Cato Handbook *for* Policymakers

8TH EDITION

CATO INSTITUTE

19. Technology and Law Enforcement

Congress should

- ensure that all federal law enforcement grants are conditioned on policies that protect privacy and promote transparency and accountability;
- impose a probable cause requirement on the collection of metadata through cell phone tracking devices used by federal law enforcement agencies, including joint federal/state task forces; and
- direct the FBI and the FCC to rescind the nondisclosure agreements and secrecy policies that federal agencies negotiate with state and local law enforcement partners regarding cell phone tracking devices, or stingrays.

Since the beginning of modern policing in 1829, law enforcement agencies have taken advantage of new technologies. As automobiles, cameras, Tasers, radios, airplanes, and eavesdropping devices arrived, police were quick to put the new technology into the field. However, recent developments in surveillance technology, combined with a lagging Fourth Amendment jurisprudence, have jeopardized the constitutional rights of millions of American citizens without adequate legislative oversight. Modern technology gives police access to tools such as body cameras, drones, and cell phone tracking devices that could, without appropriate regulations in place, allow for the warrantless and persistent surveillance of entire American cities.

Law enforcement agencies have a legitimate interest in the use of body cameras, drones, and cellular phone trackers, but that interest must be weighed against the privacy interests and constitutional rights of American citizens. Our system of checks and balances obligates legislators and judges

to ensure that law enforcement practices respect the rights of the American people.

While law enforcement is traditionally a state and local function in our federal system, over the last few decades the federal government has increasingly injected itself into local law enforcement through the proliferation of grant awards and equipment transfer programs. Ostensibly meant to help fight the drug war and the War on Terror, these federal interventions in local law enforcement serve to distort law enforcement priorities while granting the federal government a massive role in shaping law enforcement policy at the state and local level.

Congress should consider the policies outlined below, which would allow law enforcement agencies to take advantage of new technology while also increasing law enforcement accountability and transparency and guarding against persistent and indiscriminate surveillance.

Cell Phone Tracking

Cell phone trackers are colloquially referred to by the Harris Corporation trade name "StingRay" or the technical term "IMSI-catchers" (i.e., the International Mobile Subscriber Identity of nearby mobile phones). These devices operate by emitting radio signals and are regulated under the authority of the Federal Communications Commission (FCC). The FCC, in turn, requires state and local law enforcement agencies to coordinate their acquisition of stingrays with the Federal Bureau of Investigation (FBI). Pursuant to that requirement, the FBI has proffered a nondisclosure agreement to state and local agencies applying to use stingrays. Among other things, the nondisclosure agreement forbids the law enforcement agencies from disclosing any information about the use or capabilities of the technology to the public, courts, or defendants. The agreement even gives the FBI the authority to compel local prosecutors to withhold evidence or even drop entire prosecutions rather than disclose stingray evidence.

For example, a judge in New York State ordered the Erie County sheriff's office to disclose the terms of its nondisclosure agreement with the FBI. The agreement included the following provision:

> In addition, the Erie County Sheriff's Office will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (beyond the evidentiary results obtained through the use of the equipment/technology), if using or provid-

ing such information would potentially or actually compromise the equipment/technology.

The federal government's demand for such extensive secrecy threatens privacy rights and undermines important federalism and separation of powers principles. Congress should direct the FBI and FCC to abolish such requirements for state and local stingray use.

The level of secrecy surrounding stingrays has made it difficult for courts to oversee the operation of the devices. With prosecutors, at the behest of the FBI, dropping cases rather than acknowledging stingray use, the jurisprudence is relatively sparse—despite the thousands of stingray deployments around the country. In the last year, however, the use of stingrays has garnered more attention from defense attorneys, courts, and legislators.

A Maryland state appeals court recently found that a warrantless use of stingray equipment to track down an attempted murder suspect was a violation of the Fourth Amendment. The court concluded that the suspect had a reasonable expectation of privacy in the location of his cell phone within an apartment. The federal Second Circuit Court of Appeals recently reached the same conclusion about another warrantless stingray search of an apartment.

