Police Force

Author : James Grimmelmann

Date : July 1, 2016

Works mentioned in this review:

- Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet , 12 **Nw. J. Tech. & Intell. Prop.** 1 (2014)
- Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, **Stan. L. Rev.** (forthcoming 2016), available at SSRN
- Elizabeth E. Joh & Thomas W. Joo, Sting Victims: Third-Party Harms in Undercover Police Operations, 88 **S. Cal. L. Rev.** 1309 (2015)
- Elizabeth E. Joh, Bait, Mask, and Ruse: Technology and Police Deception, 128 **Harv. L. Rev. F.** 246 (2015)
- Jonathan Mayer, *Constitutional Malware* (2015), available at SSRN
- Brian L. Owsley, Beware of Government Agents Bearing Trojan Horses, 48 **Akron L. Rev.** 315 (2015)
- Stephanie K. Pell & Christopher Soghoian, A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities, 16 **Yale J.L. & Tech.** 134 (2013)

Police carry weapons, and sometimes they use them. When they do, people can die: the unarmed like Walter Scott and Tamir Rice, and bystanders like Akai Gurley and Bettie Jones. Since disarming police is a non-starter in our gun-saturated society, the next-best option is oversight. Laws and departmental policies tell officers when they can and can't shoot; use-of-force review boards and juries hold officers accountable (or are supposed to) if they shoot without good reason. There are even some weapons police shouldn't have at all.

Online police carry weapons, too, because preventing and prosecuting new twists on old crimes often requires new investigative tools. The San Bernadino shooters left behind a locked iPhone. Child pornographers gather on hidden websites. Drug deals are done in Bitcoins. Hacker gangs hold hospitals' computer systems for ransom. Modern law enforcement doesn't just passively listen in: it breaks security, exploits software vulnerabilities, installs malware, sets up fake cell phone towers, and hacks its way onto all manner of devices and services. These new weapons are dangerous; they need new rules of engagement, oversight, and accountability. The articles discussed in this review help start the conversation about how to guard against police abuse of these new tools.

In one recent case, the FBI seized control of a child pornography website. For two weeks, the FBI operated the website itself, sending a "Network Investigative Technique" — or, to call things by their proper names, a piece of spyware — to the computers of people who visited the website. The spyware then phoned home, giving the FBI the information it needed (IP addresses) to start identifying the users so they could be investigated and prosecuted on child pornography charges.

There's something troubling about police operation of a spyware-spewing website; that's something we normally expect from shady grey-market advertisers, not sworn officers of the law. For one thing, it involves pervasive deception. As Elizabeth E. Joh and Thomas W. Joo explain in Sting Victims: Third-Party Harms in Undercover Police Operations, this is hardly a new problem. Police have been using fake names and fake businesses for a long time. Joh and Joo's article singles out the underappreciated way in which these ruses can harm third parties other than the targets of the investigation. In child abuse cases, for example, the further distribution of images of children being sexually abused "cause[s] new injury to the child's reputation and emotional well-being."

Often, the biggest victims of police impersonation are the specific people or entities being impersonated. Joh and Joo give a particularly cogent critique of this law enforcement "identity theft." The resulting harm to trust is especially serious online, where other indicia of identity are weak to begin with. The Justice Department settled for $143,000 a civil case brought by a woman whose name and intimate photographs were used by the DEA to set up a fake Facebook account to send a friend request to a fugitive.

Again, deception by police is not new. But in a related essay, Bait, Mask, and Ruse: Technology and Police Deception, Joh nicely explains how "technology has made deceptive policing easier and more pervasive." A good example, discussed in detail by Stephanie K. Pell and Christopher Soghoian in their article, A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities, is IMSI catchers, or StingRays. These portable electronic devices pretend to be cell phone towers, forcing nearby cellular devices to communicate with them, exposing some metadata in the process. This is a kind of lie, and not necessarily a harmless one. Tricking phones into talking to fake cell towers hinders their communications with real ones, which can raise power consumption and hurt connectivity.

In an investigative context, StingRays are commonly used to locate specific cell phones without the assistance of the phone company, or to obtain a list of all cell phones near the StingRay. Pell and Soghoian convincingly argue that StingRays successfully slipped through holes in the institutional oversight of surveillance technology. On the one hand, law enforcement has at times argued that the differences between StingRays and traditional pen registers meant that they were subject to no statutory restrictions at all; on the other, it has argued that they are sufficiently similar to pen registers that no special disclosure of the fact that a StingRay is to be used is necessary when a boilerplate pen register order is presented to a magistrate. Pell and Soghoian's argument is not that StingRays are good or bad, but rather that an oversight regime regulating and legitimizing police use of dangerous technologies breaks down if the judges who oversee it cannot count on police candor.

