ACLU
AMERICAN CIVIL LIBERTIES UNION

FOIA Documents Reveal Massive DEA Program to Record American's Whereabouts With License Plate Readers

January 26, 2015
By Bennett Stein, ACLU Speech, Privacy, and Technology Project & Jay Stanley, Senior Policy Analyst, ACLU Speech, Privacy & Technology Project at 7:15pm

(Updated below)

The Drug Enforcement Administration has initiated a massive national license plate reader program with major civil liberties concerns but disclosed very few details, according to new DEA documents obtained by the ACLU through the Freedom of Information Act.

The DEA is currently operating a National License Plate Recognition initiative that connects DEA license plate readers with those of other law enforcement agencies around the country. A Washington Post headline proclaimed in February 2014 that the Department of Homeland Security had cancelled its "national license-plate tracking plan," but all that was ended was one Immigrations and Customs Enforcement solicitation for proposals. In fact, a government-run national license plate tracking program already exists, housed within the DEA. (That's in addition to the corporate license plate tracking database run by Vigilant Solutions, holding billions of records about our movements.) Since its inception in 2008, the DEA has provided limited information to the public on the program's goals, capabilities and policies. Information has trickled out over the years, in testimony here or there. But far too little is still known about this program.

In 2012, the ACLU filed public records requests in 38 states and Washington, D.C. seeking information about the use of automatic license plate readers. Our July 2013 report, You Are Being Tracked, summarized our findings with regard to state and local law enforcement agencies, finding that the technology was being rapidly adopted, all too often with little attention paid to the privacy risks of this powerful technology. But in addition to filing public records requests with state agencies, the ACLU also filed FOIA requests with federal agencies, including the DEA.

The new DEA records that we received are heavily redacted and incomplete, but they provide the most complete documentation of the DEA's database to date. For example, the DEA has previously testified that its license plate reader program began at the southwest border crossings, and that the agency planned to gradually increase its reach; we now know more about to where it has grown. The DEA had previously suggested that "other sources" would be able to feed data into the database; we now know about some of the types of agencies collaborating with the DEA.

The documents uncovered by our FOIA request provide additional details, but their usefulness is limited by the DEA's decision to provide only documents that are undated or years old. If the DEA's collection of location information is as extensive as the agency has suggested in its limited comments to legislatures, the public deserves a more complete and comprehensive explanation than the smattering of records we have obtained can provide.

These records do, however, offer documentation that this program is a major DEA initiative that has the potential to track our movements around the country. With its jurisdiction and its finances, the federal

government is uniquely positioned to create a centralized repository of all drivers' movements across the country — and the DEA seems to be moving toward doing just that. If license plate readers continue to proliferate without restriction and the DEA holds license plate reader data for extended periods of time, the agency will soon possess a detailed and invasive depiction of our lives (particularly if combined with other data about individuals collected by the government, such as the DEA's recently revealed bulk phone records program, or cell phone information gleaned from U.S. Marshals Service's cell site simulator-equipped aircraft). Data-mining the information, an unproven law enforcement technique that the DEA has begun to use here, only exacerbates these concerns, potentially tagging people as criminals without due process.

Some major findings from the documents

The National License Plate Recognition Initiative includes a massive database containing data from both DEA-owned automatic license plate readers *and* other readers. Among the findings from the FOIA documents:

