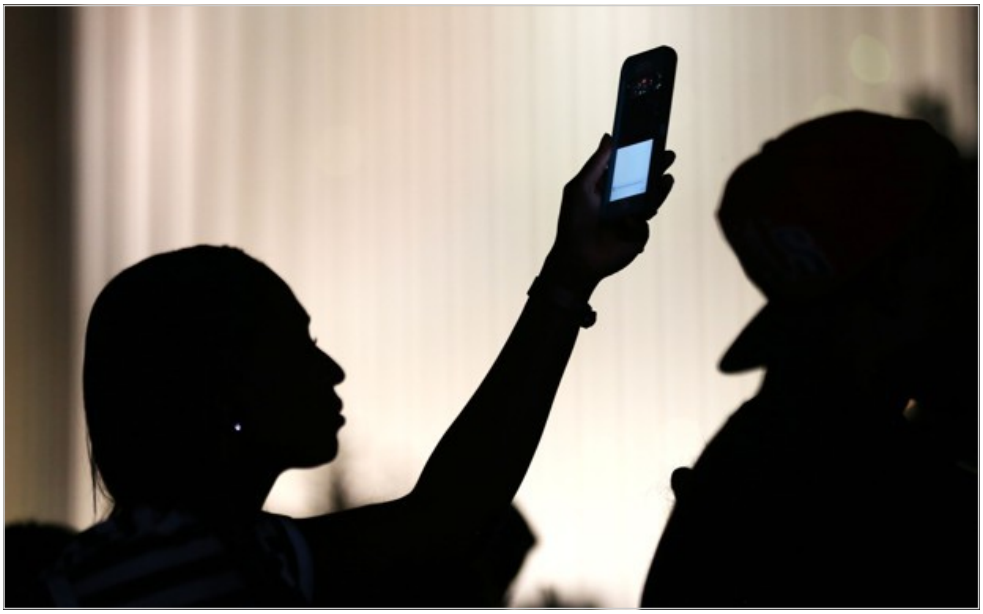
From The Atlantic CITYLAB

Cellphone Spy Tools Have Flooded Local Police Departments

Major cities throughout the U.S. have spent millions on mobile surveillance tools—but there are still few rules about what happens to the information they capture.

GEORGE JOSEPH | @georgejoseph94 | Feb 8, 2017 | 100 Comments



A protester uses her phone during a night of demonstrations over the police shooting of Keith Scott in Charlotte, North Carolina. (Mike Blake/Reuters)

A little after midnight on November 28, 2014, hundreds of Black Lives Matter protesters filled the streets of downtown Chicago. The demonstration was one of many that erupted in cities nationwide soon after a Missouri grand jury failed to indict a Ferguson, Missouri, police officer for the shooting death of Michael Brown that August. As the protesters marched, a police vehicle crept behind them. The black SUV emblazoned with "City of Chicago Emergency Management" appeared to have two 360-degree cameras sprouting from its roof and a command center in the back.

Whenever the vehicle drove by, protesters reported that their phones stopped working.

A week later, audio of a police radio dispatch from the protest was released online. In the recording, an officer alerts a department intelligence analyst about of one of the protest organizers. "One of the girls here... she's been on

her phone a lot," the officer says. "You guys picking up any information? Where they're going, possibly?"

The analyst responds, "Yeah, we're keeping an eye on it. We'll let you know if we hear anything."

The leaked conversation and the cellphone disruptions led many activists to conclude that the police were eavesdropping on them. This story circulated widely in protest circles, but the Chicago Police Department never confirmed any such surveillance operations that night. Legally, listening in on private communications between citizens talking over mobile phones would require a Title III search warrant. But one thing is indisputable: The technology to snoop on nearby phones exists—and the Chicago Police Department has had it for over ten years.

And such spy gear is not limited to Chicago. Hundreds of documents obtained by CityLab from the country's top fifty largest police departments over the last ten months reveal that similar cellphone surveillance devices have been quietly acquired by local authorities nationwide.

