"F the Police: police surveillance and how to avoid it"

Eva Galperin, Electronic Frontier Foundation
From notes of an address at the February 2015 Association of Alternative Newspapers/The Media Coalition Joint Conference, San Francisco
(lightly edited by James Wheaton, First Amendment Project; all mistakes are his)

A. Why do you care about police surveillance methods and tools?

You are journalists. If you're doing your job, you are antagonizing people in power or working with people who are antagonizing people in power. Those people may be the police or the people the police work for.

You also have or will have sources that ask to be kept anonymous, in exchange for giving you information. When you say yes, you have crated a contract. Don't break it. You have also asked the person to trust you. Don't betray that trust. What follows are basic threats to keeping your confidential information confidential. You owe it to your sources, yourself and your profession to keep your promise and not allow information to be revealed by not paying attention or being lazy.

B. The threat. What are the capabilities of your attacker?

In the course of your works you might also antagonize: corporations w/ PIs and lawyers, the FBI, the NSA, other governments. All these actors have different capabilities and they are outside of the scope of this talk. This is about local (and state) police.

1. Physical tracking

   Cops can follow you around. They have lots of time, and they are practiced in the art of physically surveilling people, including people who know that they are being watched or are trying to hide. People who don't know and are not trying to hide? They are easy.

2. Physical searches

   Police can also search your house/office/vehicle, either with a warrant, following arrest, or because the person gives consent..

3. Informational Tracking
   Warrants: a search warrant is issued in secret.
   Notably, warrants are not supposed to be issued for journalists' information or records under both state and federal law. Police have been known to "forget" to tell the judge being asked for the warrant that the subject is a journalist.
   Subpoenas: subpoenas give you more time, and they can be fought in court, and there are protections for journalists in 49 states and (maybe) in federal law. That's why cops rarely use them anymore. It's much easier to get your information from a compliant third party.

PEN registers (wiretaps): also issued with a warrant; these capture the number of every call made, including all your sources.

4. Voluntary handover of data by third parties

This is the biggest area, by far the largest threat.
It simply bypasses the requirement for a warrant or subpoena, and can be done in secret.
It works because so much of your data – or rather data about you – isn't yours. It all belongs to somebody else.

Examples:
> Google searches.
> Gmail and all other email.
> Phone companies for texted numbers, contacts and phone call metadata (NSA gets all call and texting data through National Security Letters, we learned from Snowden's disclosures).

The "third party doctrine" allows this. In a case from Maryland, the Supreme Court held that you have no expectation of privacy in the log of calls made from your phone. The phone companies are notoriously handing over calls logs and metadata to any law enforcement agency that simply asks, without requiring a subpoena or warrant.[1]

5. Data and metadata: Why your data is dangerous

> Metadata can give away a lot about you.

The government tells us that "it's just metadata" and hint that's it's all quite innocent and not very revealing. But they simultaneously tell themselves, Congress, us (and courts) that metadata is a vital tool for capturing and stopping terrorists. Which is it - innocent or highly revealing?

Examples (from EFF website):
> a call to a phone sex service at 2:24 am for 18 minutes (they say they don't know what you talked about);
> a call to the suicide prevention hotline from the Golden Gate Bridge (But the topic of the call remains a secret);

---

[1] In 2012 alone, the telephone companies turned over their customers' data 1,133,688 times.
This does not include occasions when companies turned over so called "tower dumps" in which they turn over the numbers of all cell phones within a certain tower's range at any given time, nor does it include the massive turning over of all metadata on every caller to the NSA using "National Security Letters" as revealed by Edward Snowden. Sources: http://www.forbes.com/sites/kashmirhill/2013/12/10/this-is-how-often-your-phone-company-hands-data-over-to-law-enforcement; EFF.org. Winter 2016

> a call to an HIV testing service, then your doctor, then your health insurance company in the same hour (But they don't know what was discussed);
> a call to a gynecologist, for a half hour, and then called the local Planned Parenthood's number later that day (But nobody knows what you spoke about).

Most telling, of course, for journalists, are sources' numbers; a reverse phone directory is trivially easy to procure to learn the names.

>Linkability.

One piece of data may not tell the police a lot about you (or your source), but putting different pieces of data together can paint a detailed picture.
Last time you visited a confidential source:
> Did you bring your smart phone with you?
> Did you take a cab, Uber or Lyft?
> Did you pay for the ride with a credit card?
> Did you take public transportation?
> Pay with a Clipper card?
> Did you drive across a bridge?
> Pay with a FastTrack?
> Did you park in a parking garage?
> Did that garage have a surveillance camera?
> Now, did your source do any of these?

