ELECTRONIC FRONTIER FOUNDATION
PROTECTING RIGHTS AND DEFENDING FREEDOM ON THE ELECTRONIC FRONTIER
eff.org

Law Enforcement Technology Primer for Civilian Oversight Bodies

DEFINITIONS, ISSUES, AND QUESTIONS TO ASK REGARDING EMERGING SURVEILLANCE TECHNOLOGIES AND PRACTICES IN LAW ENFORCEMENT

Dave Maass, Investigative Researcher, Electronic Frontier Foundation

National Association for Civilian Oversight of Law Enforcement Annual Conference
October 4-8, 2015. Riverside, CA

New law enforcement technologies are raising new questions about what civil rights abuses look like in the digital age. Historically, allegations of police misconduct were based on visible behavior: people generally know when they have been assaulted, detained unjustly, or had their property searched or seized without due process. Today, civil rights violations occur on computer screens, amplified by automated processes, or exacted invisibly and indiscriminately on large populations.

Often, law enforcement agencies will adopt these new technologies without community input and before adequate regulations have been enacted to control their use. For some agencies this is a political calculation: while the public is best served by having limitations in place on the front end, it can be politically difficult for elected officials to scale back once the technology has been integrated into policing. These problems are exacerbated by a lack of transparency, with journalists and researchers unable to access records critical to an informed public debate.

That's where civilian oversight of law enforcement has a role. This primer will provide background on several common technologies that oversight bodies should watch closely.

Common and emerging surveillance technologies

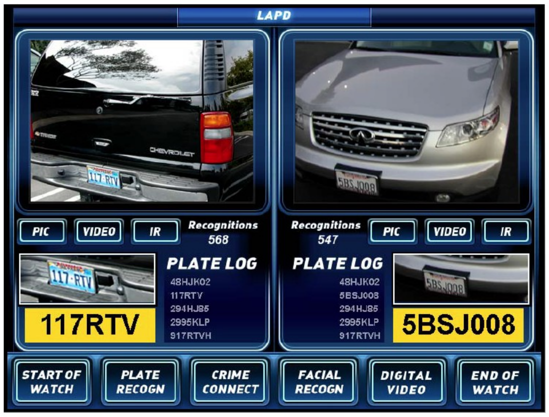
IMSI Catchers/Cell Site Simulators

International Mobile Subscriber Identity (IMSI) catchers emulate a cell tower to collect information on individual cell phones. The devices are primarily used to track suspects, but in the process collect information from any phone that connects to them including, potentially, call data and content. These devices are often placed in specialized police vehicles or even on aircraft. IMSI catchers are also known as “stingrays” and “dirtboxes,” because of the product names offered by two companies, Harris Corp. and Digital Receiver Technology. Many enforcement agencies have signed nondisclosure agreements preventing them from revealing the use of this technology to anyone, including defense counsel in criminal cases.

Unmanned Aerial Vehicles

Commonly known as “drones,” UAVs have been used by law enforcement agencies for mass surveillance, search and rescue, and tailing suspects. UAVs range in size from small quadrotors (four propellers) to “Reapers” (fixed-wing aircraft weighing several tons). Unlike traditional helicopter or airplane surveillance, UAVs are lower cost, harder to spot, and, in some cases, able to stay in the sky longer. Agencies without their own drone programs can borrow drones from federal agencies, such as Customs and Border Patrol. North Dakota recently passed a law that prohibits mounting guns on drones, but did not rule out less-lethal weapons such as tear gas and rubber bullets.

Automated License Plate Recognition



Recognitions 568

PLATE LOG
48HJK02
117RTV
294HJ85
2995KLP
917RTVH

117RTV

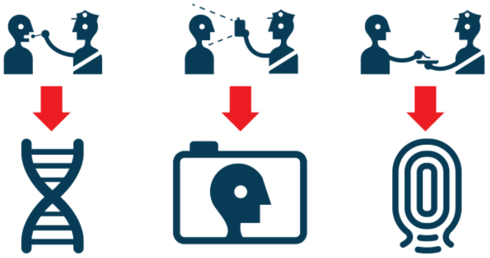
Recognitions 547

PLATE LOG
48HJK02
5BSJ008
294HJ85
2995KLP
917RTVH

5BSJ008

Also known as “automatic license plate readers” or “automated number plate recognition,” ALPR systems are networks of cameras that capture, analyze, and store the license plate data on every car that passes within range, including the time, date, and location. A single camera can capture thousands of plates in a day. The cameras are mounted to patrol vehicles or to fixed locations, such as street lights. These cameras often feed into massive databases—in aggregate, this data can reveal sensitive information about people, including where they live, worship, and what doctors they visit. Police will often create “hot lists” of vehicles that may be stolen, suspected of being linked to crime, or more generally under suspicion; police are alerted whenever a hot-listed car is spotted by an ALPR camera. Police will also subscribe to privately-operated ALPR databases, such as Vigilant Solutions' LEARN Intelligence Network and NLETS' National LPR Pointer System. Vigilant has also included language in agreements to ban agencies from speaking to the press or criticizing the product publicly without permission.