The majority of these departments have at least one of two main types of digital-age spy tools: cellphone interception devices, used to covertly track or grab data from nearby mobile devices, and cellphone extraction devices, used to crack open locked phones that are in police possession and scoop out all sorts of private communications and content.

Access to such devices was once largely limited to intelligence agencies like the NSA and the FBI; their acquisition by local police departments is a relatively recent, less-discussed part of a wider police militarization trend. With only a few clicks, police can now map out individuals' social networks, communication timelines, and associates' locations, based on the data captured by these surveillance tools.

As a tool for crime fighting, such intelligence gathering can be powerful indeed: An interception tool could, for example, help police track down a kidnapper; an extraction device could then quickly identify their network of contacts. But the prospect of handing this military-grade spy gear to local law enforcement has inspired concern, in part because of the lack of uniform regulatory safeguards to protect citizens' privacy.

"A lot of the guys using it are saying, 'I don't have to tell anyone I'm using it."

"With 18,000 federal, state, and local law enforcement agencies, you know there are going to be many that are just going to jump on the technology

bandwagon without regard for civil liberties," says Norm Stamper, former Chief of the Seattle Police Department and now a police reform advocate.

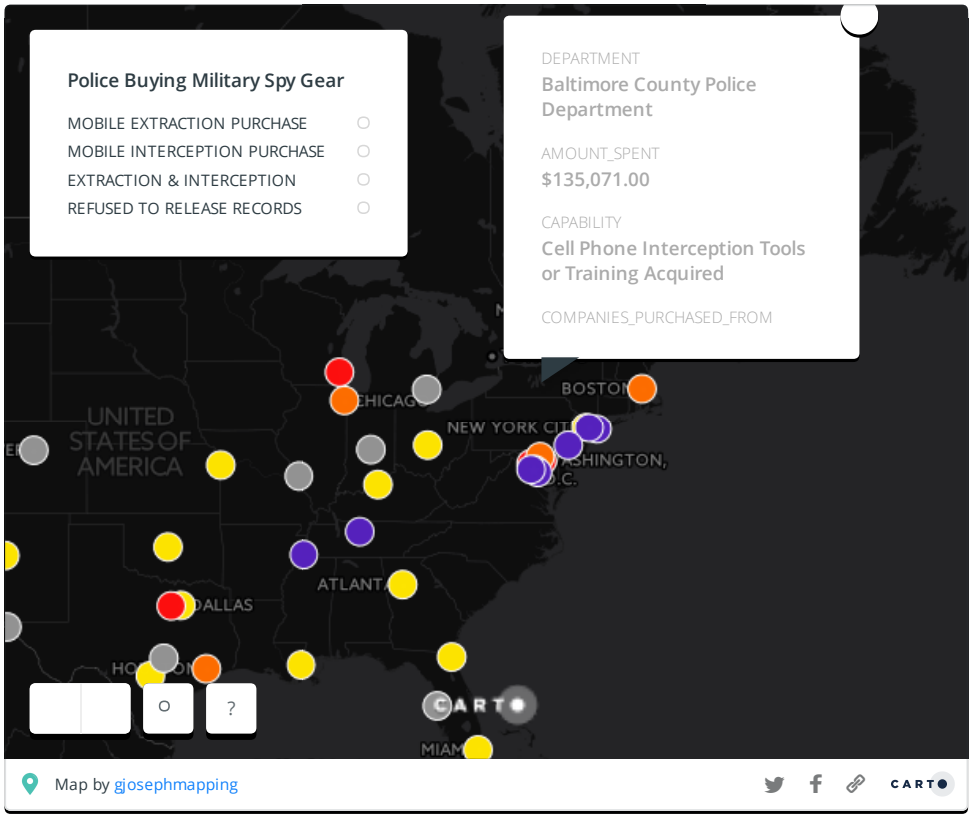
These concerns have taken on a new urgency with the ascension of Donald Trump. The new administration has taken power amid an outbreak of civil resistance in cities nationwide and signs that federal authorities are poised to expand domestic surveillance capabilities. The president has frequently spoken of his plans for the mass deportation of undocumented immigrants and mass surveillance of Muslim Americans and other domestic targets. Executing those plans would be dramatically helped by harvesting, retaining, and distributing personal information from the electronic devices many of us carry in our pockets. And your local police may already have the tools to do just that.

