularly given today's high level of concern over policing practices, the Federal Government should not be undermining the ability of local communities to assert democratic control over their police departments.

---

[1] Ali Winston, "Oakland City Council Rolls Back the Domain Awareness Center," East Bay Express, March 5, 2014, https://www.eastbayexpress.com/SevenDays/archives/2014/03/05/oakland-city-council-rolls-back-the-dac.

[2] See, e.g., Federal Emergency Management Agency, FEMA Preparedness Grants Manual (2020), https://www.fema.gov/sites/default/files/2020-06/fema_preparedness-grants-manual.pdf (describing FEMA's responsibility for administering many grant programs to state, local, and tribal governments, and detailing the purposes for which these grants can be used, including the acquisition of surveillance equipment).

Some cities and counties have passed ordinances requiring that their law enforcement agencies seek approval to deploy surveillance technology, demonstrating the feasibility and desirability of such measures.[3] But with some 18,000 law enforcement agencies nationwide, only the Federal Government can implement a solution at scale.[4]

Challenge and Opportunity

With the rise of the Black Lives Matter movement, police practices are now under intense scrutiny. The public has a rare appetite for reform—this summer, a whopping 94% of Americans said reforms are needed to make policing better.[5] While much attention rightly is focused on police use of excessive force, we should not forget a less visible but nonetheless pernicious issue: police use of powerful surveillance technologies in ways that are unaccountable to the public. There is real congressional interest in regulating law enforcement deployment of surveillance technology.[6] The time to act is now.

Examples abound.[7] In Seattle, the police obtained a surveillance drone with the approval of a city council that did not realize what it was doing. In San Diego, elected representatives were only dimly aware that the law enforcement agency they supervised had built and deployed innovative facial recognition technology. As discussed above, in Oakland, a federally-funded surveillance center was largely abandoned—after millions had been spent.

Who paid for Seattle's drone, San Diego's facial recognition technology, and Oakland's data integration center? In each case, the Federal Government was the funder.

In fact, the Federal Government's primary role in policing—and its primary source of leverage—is as a *funder* of policing strategies and policing technologies. Since September 11, 2001, the Federal Government has made billions of dollars available to provide equipment and training to state and local law enforcement agencies, including for surveillance.[8]

---

[3] Mailyn Fidler, "Fourteen Places Have Passed Local Surveillance Laws. Here's How They're Doing," Lawfare, September 3, 2020, https://www.lawfareblog.com/fourteen-places-have-passed-local-surveillance-laws-heres-how-theyre-doing.

[4] U.S. Department of Justice, Bureau of Justice Statistics, National Sources of Law Enforcement Employment Data (Apr. 2016 revised Oct. 2016), https://www.bjs.gov/content/pub/pdf/nsleed.pdf.

[5] Steve Crabtree, "Most Americans Say Policing Needs 'Major Changes,'" Gallup, July 22, 2020, https://news.gallup.com/poll/315962/americans-say-policing-needs-major-changes.aspx.

[6] See, e.g., H.R.7356 - Facial Recognition and Biometric Technology Moratorium Act of 2020, https://www.congress.gov/bill/116th-congress/house-bill/7356/cosponsors?r=7&s=1&searchResultViewType=expanded.

[7] These examples are discussed in detail in Catherine Crump, "Surveillance Policy Making by Procurement," Washington Law Review 91, no. 4 (2016): 1595.

[8] For a detailed breakdown of funding totals by agency and program, see Crump, "Surveillance Policy Making by Procurement," 1601-02.

Despite being such a major funder, the Federal Government does not require local law enforcement agencies receiving funding to disclose to local elected representatives what surveillance technologies they are acquiring, let alone to seek permission for their use.

This is a problem. Surveillance technology has the potential to enhance public safety, but it also poses risks to privacy and other civil liberties and rights. We depend on local officials to set policies for policing in their communities. Local communities vary greatly in their crime rates, the competence and trustworthiness of their police departments, and their political convictions. Local governments have a valuable role to play in tailoring surveillance policy to local conditions. The Federal Government should not undercut them.

There is a straightforward solution. As a condition of receiving funding, the Federal Government should require that law enforcement agencies seeking funding demonstrate that local elected leaders have formally approved use of the surveillance technology through a public process. It should also require approval of a formal policy delineating the situations in which it will be used, how the data it generates will be handled and secured, and how its effectiveness will be evaluated.

Plan of Action

I propose that the Biden-Harris administration support legislation, or else develop a pledge program, with the following elements:

- *First*, the Federal Government should only fund surveillance technology when local elected representatives have **approved** its acquisition through a **public process**.
- *Second*, to help local elected representatives make informed decisions about the acquisition of surveillance technology, the Federal Government should require law enforcement agencies seeking grants to prepare an **impact assessment**. The impact assessment should address the potential benefits to public safety but also the consequences for civil rights and liberties. It should be presented to local elected representatives prior to the request for them to approve surveillance technology acquisition.
- *Third*, the Federal Government should only fund surveillance technology when the law enforcement agency has drafted, and elected representatives have approved, **a formal policy constraining the use of the technology**. It should specify when the technology will be used, how data will be handled and secured, and how its effectiveness will be evaluated.

Federal legislation is the clearest way to proceed with implementing these requirements. It is possible, however, that, for certain grant programs, Congress has granted enough discretion in

implementation to the executive that it could implement these requirements by acting on its own.[9] If neither of these approaches is feasible, the Biden-Harris administration should support a voluntary pledge program in which law enforcement leaders publicly commit to take these steps.