If you have an Android phone, you can go to a link and see your location history because it broadcasts all your wifi networks, even when off, to all nearby wifi connections. Based on my location history, anyone can deduce where I live, where I work, where my friends live, the location of my gym.

And it's not just what you give away about yourself. Your friends/associates can give you away too. Your email address may be pulled off of a source's phone. A friend may tag you in a photo on Facebook.

C. The new threat: Stingrays (and their flying cousins, dirtboxes)

These are also known as "cell-site simulators," because, well, that's exactly what they do. A Stingray is a brand name for a one type of IMSI device that mimics a cell phone tower and forces all nearby mobile phones or devices to connect to it. Every phone that connects to the Stingray reports its number, GPS location, and the numbers of all out going calls and texts. That's every location and outgoing call and text log of every phone within a certain radius—up to several kilometers—of the Stingray. All of that is done without a warrant.

At least 46 state and local police departments, from Sunrise, Florida, to Hennepin County, Minnesota, have gotten cell-site simulators, which range widely in price from

$16,000 to more than $125,000 a pop. And like the federal government, local police are using this technology without any judicial oversight.[2]

The problem with Stingrays is twofold. First, Stingrays simply don't provide reliable results—if a cell phone is located near a wall separating two apartments, it is nearly impossible to determine which apartment that phone is in.

Second, the larger and scarier problem with Stingrays is that they now give local police all of the information that any particular cell tower has, without having to bother with a subpoena or even an ask to cell phone companies. It's this dragnet aspect of Stingrays—that police can simply drive to neighborhoods and log calls, numbers, and locations—that has a terrifying effect on privacy. It's easy to imagine the parade of horribles that could result from this type of continued used of Stingrays without warrants by local police: targeting and tracking of certain protesters, or a more general dragnet collection of phone numbers in high crime areas, or even use by one local police officer who has a grudge. For journalists, place a Stingray near their office or home and track their calls to sources.

Both of these issues are problems that the requirement for a judge-issued warrant—which require a level of specificity and basis for the particular search that a

---

[2] Police and surveillance companies go to great lengths to keep this a secret.

> Harris, the company that sells Stingrays, requires that police departments sign a non-disclosure agreement promising not to reference Stingrays in any public document.

> Federal agencies like the US Department of Justice and the US Marshals Service have instructed local cities and police to keep details of Stingray surveillance secret; in one instance, when a state judge was about to issue an order requiring that documents about the Stingray used by a local police department be disclosed, the US Marshals physically intervened by seizing all the local police department's documents and "federalized" them beyond the reach of state public records law.

> There have been repeated instances of police agencies across the country hiding their use of IMSI catchers from the judges entrusted to provide police oversight.

> In Sarasota, Florida internal police emails revealed officers concealed their use of Stingrays from judges, both withdrawing a warrant affidavit that mentioned the use of an IMSI catcher, and using a policy of referring to Stingrays as a "confidential source" in court documents.

> Judges in Tacoma, Washington signed more than 170 orders unknowingly authorizing Stingray use from 2009 to 2014 because police officers did not disclose the orders would be used to operate an IMSI catcher. Judges first learned they were approving IMSI catchers from local newspaper reporting.

> In a robbery case in Baltimore, Maryland, prosecutors abandoned their use of Stingray evidence after a judge threatened to hold a police officer in contempt for refusing to testify about the device.

> The Wall Street Journal has reported on a secret US Marshals surveillance program that attaches IMSI catchers called "DRTboxes" to airplanes to track suspects, gathering data about scores of innocent people in the process.

reasonable human being must accept—were designed to solve.

Groups like the American Civil Liberties Union and the Electronic Frontier Foundation are working to pass statutes requiring disclosure and transparency by the police when they use and request warrants for the use of Stingrays. “In order for warrants to meaningfully constrain police action, the government must be candid with judges about when it intends to use Stingrays and what Stingrays’ capabilities are,” says Nathan Wessler, an attorney at the Speech, Privacy, and Technology Project at the ACLU. “Without that information, courts simply cannot ensure that the government is complying with the Fourth Amendment.” So far 11 states—Colorado, Illinois, Indiana, Maine, Maryland, Minnesota, Montana, Tennessee, Utah, Virginia, and Wisconsin—have passed laws that require police to get a warrant to use a Stingray.[3]

D. Malware

Police may also use malware to compromise endpoints. European companies such as HackingTeam and FinFisher sell exclusively to governments and law enforcement, but most US police departments are not very sophisticated in this area.