The spy game begins

Two decades ago, cellphone surveillance tools were mostly used by federal law enforcement and intelligence community personnel for national security and high-level criminal investigations. But after 9/11, as police departments ventured into counter-terror operations themselves, local cops began to snatch up these sophisticated devices.

In December 2015, *The Intercept* released a catalogue of military surveillance tools, leaked by an intelligence community source concerned by this perceived militarization of domestic law enforcement. The catalogue included tools that could track thousands of people's cellphones at once, extract deleted text messages from captured phones, and monitor ongoing calls and text messages. Following this news, last April, CityLab began sending public records requests to the top fifty largest police across the country asking for purchasing orders and invoices over 2012 to 2016 related to any of the devices listed in the catalogue. (Note: The fifty largest list is based on data released in 2010 from the Police Pay Journal, and thus does not include some departments now among the top fifty largest).

Of the fifty departments sent public records requests, only eight claimed not to have acquired any spy tools leaked by *The Intercept's* intelligence source. At least twelve have admitted to having cellphone interception devices, and nineteen have admitted to having cellphone extraction devices. The responses, security-based rejections, and outstanding requests still being processed for CityLab suggest that, at a minimum, thirty-nine of the fifty departments have acquired at least some of these military-grade surveillance tools over the last four years. (Click here to see the original cache of documents, or scroll down to the bottom of this article)



In the map above, you can get more details on the various capabilities that the police departments who responded to our requests have acquired in recent years. Click on a city to see its department's spending, years of spending, acquired capabilities, and surveillance gear vendors. The non-redacted purchases, recorded in documents obtained from 27 departments, total more than $4.6 million. (Note: This figure includes all equipment disbursements released in the documents, going as far back as 2008 in a handful of cases.)

How Much Are Police Spending on Cellphone Spy Tools?

Police department	Money spent
Ft. Worth	$765,918
Chicago	$484,150
San Jose	$432,007
Boston	$431,290*
San Francisco	$347,215
Phoenix	$327,826*
Baltimore	$307,322*
Las Vegas	$265,899
Montgomery County (Maryland)	$252,021
Milwaukee	$141,626
Baltimore County	$135,071
Los Angeles	$123,211

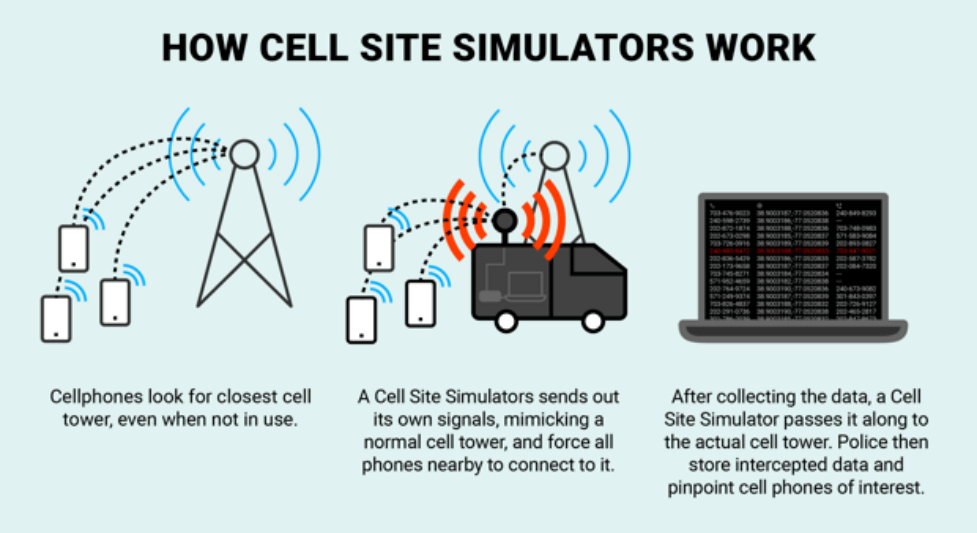
Los Angeles	$123,211
Tuscon	$121,036
Seattle	$78,468
Long Beach	$68,783
Jacksonville	$60,782
Kansas City (Missouri)	$48,748
Oklahoma City	$45,011
Miami	$44,783
Louisville	$32,713
Houston	$22,500
Dallas	$22,045
San Antonio	$18,353
Atlanta	$12,583
Albuquerque	$9,362
Columbus (Ohio)	$8,799