In a broader sense, Joh and Joo and Pell and Soghoian are all concerned about police abuse of trust. Trust is tricky to establish online, but it is also essential to many technologies. This is one reason why so many security experts objected to the FBI's now-withdrawn request for Apple to use its code signing keys to vouch for a modified and security-weakened custom version of iOS. Compelling the use of private keys in this way makes it harder to rely on digital signatures as a security measure.

The FBI's drive-by spyware downloads are troubling in yet another way. A coding mistake can easily destroy data rather than merely observing it, and installing one piece of unauthorized software on a computer makes it easier for others to install more. Lawful Hacking, by Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, thinks through some of these risks, along with more systemic ones. In order to get spyware on a computer, law enforcement frequently needs to take advantage of an existing unpatched vulnerability in the software on that computer. But when law enforcement pays third parties for information about those vulnerabilities, it helps incentivize the creation of more such information, and the next sale might not be to the FBI. Even if the government finds a vulnerability itself, keeping that vulnerability secret undercuts security for Internet users, because someone else might find and exploit that same vulnerability independently. The estimated $1.3 million that the FBI paid for the exploit it employed in the San Bernadino case — along with the FBI's insistence on keeping the details secret — sends a powerful signal that the FBI is more interested in breaking into computers than in securing them, and that that is where the money is.

The authors of *Lawful Hacking* are technologists, and their article is a good illustration of why lawyers need to listen to technologists more. The technical issues — including not just how software works but how the security ecosystem works — are the foundation for the legal and policy issues. Legislating

security without understanding the technology is like building a castle on a swamp.

Fortunately, legal scholars who do understand the technical issues — because they are techies themselves or know how to listen to them — are also starting to think through the policy issues. Jonathan Mayer's Constitutional Malware is a cogent analysis of the Fourth Amendment implications of putting software on people's computers without their knowledge, let alone their consent. Mayer's first goal is to refute what he calls the "data-centric" theory of Fourth Amendment searches, that so long as the government spyware is configured such that it discloses only unprotected information, it is irrelevant how the software was installed or used. The article then thinks through many of the practicalities involved with using search warrants to regulate spyware, such as anticipatory warrants, particularity, and notice. It concludes with an argument that spyware is sufficiently dangerous that it should be subject to the same kind of "super-warrant" procedural protections as wiretaps. Given that spyware can easily extract the contents of a person's communications from their devices at any time, the parallel with wiretaps is nearly perfect. Indeed, on any reasonable measure, spyware is worse, and police and courts ought to give it closer oversight. To similar effect is former federal magistrate judge Brian Owsley's Beware of Government Agents Bearing Trojan Horses, which includes a useful discursive survey of cases in which law enforcement has sought judicial approval of spyware.

Unfortunately, oversight by and over online law enforcement is complicated by the fact that a suspect's device could often be anywhere in the world. This reality of life online raises problems of jurisdiction: jurisdiction for police to act and jurisdiction for courts to hold them accountable. Ahmed Ghappour's Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web points out that when a suspect connects through a proxy-based routing service such as Tor, mapping a device's location may be nearly impossible. Observing foreigners abroad is one thing; hacking their computers is quite another. Other countries can and do regard such investigations as violations of their sovereignty. *Searching Places Unknown* offers a best-practices guide for avoiding diplomatic blowback and the risk that police will open themselves up to foreign prosecution. One of the most important suggestions is minimization: Ghappour recommends that investigators proceed in two stages. First, they should attempt to determine the device's actual IP address and no more; with that information, they can make a better guess at where the device is and a better-informed decision about whether and how to proceed.

This, in the end, is what tainted the evidence in the Tor child pornography investigation. Federal Rule of Criminal Procedure 41 does not give a magistrate judge in Alexandria, Virginia the authority to authorize the search of a computer in Norwood, Massachusetts. This NIT-picky detail in the Federal Rules may not be an issue much longer. The Supreme Court has voted — in the face of substantial objection from tech companies and privacy activists — to approve a revision to Rule 41 giving greater authority to magistrates to issue warrants for "remote access" searches. But since many of these unknown computers will be not just in another district but abroad, the diplomatic issues Ghappour flags would remain relevant even under a revised Rule 41. So would Owsley's and Mayer's recommendations for careful oversight.

Reading these articles together highlights the ways in which the problems of online investigations are both very new and very old. The technologies at issue — spyware, cryptographic authentication, onion routing, cellular networks, and encryption — were not designed with much concern for the Federal Rules or law enforcement budgeting processes. Sometimes they bedevil police; sometimes they hand over private data on a silver platter. But the themes are familiar: abuse of trust and positions of authority, the exploitation of existing vulnerabilities and the creation of new ones. Oversight is a crucial part of the solution, but at the moment it is piecemeal and inconsistently applied. The future of policing has already happened. It's just not evenly distributed.

Cite as: James Grimmelmann, *Police Force*, JOTWELL (July 4, 2016) (reviewing seven works), https://cyber.jotwell.com/police-force/.