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 cellphone tracking devices used by federal law enforcement agencies, including joint federal and state task forces; and
- direct the Federal Bureau of Investigation and the Federal Communications Commission to rescind the nondisclosure agreements and secrecy policies that federal agencies negotiate with state and local law enforcement partners regarding cellphone tracking devices, or stingrays.

Since the beginning of modern policing in 1829, law enforcement agencies have taken advantage of new technologies. From two-way radios and eavesdropping devices to tasers and drones, police have been quick to put new technology into the field. However, recent developments in surveillance technology, combined with a lagging Fourth Amendment jurisprudence and inadequate legislative oversight, have jeopardized the constitutional rights of millions of American citizens. Modern technology gives police access to tools such as body cameras, drones, facial recognition technology (FRT), and cellphone tracking devices that could, without appropriate regulations in place, allow for the warrantless and persistent surveillance of entire American cities.

Police departments have a legitimate interest in the use of body cameras, drones, FRT, and cellphone 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.

Law enforcement is traditionally a state and local function in our federal system; however, over the past few decades, the federal government has increas-

ingly injected itself into local policing 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 policing priorities while granting the federal government a massive role in shaping law enforcement policy at the state and local levels.

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

Cellphone Tracking

Cellphone 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 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 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, in 2012, 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 providing 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.

A Maryland state appeals court 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 cellphone within an apartment. The Second Circuit Court of Appeals 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, passed the Citizen Privacy Protection Act, which conditions police deployment of stingrays on a showing of probable cause before a court. Congress should follow the lead of reforming states 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.

Since then, the federal government has spent millions of dollars on state and local police body camera grants. These grants should be conditioned on a set of body camera policies that emphasize accountability, transparency, and privacy, which are outlined in a later section.

Drones

Unmanned aerial vehicles (UAVs), commonly called "drones," vary considerably in size and capability and are used to collect video data. Police departments do not require federal permission to adopt body cameras, but 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 the FAA's Small Unmanned Aircraft Systems (Part 107) rules, which require (among other things) that the drone not be flown over people or at night, 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.

Facial Recognition

Law enforcement agencies at the local, state, and federal levels are increasingly using facial recognition technology. FRT confirms identity via the automated measurement of facial features in an image. These measurements are compared with measurements in a database. A match confirms the identity of the person in the image. Dozens of federal agencies and thousands of state and local police departments use FRT. Given its potential as a mass surveillance technology, FRT ought to be strictly controlled.

According to research from Georgetown Law's Center on Privacy and Technology, at least half of American adults are in databases that law enforcement can search with FRT. This situation is thanks in part to the fact that some states volunteer their department of motor vehicles data to law enforcement.

Some jurisdictions have taken steps to ban police use of FRT in light of the surveillance concerns associated with the technology. However, FRT has valuable private-sector applications and can be used to find missing persons. A ban is therefore not the best policy. Rather, policies that accept the benefits of facial recognition while also protecting privacy are worth pursuing.

Transparency, Accountability, and Privacy

Stingrays, body cameras, drones, and FRT 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 help promote increased accountability and transparency in law enforcement. However, these benefits come with significant privacy concerns that Congress should address.

Each of these tools can collect a vast amount of sensitive data and subject law-abiding citizens to intrusive monitoring. Subjects of body cameras include

not only the victims of crimes but also children, informants, and those involved in accidents. In addition, police body cameras can film inside homes. FRT can capture footage of people unconnected with any investigation peacefully going about their day.

As for UAVs, in the course of collecting video data, drones can gather information about "open fields" 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 privacy-protecting safeguards, 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. Some states have imposed warrant requirements for drone surveillance, but Congress has yet to pass such a requirement for federal law enforcement agencies.

Stingrays can be helpful in locating suspects and kidnapping victims, but they also raise an array of privacy and constitutional issues. Although the full capabilities of the devices remain shrouded in secrecy, the ability to intercept content from the cellphones 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—allow the government to piece together the intimate 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. Journalists, not government bodies, provide the most comprehensive databases. Congress can improve the poor state of policing transparency by conditioning grants on police departments collecting data related to police-involved shootings.

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 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

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.

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

Transparency

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

Accountability

- Make footage of incidents of public interest available.
- Prohibit officers from viewing UAV or body camera footage in which they appear 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 and nonlethal weapons.

Privacy

- Require law enforcement agencies to secure a warrant before using a stingray or UAV, except in exigent circumstances.

- Ban the release of UAV and body camera footage showing the interior of private residential property. Such footage should be available to residents of the property or their next of kin.
- Ban the collecting or reading of text message and phone call content collected by stingrays without a warrant.
- Ban the use of biometric software, such as FRT, on body camera and UAV data.

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

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

Bates, Adam. "Stingray: A New Frontier in Police Surveillance." Cato Institute Policy Analysis no. 809, January 25, 2017.

Bier, David, and Matthew Feeney. "Drones on the Border: Efficacy and Privacy Implications." Cato Institute Immigration Research and Policy Brief no. 5, May 1, 2018.

Feeney, Matthew. "Surveillance Takes Wing: Privacy in the Age of Police Drones." Cato Institute Policy Analysis no. 807, December 13, 2016.

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

—Prepared by Matthew Feeney