** = Police department provided totals from 2008 - 2011. All other totals from 2012 - 2016.*

(Mark Byrnes, CityLab)

Interception: Seizing data from the skies

At least twelve of the departments surveyed have cellphone interception devices, known as cell site simulators (though this is likely an undercount given that eight departments refused to hand over records). Sometimes referred to as a "Stingray," the suitcase-sized device masquerades as a cell tower, tricking all nearby cellphones to connect to itself. This connection can then be exploited to collect hundreds of phones' locations, call and text logs, and, with certain versions, voice calls and text messages. Cell site simulators can be used to collect data on phones in a target area or to locate phones of interest.



(Katie Martin, The Atlantic)

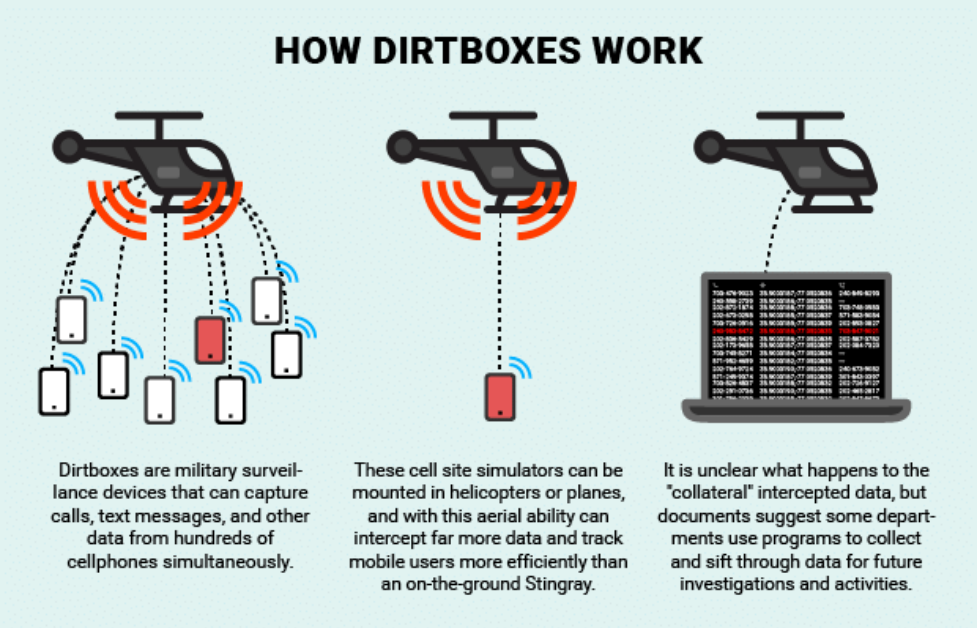
Cell site simulators have aroused the ire of privacy advocates because they can seize data from thousands of phones nearby that may be irrelevant to an ongoing police investigation. What is known about police use of these tools suggests that these invasive data pulls are not distributed randomly. A recent CityLab analysis, for example, found that interceptions were overwhelmingly deployed in low-income and black neighborhoods. Black Lives Matter and left-wing activists have reported the suspected use of cell site simulators at numerous political demonstrations over the last fifteen years.