Biometric Identification



Biometric technology is used to capture, analyze, and match a person’s physical or biological features. This may include fingerprinting, face recognition, iris scanning, tattoo recognition, and Rapid DNA processing—all of which may draw from or feed into massive databases of biometric information. In addition, many of these technologies are now capable of near-instantaneous processing and use in the field with mobile devices or apps. Some agencies have investigated applying technologies such as facial recognition to CCTV cameras, video footage, and photographic images, similar to ALPR.

Learn about EFF's work on street-level surveillance at eff.org/sls

Social Media Monitoring

Law enforcement are using sophisticated software systems to mine and analyze public social media data. However, as users become more mindful of their privacy, law enforcement are creating fake accounts, impersonating other users, or obtaining login credentials from informants in order to access or surveil in private online spaces—sometimes in violation of the social network's terms of service. This has included keeping tabs on groups engaged in legitimate First Amendment activities.

Emerging civil liberties issues

What might a civil rights violation look like in the digital age? Here are concerning issues, many of which have already been documented:

- Mass surveillance itself can be a violation of rights. By definition, it collects information on members of the public who are not suspected of any wrongdoing.
- Targeted surveillance can be a violation of rights if the surveillance is unauthorized or goes beyond the scope of the authorization.
- These technologies can be used to gather intelligence on people engaged in First Amendment-protected activities, such as protesters, journalists, or political organizations.
- Surveillance technologies can be used disproportionately on ethnic, religious, or cultural communities—a kind of digital racial profiling.
- Financial relationships with companies and grantmakers may skew policing priorities, especially when companies provide technology at no cost in exchange for an interest in warrant settlements.
- Asset forfeiture may incentivize disproportionate use of surveillance technology.
- Technological errors may result in wrongful stops, detentions, or arrests.
- Individuals added to databases (such as ALPR hot lists) may find themselves stopped disproportionately.
- Staff may access law enforcement databases to inappropriately retrieve information on people for personal reasons, such as spying on former spouses or background-checking online dating profiles.
- Insecure storing of information could result in data breaches, putting people's sensitive information at risk.
- Capturing biometric information from people in the field without consent or due cause can be invasive.
- Undercover social media investigations can chill rights to expression and organization and undermine community relationships.

What oversight bodies can do

Law enforcement agencies are notoriously opaque when it comes to surveillance technologies, especially when questioned by the press. Civilian oversight boards may be better positioned to investigate these technologies. Actions to take include:

- Create a clear process for the public to report digital privacy related complaints and include digital categories in annual reports and questionnaires
- Investigate mass surveillance complaints (i.e. when a member of the public believes that a technology is inappropriately collecting information on a large number of people)
- Request and inspect documents, such as procedures, capabilities, privacy policies, audits, and misuse investigations
- Receive informational updates from skilled law enforcement personnel, including those in charge of managing IT
- Engage with agencies before new technologies are purchased or policies are written

What oversight bodies should be asking

Here are lines of inquiry that can and should be applied to each technology individually:

- How long are records kept? What are the data retention and purging policies?
- How many devices does the law enforcement agency have? Are they able to borrow this technology from other agencies?
- Who has access to the data, and how is access controlled? Are external agencies able to tap into the data?
- Who is authorized to use these technologies ad what kind of training do they receive? How is authorization granted to use these technologies and methods?
- How much data are systems and devices able to capture over a specified period of time (e.g. a year, month, single day, and per single use)?
- How many individuals' data and unique files are maintained in a system? How are people added to “hot lists”?
- How are these programs funded and what are the financial relationships involved? How does asset forfeiture impact use of these systems?
- How are systems audited, both for technical security (e.g. encryption) and for inappropriate access (e.g. misuse)? How are misuse cases reported, investigated, and documented? How many were there and what were the outcomes?
- Who is able to adjust the match sensitivity of biometric devices?

Contacts for EFF's Street Level Surveillance project:

Jennifer Lynch
Senior Staff Attorney
jlynch@eff.org
(415) 436-9333 ext. 136

Nadia Kayyali
Activist
nadia@eff.org
(415) 436-9333 ext. 104

Dave Maass
Investigative Researcher
dm@eff.org
(415) 436-9333 ext. 151

Learn about EFF's work on street-level surveillance at eff.org/sls