- At the time of an undated slideshow, the DEA had deployed at least 100 license plate readers across the United States (eight states are identified: California, Arizona, New Mexico, Texas, Florida, Georgia, Nevada, and New Jersey). A 2010 document also explains that the DEA had by then set up 41 plate reader monitoring stations throughout Texas, New Mexico, and California.
- The DEA is also inviting federal, state, and local law enforcement agencies around the country to contribute location information to the database. For example, the documents show that local and regional law enforcement systems in Southern California's San Diego and Imperial Counties and New Jersey all provide data to the DEA. The program was "officially opened" to these partners in May 2009. Other agencies are surely partnering with the DEA to share information, but these agreements are still secret, leaving the public unable to know who has their location information and how it is being used.
- Customs and Border Patrol (CBP) is one of the federal agencies that has shared information with the DEA. An undated Memorandum of Understanding explains that the agencies will, "at regular intervals," provide each other license plate reader data. It also authorizes the two agencies to further share each other's data with other federal, state, and local law enforcement and prosecutors as well as to "intelligence, operations, and fusion centers." This is a lot of location points. CBP collects "nearly 100 percent of land border traffic," which amounts to over 793.5 million license plates between May 2009 and May 2013, according to CBP's response to our FOIA request.
- Additionally, any federal, state, or local law enforcement agent vetted by the DEA's El Paso Intelligence Center can conduct queries of the database, located in Merrifield, Va.
- The same undated slideshow suggests that there were over 343 million records in the database at the date of the slide's publication (due to redactions, it is impossible to confirm that date from this document).
- The unredacted parts of the documents and news reports suggest that the DEA recently changed its retention policy to six months for non-hit data. While this is an improvement from previous statements of DEA retention policy, it is still far too long. The government should not collect or retain information revealing the movements of millions of people accused of no crime. But even that long retention period is only meaningful if it comes with strict rules limiting data use, sharing, and access. Like its retention policy, the DEA should make these policies public.

- The DEA says that the National License Plate Recognition Initiative targets roadways that the agency believes are commonly used for contraband transport. But it's not clear what this means or what it is based on. Every highway in the United States must be regularly used for contraband transport. Is the DEA using this undefined mandate to target people of color? Without more information from the DEA, we have no idea.

- One DEA document references steps needed to ensure the program meets its goals, "of which asset forfeiture is primary." Asset forfeiture has been in the news a lot lately, criticized as a widely abused law enforcement tactic that doesn't advance public safety but simply enriches police and federal agencies.

- The program also apparently data mines license plate reader data "to identify travel patterns." The extent of this data mining is unknown. Is the DEA running all of our license plate reads through a program to predict our likelihood of committing a crime? Are we all suspects if we drive on a certain road? What else does the DEA think it knows about us just from the collection and analysis of our locations via license plate reader data?

More answers are needed

The DEA's license plate reader programs raise serious civil liberties concerns, and the agency should be open about what it is doing so that those activities can be subject to public debate. Among other questions, the agency should answer these:

- How many license plate readers does DEA currently own and operate? In which states? And, how much did it spend on these license plate readers?
- Which policies govern the use of the license plate readers? Which policies govern the use of the license plate reader database? Has the agency done a Privacy Impact Assessment on these programs?
- How many license plate reader hits have resulted in arrest and prosecution of a serious crime? How many license plate reader hits have not correlated to an alert upon further investigation (a "mis-hit")?
- From which local, state, and tribal law enforcement agencies does the DEA receive license plate reader data?
- Which additional agencies does the DEA partner with? How many people have been approved to conduct queries of the DEA database?
- Has the DEA used or attempted to use Vigilant Solution's National Vehicle Location Service or a similar privately-run license plate reader database? Does DEA combine information from its own database with records in Vigilant's, creating a mega-database in a public-private surveillance partnership?

As is the case with most police and federal law enforcement spy technologies, license plate tracking programs have flown under the radar of courts and legislators for far too long, silently collecting records about ordinary Americans in the cover of secrecy. When programs are secret, we have no way of challenging them or ensuring they conform with our values and the law. Before accountability comes transparency. Over the coming weeks, we will continue to release records documenting the federal government's significant investment in automatic license plate readers and its unregulated and largely unseen location tracking programs.