RELATED STORIES

Racial Disparities in Police 'Stingray' Surveillance, Mapped

Are Police Searching Inauguration Protesters' Phones?

According to the records, departments are also rapidly improving their interception capabilities through cell site simulator upgrades. Last September, for example, in response to our records request, the Baltimore County Police released a redacted 2012 purchase order, showing the department had acquired a redacted device from Digital Receiver Technology, a subsidiary of Boeing. The device is likely a "Dirtbox" cell site simulator, given that these are the only kinds of Digital Receiver Technology devices CityLab inquired about. Dirtboxes are far more powerful than ordinary cell site simulators and have been used by the NSA to intercept tens of millions of communications in France, according to freelance reporter Ali Winston in *Reveal*. They can be mounted on planes to track ten thousand cellphones at once or to capture calls and text messages from hundreds of cellphones at the same time. It is unclear if Baltimore County police use their DRT tool in a similar way, but the department's aviation unit does have helicopters in which a Dirtbox could be mounted. (The department did not respond to CityLab inquiries about its DRT surveillance tool, and DRT spokesperson Meghan McCormick said they could not comment on CityLab's request for information.)



(Katie Martin, The Atlantic)

The records also show several of the departments have acquired other tools to increase the types of phones they can intercept, improve the range of their interceptions, and sharpen the precision of their tracking.

At least eleven departments have purchased other brands of cell site simulators from Harris Corporation, which can capture the phone locations, call logs, and text logs of anyone—criminal suspect, protester, or random bystander—within roughly 200 meters of their deployment, depending on the model. Over 2012 to 2014, for example, Baltimore, Boston, Milwaukee, and Phoenix police each spent between $60,000 and $154,000 to upgrade older cell site simulator models to the company's Hailstorm device, which can intercept more secure 4G phones. The documents show that all four of these departments have also purchased Harris "Harpoon" devices, which amplify the signals of cell site simulators' interceptions. Harris, a Florida-based defense contractor, accounted for over $3.2 million of the disbursements released in the documents. (Harris spokesperson Jim Burke declined to comment for this article.)

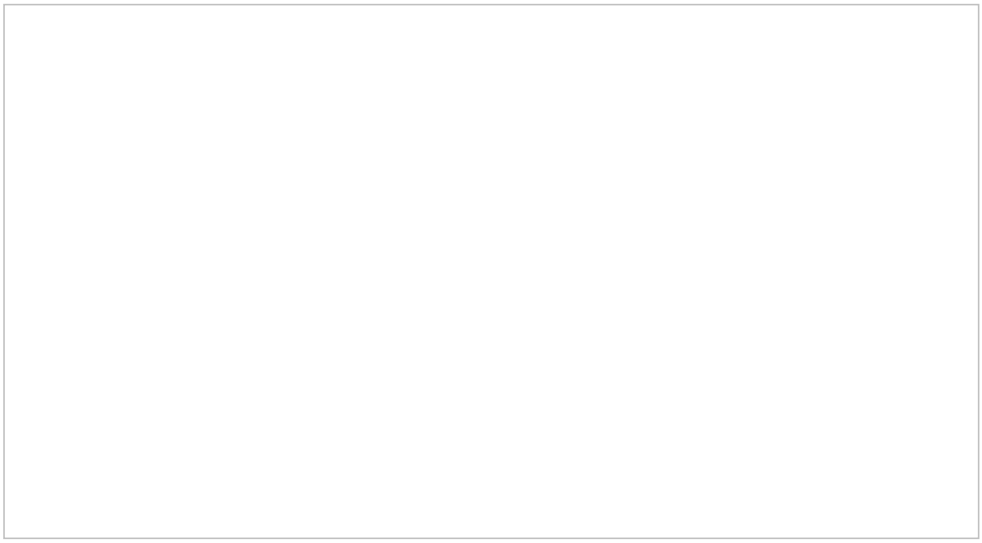
Some departments are also opting for cellphone trackers that are even more precise and covert than cell site simulators. A 2012 Fort Worth police invoice and accompanying quote shows the department acquired two hand-held electronic tracking devices: KeyW Corporation's Quasimodo and Jugular3. These tools track can help authorities locate target phones in crowds or in large buildings, and are very useful in combination with cell site simulators like the Hailstorm, which cannot locate target phones as precisely. "The latest Hailstorm Stingray is used for locating a specific building, but the hand held device can get you close to the right room or apartment," says Mike Katz-Lacabe, a privacy activist with the The Center for Human Rights and Privacy.