Rather than wait for the courts, several state legislatures have taken steps to prevent stingray abuses by state and local law enforcement. Illinois, for instance, recently passed the Citizen Privacy Protection Act, which requires a showing of probable cause before a court will authorize the deployment of a stingray device. Congress should do the same and impose a warrant requirement on the collection of telephony metadata or digital content by stingray technology.

Body Cameras

The body camera, another tool that raises federalist concerns, has become an increasingly prominent hallmark of criminal justice reform debates. Overwhelmingly popular among the public and used by an increasing number of police departments, body cameras can help improve evidence gathering as well as accountability and transparency in law enforcement. In December 2014, a month after it was announced that Ferguson, Missouri, police officer Darren Wilson would not face charges over the killing of Michael Brown, the Obama administration proposed 50 percent matching funds for the purchase of 50,000 police body cameras.

In 2015, the Department of Justice announced that more than $23.2 million worth of body camera funds would be awarded to police departments in 32 states. Body camera funds worth more than $20 million were also awarded to 106 law enforcement agencies in 32 states and Puerto Rico in 2016. It's not surprising that the federal government has awarded body camera funds. In the wake of Brown's killing, there were renewed discussions about police use-of-force and police interactions with the communities they serve. The deaths of Alton Sterling, Samuel DuBose, Walter Scott, five Dallas police officers, and many others have maintained the urgency of these discussions. But while body cameras are popular, it's important to note that they can be expensive; federal grants will appeal to departments that otherwise would struggle with the fiscal impact of a body camera program.

Drones

Unmanned aerial vehicles (UAVs), commonly called "drones," vary considerably in size and capability and are used to collect video data. Unlike body camera programs, which do not require federal permission to use, drones are already regulated by the federal government. Police departments and other public entities can fly drones after either receiving a Certificate of Waiver or Authorization from the Federal Aviation Administration (FAA), or by operating drones under "Part 107" rules, which require (among other things) that the drone be in the line of sight of the pilot and not be flown over people, although police departments can request that those requirements be waived.

Still, under certificates and "Part 107" rules, police departments are not required to adhere to the types of privacy and transparency policies necessary to protect the rights of Americans from excessive government intrusion. Indeed, as the head of the FAA's Unmanned Aircraft Systems Integration Office said in 2013, "The FAA has no authority to make rules or enforce any rules relative to privacy." Congress, however, *can* condition law enforcement grants on the acceptance of policies that protect important constitutional values.

Transparency, Accountability, and Privacy

Stingrays, body cameras, and drones can play a role in improving law enforcement by making it easier for police to search for suspects and missing persons and gather evidence. Body cameras in particular can be

valuable in promoting increased accountability and transparency in law enforcement. However, these benefits come with significant privacy concerns that Congress should address.

Each of these tools is capable of collecting a vast amount of sensitive data. Subjects of body cameras include not only the victims of crimes, but children, informants, and those involved in accidents. In addition, police body cameras can film inside homes.

As for UAVs, in the course of collecting video data, drones can gather information about backyards and other private property observable from the air. Thanks to Supreme Court rulings from the 1980s, warrantless naked-eye aerial surveillance of backyards is *not* proscribed. Thus, in the absence of restrictive regulations, Americans may have to adapt to a heightened level of surveillance: the explosion in the number of drones means that police will be able to snoop on people hosting barbecues, sunbathing, gardening, or playing with their children in backyards without having to secure a warrant first. That would be disturbing enough if drones were outfitted only with cameras, but they can also be used as platforms for a host of other surveillance tools such as license plate readers and thermal imagers.

Stingrays, which can be helpful in locating suspects and kidnapping victims, nonetheless present an array of privacy and constitutional issues. While the full capabilities of the devices remain shrouded in secrecy, the ability to intercept content from the cell phones of everyone in a given geographic area without a warrant or even notification to the user is troubling. Telephony metadata such as call times, durations, and incoming and outgoing numbers allows the government to piece together the intimate, private details of an individual's life. While the government insists that its stingray devices "are not configured" to intercept the actual content of calls, the capability exists. Without proper oversight that capability will remain an even greater threat to privacy than the bulk collection of metadata and warrantless location tracking.