Here are the documents discussed in this piece (we also link to them above):

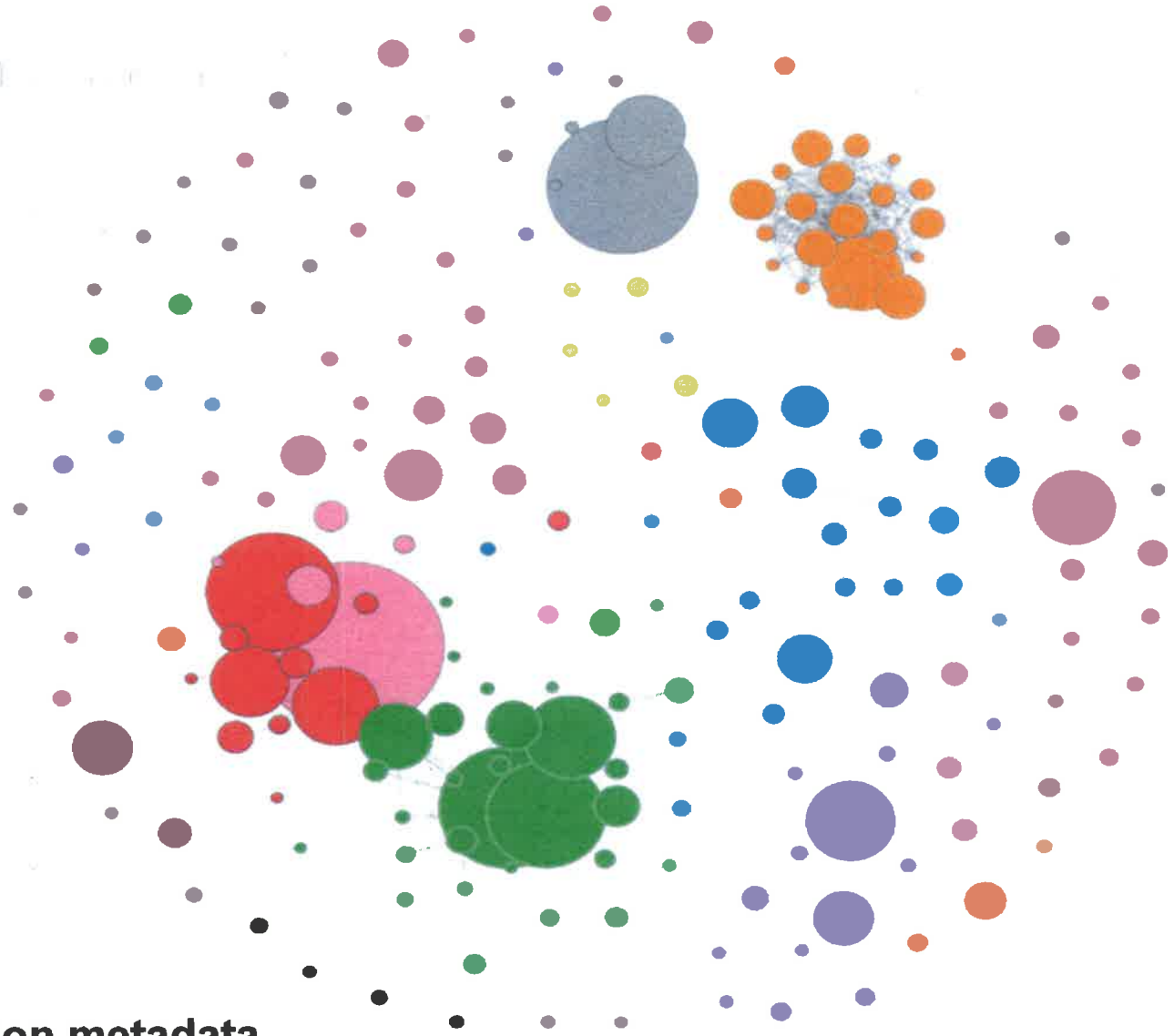
2010 DEA Email
Undated slideshow
October 2011 DEA email
April/May 2010 DEA emails
May 2010 DEA emails
March 2014 DEA Response to ACLU FOIA Request, assorted emails
October 2011 DEA emails
January 2014 CBP Response to ACLU FOIA Request

Update (1/28/15):

EFF's Dave Maass alerted us that he has found additional documentation of the DEA's license plate reader infrastructure. The document details a proposed contract to provide maintenance and support for "currently deployed" license plate readers.