These trackers' passive design, only measuring radio signals, also means they can never be detected. As Scott Schober, a cell tracking manufacturer, told the Wall Street Journal, "A lot of the guys using it are saying, 'I don't have to tell anyone I'm using it ... because your device is completely passive, so I'm not getting into any privacy issues.'" A redacted 2013 LAPD document suggests the force also has a handheld passive tracking device.

Extraction: A lifetime of data moves from your pocket to a police lab

The records show that at least nineteen police departments acquired cellphone extraction devices, which allow police to crack open locked devices and collect vast amounts of phone data, such as call logs, emails, social media messages, time-stamped past location data, and even deleted texts and photos—without any assistance from cellphone companies. All nineteen of these departments bought extraction devices made by the Israeli firm Cellebrite, whose various versions of the "Universal Forensic Extraction Device" allow cops to scoop up both data immediately visible on the phone and that which has been deleted or hidden. Police spent nearly $745,000 on such tools, which are far less expensive than cellphone interception devices, and thus more accessible to

smaller departments. As Joseph Cox revealed at Motherboard, numerous state police agencies have also purchased these devices.



(Katie Martin, The Atlantic)

The records also suggest these Cellebrite products enable departments to go far beyond the simple collection of data contained within phones. The Baltimore, Seattle, Oklahoma City, Jacksonville, Kansas City, Louisville, Tucson, and Miami police departments' Cellebrite "Pro Series" purchases all appear to include the firm's Cloud Analyzer tool, which extracts "private-user cloud data" by "utilizing login information extracted from the mobile device." According to Cellebrite, in some cases cloud data does not only include communications on platforms like Facebook and Instagram, but also individuals' "timestamped movements minute by minute," based on on private Google Location History collected from Google cloud servers.

Cellebrite did not respond to CityLab's request for an interview, but its blog features testimonials from police, who praise the devices' efficiency.

Some activists contend that past experiences suggest similar tools have been used to extract information from their phones. M.J. Williams, an attorney who is active in the Black Lives Matter movement in New York City, says that she suspects police may have extracted information from her phone during an arrest at a protest last September. "While we we're in handcuffs waiting for transport to the precinct, a white shirt [a senior officer] took my phone out of my pocket and took the phones of four others," says Williams. "After leaving for a while, he put my phone back in my bag before we went to the precinct. Three hours later when I finally got access to my phone to call my attorney, I didn't have to put in any password. It was already open."

Williams doesn't know what, if anything, police may have done with her phone, but she still feels uneasy. "It was shocking that it appeared as though my phone had been tampered with," she says. "There couldn't have been a warrant because it was done immediately after an arrest. I don't know what they've gotten."

Similar concerns about the use of cellphone extraction devices abound across the country. Some legal advocates, for example, worry the recent decision by Washington, D.C., police to hold phones of activists, lawyers, and journalists arrested during the Trump inauguration protests for "evidence" may expose sensitive source and client communications to police.

An ocean of data—and few rules about what to do with it

As these military-grade spy tools pour down into local police departments across the country, legal experts are concerned that their use isn't in keeping with individuals' due process rights. Law enforcement practices vary dramatically across the country. In 2014, the U.S. Supreme Court unanimously ruled that police could not extract data from an arrested individual's cellphone without obtaining a warrant. But the ruling itself did not give clear guidance on how broad police warrant requests could be designed, and such decisions are still left up to law enforcement discretion in many cases.