In addition to privacy concerns associated with modern policing, there are also worries about transparency. Despite widespread international coverage of American police killings, the standard of nationwide data on fatal police encounters is poor. Journalism outlets, not government bodies, provide the most comprehensive databases.

New technologies do help police gather evidence; but under the right guidelines, those technologies can also play a role in informing the public about law enforcement activities. As more and more police departments

seek out new technologies, Congress should ensure that the federal government only funds or lends drones, body cameras, and stingrays for law enforcement agencies that demonstrate a commitment to transparency, accountability, and privacy.

Conditions for Use of Equipment

At a minimum, any of America's roughly 18,000 law enforcement agencies applying for federal grants related to body cameras, drones, or stingrays or seeking to borrow such equipment from federal agencies should outline policies that protect privacy and are consistent with increased accountability and transparency in law enforcement. Unfortunately, federal law enforcement grants have too often been awarded to police departments with poor policies. To promote increased law enforcement transparency and accountability while protecting privacy, Congress should make federal law enforcement grants conditional on agencies' adherence to the following requirements:

Transparency

- Regularly publish the number of drones, body cameras, and IMSI-catchers the agency has, how often these tools are used, and how much data they collect.
- Make the agency's drone, body camera, and IMSI-catcher policies available online.
- Collect and regularly release data related to use-of-force incidents, including those unrelated to the use of body cameras, drones, and IMSI-catchers.
- Publish specifications allowing courts, defense attorneys, and the public at large to understand the full capabilities of the surveillance devices in use.

Accountability

- Make available footage of incidents of public interest.
- Prohibit officers from viewing UAV or body camera footage before making statements related to a use-of-force incident.
- Establish guidelines that clearly state when body cameras should be on: during traffic stops, searches, arrests, detentions, use-of-force incidents, and all 911 responses.
- Ban drones from being outfitted with lethal as well as nonlethal weapons.

Privacy

- Require law enforcement agencies to secure a warrant before using an IMSI-catcher or UAV, except in exigent circumstances.
- Ban the release of UAV and body camera footage showing the interior of private residential property.
- Ban the collecting and/or reading of text message and phone call content collected by IMSI-catchers without a warrant.
- Ban the use of biometric software on body camera and UAV data.

Finally, Congress should take steps to apply these policies to federal law enforcement agencies. Those agencies are not only some of the country's largest law enforcement agencies, but also some of the best funded.

Since the advent of the drug war and the War on Terror, the federal government has become a powerful and pervasive influence on state and local law enforcement policies. As long as the federal government maintains that role, Congress should endeavor to protect Americans' most cherished constitutional rights and prevent abuse. Congress should require appropriate transparency, accountability, and privacy-respecting policies before flooding state and local law enforcement agencies with grant money and cutting-edge surveillance technology.

Suggested Readings

Brown, C. Justin, and Kasha M. Lee. "StingRay Devices Usher in a New Fourth Amendment Battleground." National Association of Criminal Defense Lawyers, *The Champion*, June 2015.

Coburn, Tom. "Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities." Office of Sen. Tom Coburn, Committee on Homeland Security and Governmental Affairs, December 2012.

Feeney, Matthew. "Watching the Watchmen: Best Practices for Police Body Cameras." Cato Institute Policy Analysis no. 782, October 27, 2015.

McNeal, Gregory. "Drones and Aerial Surveillance: Considerations for Legislatures." Brookings Institution Project on Civilian Robotics, November 2014.

Miller, Lindsay, Jessica Toliver, and Police Executive Research Forum. *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned*. Washington: Department of Justice, Office of Community Oriented Policing Services, 2014.

Rule, Troy A. "Airspace in an Age of Drones." *Boston University Law Review* 95 (2015): 155–208.

Stanley, Jay. "Police Body-Mounted Cameras: With Right Policies in Place, a Win for All—Version 2.0." American Civil Liberties Union, March 2015.

—Prepared by Adam Bates and Matthew Feeney