The system that is described includes: 53 fixed cameras, 24 barrel cameras, and 47 license plate reader trailers. These cameras are distributed in 12 locations in East Texas, 21 location in West Texas and New Mexico, 6 locations in Arizona, and 6 locations in California.

It is unclear what the status of the contract is. It is also unclear if this contract would cover all of the cameras in the region, and whether there are other regions with many cameras. As we point out above, the public should not be forced to guess the scope and details of this program just based on clues left around the internet or left unredacted in FOIA documents.



Immersion metadata

Sample gmail account – 8.3 years.

The New York Times http://nyti.ms/1GaPGZu

TECHNOLOGY

A Police Gadget Tracks Phones? Shhh! It's Secret

By MATT RICHTEL MARCH 15, 2015

A powerful new surveillance tool being adopted by police departments across the country comes with an unusual requirement: To buy it, law enforcement officials must sign a nondisclosure agreement preventing them from saying almost anything about the technology.

Any disclosure about the technology, which tracks cellphones and is often called StingRay, could allow criminals and terrorists to circumvent it, the F.B.I. has said in an affidavit. But the tool is adopted in such secrecy that communities are not always sure what they are buying or whether the technology could raise serious privacy concerns.

The confidentiality has elevated the stakes in a longstanding debate about the public disclosure of government practices versus law enforcement's desire to keep its methods confidential. While companies routinely require nondisclosure agreements for technical products, legal experts say these agreements raise questions and are unusual given the privacy and even constitutional issues at stake.

"It might be a totally legitimate business interest, or maybe they're trying to keep people from realizing there are bigger privacy problems," said Orin S. Kerr, a privacy law expert at George Washington University. "What's the secret that they're trying to hide?"

The issue led to a public dispute three weeks ago in Silicon Valley, where a sheriff asked county officials to spend $502,000 on the technology. The Santa Clara County sheriff, Laurie Smith, said the technology allowed for locating cellphones — belonging to, say, terrorists or a missing person. But when asked for details, she offered no technical specifications and acknowledged she had not seen a product demonstration.

Buying the technology, she said, required the signing of a nondisclosure agreement.

"So, just to be clear," Joe Simitian, a county supervisor, said, "we are being asked to spend $500,000 of taxpayers' money and $42,000 a year thereafter for a product for the name brand which we are not sure of, a product we have not seen, a demonstration we don't have, and we have a nondisclosure requirement as a precondition. You want us to vote and spend money," he continued, but "you can't tell us more about it."

The technology goes by various names, including StingRay, KingFish or, generically, cell site simulator. It is a rectangular device, small enough to fit into a suitcase, that intercepts a cellphone signal by acting like a cellphone tower.

The technology can also capture texts, calls, emails and other data, and prosecutors have received court approval to use it for such purposes.

Cell site simulators are catching on while law enforcement officials are adding other digital tools, like video cameras, license-plate readers, drones, programs that scan billions of phone records and gunshot detection sensors. Some of those tools have invited resistance from municipalities and legislators on privacy grounds.

The nondisclosure agreements for the cell site simulators are overseen by the Federal Bureau of Investigation and typically involve the Harris Corporation, a multibillion-dollar defense contractor and a maker of the technology. What has opponents particularly concerned about StingRay is that the technology, unlike other phone surveillance methods, can also scan all the cellphones in the area where it is being used, not just the target phone.

"It's scanning the area. What is the government doing with that information?" said Linda Lye, a lawyer for the American Civil Liberties Union of Northern California, which in 2013 sued the Justice Department to force it to disclose more about the technology. In November, in a response to the lawsuit, the government said it had asked the courts to allow the technology to capture content, not just identify subscriber location.

The nondisclosure agreements make it hard to know how widely the technology has been adopted. But news reports from around the country indicate use by local and state police agencies stretching from Los Angeles to Wisconsin to New York, where the state police use it. Some departments have used it for several years. Money for the devices comes from individual agencies and sometimes, as in the case of Santa Clara County, from the federal government through Homeland Security grants.