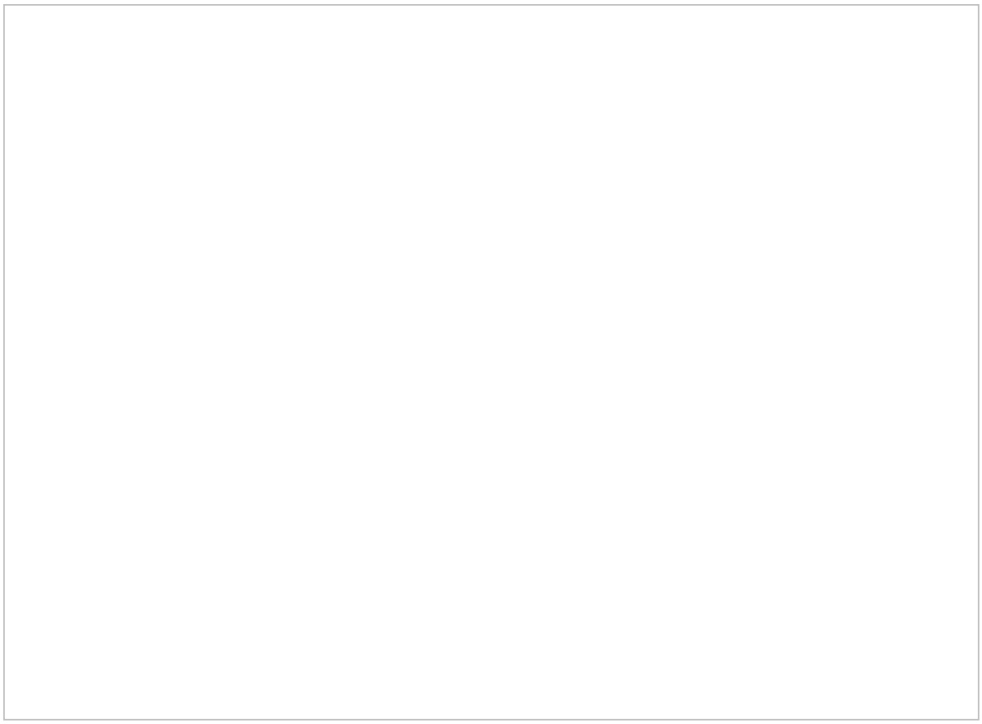
> "Technology is supposed to not have all the bad optics of racial profiling. But this is a way that profiles people by where they live, which is essentially by race."

And with interception of cellphone data, the picture is even murkier. Given the dragnet nature of cell site simulator interceptions, federal agencies like the Department of Homeland Security and the Department of Justice and a few states, such as California, Washington, Virginia, Minnesota, Maryland, and Utah have required police obtain a search warrant before deployments. But police agencies in other states continue to intercept cell data after presenting judges with a pen register application, a court order whose standard is lower than that of a search warrant. Authorities need only show that captured information will be "relevant to an ongoing criminal investigation." Civil liberties advocates argue this lower standard is particularly troubling, given cell site simulators' interceptions of "innocent" nearby phones in the process.

More opaque still is what happens to all this data, extracted or intercepted, once police have it. Michael Price, counsel at the NYU School of Law's Brennan Center, says that some courts have not placed any explicit limits on how long intercepted data can be retained after police extraction for forensic analysis. "The policies are not uniform," he says. "There is a Department of Justice guidance on retention of data from cell site simulators, but state or local policies may be very different."

The documents CityLab obtained indicate some police departments are acquiring software to build up large surveillance databases, based, in part, on

data captured by cellphone interception and extraction devices. In 2012, the Fort Worth police, for example, bought servers and software from a Nebraska company called Pen-Link that enables police to store and organize intercepted cellphone metadata, such as call logs and locations, in computer databases. The Fort Worth Police Department, which secured the acquisition using a DHS Homeland Security Grant program, declined CityLab's request for interview on its use of Pen-Link, suggesting we file another public records request. And Pen-Link did not respond to CityLab's request for comment. But publicly available literature on Pen-Link shows that its products can store and process large amounts of intercepted metadata, allowing officers to create visualizations of individuals' social networks and geolocated calling patterns.