Each of these elements is important. It is important that local elected leaders approve the use of surveillance technology because its deployment often involves trade-offs between values such as public safety, civil rights, and civil liberties. Elected representatives are better positioned to make these types of policy decisions, aided by public input, than law enforcement agencies acting on their own.

It is also important that elected representatives be guided by impact assessments because these assessments will make those decisions more informed. Law enforcement agencies should draft them because they are most familiar with their justifications for seeking to acquire specific technologies, as well as their relevant technical features. Impact assessment will help elected leaders understand the need for the technology, why non-tech alternatives may be inadequate, and what the potential consequences for civil rights and liberties might be. Requiring an impact assessment is reasonable and workable. The Federal Government already requires all federal agencies to conduct privacy impact assessments "for all new or substantially changed technology that collects, maintains or disseminates personally identifiable information."[10] New York City recently passed an Act requiring the New York Police Department to develop surveillance impact and use policies for surveillance technology. [11] Smaller municipalities have done so as well. [12]

Finally, it is important that use of surveillance technology be constrained by formal policies so that it is used to address valuable law enforcement ends without overly burdening civil rights and liberties, so that sensitive data about individuals is not kept longer than necessary to advance the stated purposes of using the technology, and so that the public has a way to know how the technology functioned in practice so changes can be made if necessary.

The new administration would not need to create a proposal from scratch. Although acting at the federal level would be new, more than a dozen localities have already imposed these types of requirements on the law enforcement agencies reporting to them, which means that there are road-tested models ready to be adopted nationwide.[13] Generally speaking, these ordinances instruct local government agencies about what they need to do before acquiring surveillance technology in their jurisdictions. The ordinances then define the steps local authorities must take

[9] Please contact the author if there is interest in exploring this possibility further.
[10] "Privacy Impact Assessments," National Archives, accessed September 21, 2016, http://archives.gov/privacy/privacy-impact-assessments/index.html [https://perma.cc/P84U-U2U4].
[11] New York City, New York, Administrative Code § 14-188(a) (2020).
[12] Yellow Springs, Ohio, Municipal Code § 607.02(d) (2018).
[13] Fidler, "Passed Local Surveillance Laws."

to prepare policies that dictate the use of the surveillance technologies once acquired and how the public and elected bodies will be able to periodically review how the acquired technology is being used.

Conclusion

Today local police departments have powerful surveillance technologies available to them. Police departments should not decide whether and how to deploy them without democratic input. The Federal Government should ensure that its grant programs do not have this unintended effect. Requiring that local law enforcement agencies seeking federal funds for surveillance technology have the approval of local elected representatives is a sensible, achievable remedy. It is also one that should win bipartisan support. Fundamentally, this proposal is not for or against surveillance technology. It is about ensuring that elected leaders and affected communities have input into policy decisions. That is a principle everyone should be able to get behind.

Frequently Asked Questions

1. Shouldn't the Federal Government focus on fixing federal surveillance rather than state and local surveillance?

No. There are 18,000 law enforcement agencies in the United States and almost all of them are state and local agencies. People are far more likely to interact with a local police officer than they are to meet an FBI agent. The Federal Government funds a significant amount of surveillance at the state and local levels, for the specific purpose of promoting more surveillance. It should at the least ensure that it doesn't undermine local democratic control of policing in the process.

2. Isn't this just a massive paperwork requirement? Shouldn't the Federal Government instead set limits on when federally funded surveillance technology should be used?

No. Local communities vary significantly. Some have competent police departments that are generally trusted. Some have notoriously backwards departments that have, e.g., been under court supervision for years. Not every community will have the same views about whether powerful surveillance technology should be deployed. The purpose here is to make sure federal funding doesn't undermine the primary source of democratic control over policing, which is local control.

3. Why is federal legislation specifically, as opposed to some other form of federal-level reform, necessary?

My conversations with former administration members indicate that because existing statutes authorizing federal grant programs do not mandate that local democratically-elected officials sign off on surveillance technology acquired using federal funds, there would, in many cases, be no source of authority for agency employees to enforce such a requirement.

4. In what ways can technology negatively impact rights?

The Fourth Amendment to the U.S. Constitution protects against unreasonable searches, which includes many forms of surveillance. People have a right to privacy, which typically has included being able to go out in public in relative anonymity. People do not expect the government to monitor their movements every time they leave their houses. Communities should have some say about whether mass surveillance technologies such as license plate readers are used in their communities.

Furthermore, some settings are particularly sensitive. People have a First Amendment right to engage in political protest, for example. When the government deploys surveillance technology to identify and monitor peaceful protesters, that can chill people's ability to exercise their First Amendment rights by making them uncomfortable expressing their views.

5. Can't we count on courts to protect people's rights?

Not when it comes to deployment of surveillance technology. The deployment of surveillance technology is often invisible, and it is of course impossible for people to challenge surveillance if they don't know that it's occurring. That's why transparency measures such as this one are particularly important for surveillance.

About the Author

Catherine Crump is a clinical professor at UC Berkeley, School of Law, where she directs the Samuelson Clinic for Law, Technology & Public Policy. An expert on legal issues relevant to government deployment of police surveillance technology, she has testified before Congress and the European Parliament about related policy issues and litigated constitutional challenges to government surveillance in federal district and appellate courts.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit **dayoneproject.org**.