Christopher Allen, an F.B.I. spokesman, said "location information is a vital component" of law enforcement. The agency, he said, "does not keep repositories of cell tower data for any purpose other than in connection with a specific investigation."

A fuller explanation of the F.B.I.'s position is provided in two publicly sworn affidavits about StingRay, including one filed in 2014 in Virginia. In the affidavit, a supervisory special agent, Bradley S. Morrison, said disclosure of the technology's specifications would let criminals, including terrorists, "thwart the use of this technology."

"Disclosure of even minor details" could harm law enforcement, he said, by letting "adversaries" put together the pieces of the technology like assembling a "jigsaw puzzle." He said the F.B.I. had entered into the nondisclosure agreements with local authorities for those reasons. In addition, he said, the technology is related to homeland security and is therefore subject to federal control.

In a second affidavit, given in 2011, the same special agent acknowledged that the device could gather identifying information from phones of bystanders. Such data "from all wireless devices in the immediate area of the F.B.I. device that subscribe to a particular provider may be incidentally recorded, including those of innocent, nontarget devices."

But, he added, that information is purged to ensure privacy rights.

In December, two senators, Patrick J. Leahy and Charles E. Grassley, sent a letter expressing concerns about the scope of the F.B.I.'s StingRay use to Eric H. Holder Jr., the attorney general, and Jeh Johnson, the secretary of Homeland Security.

The Harris Corporation declined to comment, according to Jim Burke, a company spokesman. Harris, based in Melbourne, Fla., has $5 billion in annual sales and specializes in communications technology, including battlefield radios.

Jon Michaels, a law professor at the University of California, Los Angeles, who studies government procurement, said Harris's role with the nondisclosure agreements gave the company tremendous power over privacy policies in the public arena.

"This is like the privatization of a legal regime," he said. Referring to Harris, he said: "They get to call the shots."

For instance, in Tucson, a journalist asking the Police Department about its StingRay use was given a copy of a nondisclosure agreement. "The City of Tucson

shall not discuss, publish, release or disclose any information pertaining to the product," it read, and then noted: "Without the prior written consent of Harris."

The secrecy appears to have unintended consequences. A recent article in The Washington Post detailed how a man in Florida who was accused of armed robbery was located using StingRay.

As the case proceeded, a defense lawyer asked the police to explain how the technology worked. The police and prosecutors declined to produce the machine and, rather than meet a judge's order that they do so, the state gave the defendant a plea bargain for petty theft.

At the meeting in Santa Clara County last month, the county supervisors voted 4 to 1 to authorize the purchase, but they also voted to require the adoption of a privacy policy.

(Sheriff Smith argued to the supervisors that she had adequately explained the technology and said she resented that Mr. Simitian's questioning seemed to "suggest we are not mindful of people's rights and the Constitution.")

A few days later, the county asked Harris for a demonstration open to county supervisors. The company refused, Mr. Simitian said, noting that "only people with badges" would be permitted. Further, he said, the company declined to provide a copy of the nondisclosure agreement — at least until after the demonstration.

"Not only is there a nondisclosure agreement, for the time being, at least, we can't even see the nondisclosure agreement," Mr. Simitian said. "We may be able to see it later, I don't know."

A version of this article appears in print on March 16, 2015, on page A1 of the New York edition with the headline: A Police Gadget Tracks Phones? Shhh! It's Secret.

UFED TOUCH ULTIMATE

All-inclusive Mobile Forensic Solution

Cellebrite's UFED Touch Ultimate is an innovative, high performing mobile forensic solution. With its intuitive GUI and easy-to-use touch screen, the UFED Touch Ultimate enables the physical, file system, and logical extractions of all data, passwords, included deleted data, from the widest range of mobile phones, memory cards, portable GPS devices and tablets.

The UFED Touch Ultimate includes:

- **UFED Physical Analyzer**: Powerful application for decoding, analysis and reporting
- **UFED Phone Detective**: Instant mobile identification application
- **UFED Reader**: Free application for sharing analysis reports with any authorized personnel. No license or installation required.