An image from a Cellebrite product brochure. (Miami Police Department)

Police departments are also linking together hundreds of people at a time using data captured in cellphone extraction operations. As with Pen-Link, departments that have Cellebrite's Link Analysis, such as the Miami Police Department, can also create network maps based on individuals' call and text log histories. Cellebrite's Link Analysis can also create timelines of all extracted communications between two or more people, including call logs, text messages, and mutual locations. Such data analysis operations, which would have taken police weeks in the past, can now be accomplished with just a few clicks.

Raymond Foster, a former Los Angeles Police Department lieutenant and police technology expert, says police are inclined to gather as much data as possible, even information from people whose phones just happened to be caught up in a nearby interception operation. "For a specific crime, the data gives you leads on witnesses and suspects by looking at who made the cellphone calls nearby," says Foster. "Your phone geolocates you... You have a little machine that is constantly communicating tons of information about you."

But such a broad approach to intelligence gathering, critics say, puts some people under suspicion simply for living in a neighborhood near a suspected crime, or for knowing someone whose phone has been searched. "They are essentially using a dragnet approach to figure out who they are going to go after," says Josmar Trujillo, a writer and anti-police brutality activist in New York City. "The turn towards technology is supposed to not have all the bad optics of racial profiling and not be prone to human bias, but this is obviously a way that profiles people by where they live, which is essentially by race."

Surveillance fears in the Trump era

How far could locally captured data travel? According to the records released by the department, Fort Worth's data-organizing products are being used "as a regional asset for surrounding local and state agencies." News reports suggest that departments in Virginia and Washington are sharing intercepted data through joint access to Pen-Link software and servers. Pen-Link's product guides point out that law enforcement can use its software to import and export intercepted data to and from national intelligence databases, operated by federal law enforcement agencies who also use Pen-Link, such as the Drug Enforcement Administration, the Federal Bureau of Investigation, and U.S. Immigration and Customs Enforcement.

The distribution of local police data to federal agencies could be crucial for ICE and FBI officials seeking to identify the networks and track the locations of groups facing extra scrutiny from the Trump administration, such as undocumented immigrants and Muslim Americans. CityLab made numerous inquiries to the Department of Homeland Security about its data sharing policies with local police departments, but DHS official Shauntece Long told CityLab that any information requested about ICE's privacy policies on this matter would have to be sought through a FOIA request, which CityLab has since filed.

Mike German, a former FBI agent and now a fellow with the Brennan Center's Liberty and National Security Program, says that federal law enforcement officials are able to access locally captured police data, both through official and informal sharing channels. "They can literally be looking over someone's shoulder to get what they need," says German, pointing to the fact that DHS, FBI, and local police officials sometimes work under the same roof at DHS-organized fusion centers.

Neema Singh Guliani, a legislative counsel for the ACLU on privacy and technology issues, says this data sharing may play a role in the administration's immigration enforcement plans. "You're going to have states and localities increasingly sharing sensitive information—where somebody is, who they know, what their social networks are—not just with each other, but also with the federal government," says Guliani. "If you are a targeted DACA recipient, will ICE use it to target your social network because some of those are assumed to be undocumented? These are mass, dragnet surveillance techniques, originally

designed to be for national security purposes overseas, not domestic immigration enforcement."

As German notes, cellphone tracking can be tremendously effective on otherwise law-abiding targets. "Criminals tend to try and make tracking their data more difficult, so this kind of mass collection of telephony data will more easily find our political activists, our civil society leaders, and just regular people," he says. "If the courts—if the public—knew how powerful these tools were, they would move to restrict their use."

About the Author

George Joseph is an editorial fellow at CityLab, originally from Denton, Texas. He covers policing, surveillance, and criminal justice systems.

ALL POSTS | @georgejoseph94 | Feed