The malware can come in the form of clicking on a link that seems innocent (or apparently from a trusted source), or opening an attachment, again that appears innocent or from a trusted source. Once installed, the malware grants the snooper essentially unlimited access to the device and all information on it. For a phone that includes all contacts, the full text of all texts, and possibly emails as well.

E. Dragnet surveillance

1. Surveillance cameras

Cameras are becoming ubiquitous. Even Deep Throat and Bob Woodward could not meet as they used to: parking garages now have surveillance cameras. Mostly private, but also public, cameras are everywhere. One Bay Area reporter was trying to dispose of some secret documents leaked to him by a police source; he had to drive all over Oakland and Berkeley to try to find a place he could do so without being on camera (incase the trove was discovered).

2. License Plate Readers

Police Departments throughout the country are installing Automatic License Plate Readers (ALPRs) both on fixed positions on buildings and poles, and on police cars as they cruise. ALPRs capture the plate number and precise location, date and

[3] There’s an Android app called SnoopSnitch that can be used to detect IMSI catchers, but just like the Stringray gets false positives, so does SnoopSnitch. Eva Galperin of EFF got a report of an IMSI catcher -- while on a ferry in the middle of San Francisco Bay. While it would be interesting to take these to some protests, for the most part carrying one of these around is just going to make you feel more paranoid.

time of every single license plate it comes across, potentially thousands every hour. For example, there is a fixed ALPR above the Caldecott Tunnel on Highway 24, recording every car that passes through.

It has been reported that the LA Sheriff and Police Department collect nearly 3 million every week, and have a database "with roughly half a billion license plate scans – an average of about 66 hits for each of the approximately 7.6 million vehicles registered in Los Angeles County." Some police departments claim that information is entirely secret and cannot be released as a public record; that position has been challenged and is before the California Supreme Court.[4]

One journalist sought and received the data on his own car from Oakland; despite having no warrants, arrests or even suspicions about him, Oakland captured 13 sitings of his car over a year, more than once a month.[5]

The cities and counties share this data in massive regional collective databases, meaning a vehicle can be tracked across multiple jurisdictions. The implications for a journalist visiting a source, or especially the journalist who seeks to meet clandestinely with a source, are obvious.

F. So what do you do?

First, don't be a privacy nihilist. Don't just throw up your hands and give up, or simply ignore the issue. Remember: you gave your source your solemn word you would not reveal their identity. You have a duty to that source, to yourself and to your profession not to let that identity become known because you were lazy.

Second, there are secure or anonymous communications tools. But your best bet for avoiding the police is making sure that you don't create data they can track in the first place.

1. <u>For devices like phones, laptops and tablets:</u>

   > Learn to use security/privacy/anonymity tools. Learn them well enough that you can train your sources to use them. Your knowledge of these tools is meaningless if your source does not use them.

   > Encrypt the drives on your devices.

---

[4] ACLU v. Superior Court, Cal. Court of Appeal, 2d Dist., No. _____; Verified Petition for Writ of Mandate, etc., at 2. Currently fully briefed and awaiting oral argument in the California Supreme Court. Case No. S227106..

[5] https://arstechnica.com/tech-policy/2013/07/the-cops-are-tracking-my-car-and-yours/

> Password protect your devices.

2. <u>If questioned by police, politely but firmly:</u>

> ask to speak to your attorney;

> request that all further questioning stop until your attorney is present;

> decline to consent to a search of your phone if asked for it;

> decline to give over a password or otherwise confirm that it is in fact your phone – state only that you have lawful possession of the phone;

> If for whatever reason to decide to talk without a lawyer being present do NOT lie.

3. <u>Do not create a paper trail.</u>

> If you don't use a Clipper Card or credit card, public transit leaves no trail. Bikes leave no trail. Neither does walking.

> Landlines leave far fewer traces than cell phones.

> Face to face meetings and conversations leave far fewer traces than any calls, texts or emails.

> Do not use texts, emails, messaging or other communications that leave permanent records of not only who you communicated with but also about what.

4. <u>Phone protections</u>

> Don't take your smart phone with you to a sensitive meeting.

> Don't take your smart phone to a protest where you risk arrest and having it seized. At minimum you should assume there is a Stingray at any protest that will capture your cell phone's data.

> Consider using a burner phone in such places.

> Turn your phone off or take the battery out if you are worried about recording the conversation. (Notice you can't take the battery out of an iPhone.)

> Know when *not* to communicate.