The UFED Touch Ultimate is a mission-ready solution for investigations in the field or lab and available in both standard and ruggedized versions.

The UFED Touch Ultimate Advantage

Setting the industry standard for mobile data forensic solutions, the UFED Touch Ultimate provides investigators with maximum capabilities:

- Unmatched support for the widest range of mobile devices
- Physical extraction from BlackBerry® devices running OS 4-7. Exclusive decoding: BBM data, apps, emails, Bluetooth, calendar entries etc.
- Widest support for Apple devices running iOS3+
- Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices including Samsung Galaxy S family , HTC, LG, Motorola and more
- Password extraction and removal on selected devices
- Physical extraction from Nokia BB5 devices – password extraction is enabled from selected devices
- File system extraction from any device running Windows phone 7.5 and 8 including Nokia, HTC, Samsung, Huawei and ZTE
- Data extraction from portable GPS devices and decoding of the TomTom® trip-log
- Proprietary technology and bootloaders ensure forensically sound extractions
- Complete field-ready operational kit – compact tip connectors with 4 master cables for extraction and charging during usage
- The most powerful solution for phones with Chinese chipsets
- Frequent software updates to ensure compatibility with new phones as they enter the market

Mission-Ready

The all-inclusive standard and ruggedized mobile forensic kit contains a full range of peripherals and accessories for successful investigations in the field or lab. Complete with lightweight data cables, phone connector tips, an embedded work shelf in the ruggedized case, integrated long-life battery and external hard drive make mobile investigations quicker, easier and more efficient.

RUGGEDIZED KIT

STANDARD KIT

WHAT IS XRY?

XRY is a software application designed to run on the Windows operating system which allows you to perform a secure forensic extraction of data from a wide variety of mobile devices, such as smartphones, gps navigation units, 3G modems, portable music players and the latest tablet processors such as the iPad.

Extracting data from mobile / cell phones is a specialist skill and not the same as recovering information from computers. Most mobile devices don't share the same operating systems and are proprietary embedded devices which have unique configurations and operating systems. What does that mean in terms of getting data out of them? Well in simple terms, it means it is very difficult to do.

XRY has been designed and developed to make that process a lot easier for you, with support for over 13,000 different mobile device profiles and over 500 smartphone app versions. We supply a complete solution to get you what you need and the software guides you through the process step by step to make it as easy as possible.

Multiple Extraction Wizard

The latest version of XRY includes the Multiple Extraction Wizard as standard. This functionality allows users to examine 3 different mobile devices all at the same time, to speed up the time taken to perform examinations and ensure you make the best use of your time.

There are several different XRY variants available depending upon your needs:

XRY Logical

This is our most established product designed to perform a 'logical' extraction of data from the mobile device.

What this means is that we communicate with the operating system on the device and request information from the system. In general terms this will allow you to recover most of the live data from the device.

It is effectively the automated equivalent of manually examining each available screen on the device yourself and recording what is displayed.

XRY Logical is by far our most popular product, useful for the vast majority of our customers and their tasks.

XRY Physical

Is more advanced – it allows you to perform a 'physical' extraction from a mobile device. Where we recover all available raw data stored in the device. Typically this is performed by bypassing the operating system and this offers you the opportunity to go deeper and recover deleted data from the device.

A physical extraction is separated out into two distinct stages, the initial 'dump' whereby the raw data is recovered from the device and then the second stage 'decode' – where XRY can automatically reconstruct the data into something meaningful; such as a deleted SMS without the need for manual carving of data.

XRY Physical is particularly useful when faced with a GSM mobile phone without a SIM Card, or with security locked devices.

XRY Complete

This is our top of the range solution combining the best of both worlds with XRY Logical and XRY Physical in one complete package, hence the name.

With XRY Complete you will be able to perform both logical and physical extractions from a device, giving you the best possible opportunity to recover all the available data from a mobile device. Allowing you to compare the results between the different recovery methods.

This system is supplied with all the necessary hardware from both the Logical and the Physical systems to ensure you have everything you need to do complete the task.