LAW & DISORDER —

FBI would rather prosecutors drop cases than disclose stingray details

New documents released by NYCLU shed light on Erie County's use of spying tool.

CYRUS FARIVAR - 4/7/2015, 5:35 PM

Cubmundo

Not only is the FBI actively attempting to stop the public from knowing about stingrays, it has also forced local law enforcement agencies to stay quiet even in court and during public hearings, too.

FURTHER READING
New York county sheriff must give up stingray records, judge orders

An FBI agreement, published for the first time in unredacted form on Tuesday, clearly demonstrates the full extent of the agency's attempt to quash public disclosure of information about stingrays. The most egregious example of this is language showing that the FBI would rather have a criminal case be dropped to protect secrecy surrounding the stingray.

Relatively little is known about how, exactly, stingrays, known more generically as cell-site simulators, are used by law enforcement agencies nationwide, although new documents have recently been released showing how they have been purchased and used in some limited instances. Worse still, cops have lied to courts about their use. Not only can stingrays be used to determine location by spoofing a cell tower, they can also be used to intercept calls and text messages. Typically, police deploy them without first obtaining a search warrant.

Ars previously published a redacted version of this document in February 2015, which had been acquired by the *Minneapolis Star Tribune* in December 2014. The fact that these two near-identical documents exist from the same year (2012) provides even more evidence that this language is boilerplate and likely exists in other agreements with other law enforcement agencies nationwide.

The new document, which was released Tuesday by the New York Civil Liberties Union (NYCLU) in response to its March 2015 victory in a lawsuit filed against the Erie County Sheriff's Office (ECSO) in Northwestern New York, includes this paragraph:

> In order to ensure that such wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation and use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including but not limited to: press releases, in court documents, during judicial hearings, or during other public forums or proceedings.

In the version of the document previously obtained in Minnesota, the rest of the sentence after the phrase "limited to" was entirely redacted.

FURTHER READING
California bill requires warrant for stingray use

Mariko Hirose, a NYCLU staff attorney, told Ars that she has never seen an agreement like this before.

"This seems very broad in scope and undermines public safety and the workings of the criminal justice system," she said.

Your tax dollars at work

The FBI letter also explicitly confirms a practice that some local prosecutors have engaged in previously, which is to drop criminal charges rather than disclose exactly how a stingray is being used. Last year, prosecutors in Baltimore did just that during a robbery trial—there, Baltimore Police

Detective John L. Haley cited a non-disclosure agreement, and he declined to describe in detail how he obtained the location of the suspect.

The newly revealed sections state:

> 7) The Erie County Sheriff's Office shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology including, but not limited to, during pre-trial matters, in search warrants, and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI.
>
> 8) In addition, the Erie County Sheriff's Office will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (beyond the evidentiary results obtained through the use of the equipment/technology), if using or providing such information would potentially or actually compromise the equipment/technology. This point supposes that the agency has some control or influence over the prosecutorial process. Where such is not the case, or is limited so as to be inconsequential, it is the FBI's expectation that the law enforcement agency identify the applicable prosecuting agency, or agencies, for inclusion in this agreement.

"Why is it spending over $350,000 on this when prosecutions might have to be dismissed?" Hirose added, referring to the approximate total amount that the ECSO spent on the hardware and related software and training.

Everyone's gone quiet

In response to a media inquiry by Ars, Christopher Allen, an FBI spokesman, wrote: "As you know I am not able to comment beyond what I have previously provided."

FURTHER READING
To explain stingrays, local cops cribbed letter pre-written by FBI

Last year, Allen sent Ars an affidavit outlining the agency's position on why so little information has been publicly disclosed.

"The FBI routinely asserts the law enforcement sensitive privilege over cell site simulator equipment because discussion of the capabilities and use of the equipment in court would allow criminal defendants, criminal enterprises, or foreign powers, should they gain access to the items, to

determine the FBI's techniques, procedures, limitations, and capabilities in this area," Bradley Morrison, chief of the tracking technology unit at the FBI, stated in the affidavit.

"This knowledge could easily lead to the development and employment of countermeasures to FBI tools and investigative techniques by subjects of investigations and completely disarm law enforcement's ability to obtain technology-based surveillance data in criminal investigations."

The Erie County Sheriff's Office did not immediately respond to Ars' request for comment. Meanwhile, local legislators have not yet had adequate time to review the new documents.

"A year ago, when the issue was first brought to light, the equipment was discussed in the Legislature's Committee process with the Sheriff's Office," Jessica O'Neil, a spokesman for the Majority Caucus of the Erie County Legislature, told Ars by e-mail.

"The members of the Legislature have stated that the privacy of residents should be protected and will review the documents fully before deciding if any action can or should be taken."

The Erie County public defender also did not immediately respond.

UPDATE Wednesday 12:08pm CT: Kevin Stadelmaier, the chief attorney with the Criminal Defense Unit at Legal Aid Buffalo, the local public defender, told Ars he had never heard of stingrays prior to this case and would be investigating further.

"The Erie County Sheriff's Office is basically subverting the Fourth Amendment," he said.

"The point of the matter is not only are they pulling info off people they're looking for, but the same technology could be used against people that are not subject to criminal investigations."

Authorities only sought court permission once, out of 47 times

Finally, the trove of documents released Tuesday includes a June 2014 memo from Chief Scott Patronik to all members of the "Cellular Phone Tracking Team." It states: "Cellular tracking equipment is to be used for official law enforcement purposes only."

FURTHER READING
Chicago owes lawyers over $120,000 for defense against two stingray cases

In the documentation, officers are also ordered to "describe the legal authority for tracking the cellular phone (exigent circumstances, arrest warrant, court order, etc)," in their police records each time that a stingray is used.

But the list of the 47 instances provided to the NYCLU detailing such usages only specifically mentions one occasion when a pen register was sought—on October 3, 2014 as part of a robbery investigation in Buffalo. Ars has contacted the Erie County Court in an attempt to obtain the pen register application and related court documents.

In the pre-cellphone era, a "pen register and trap and trace order" allowed law enforcement to obtain someone's calling metadata in near-real time from the telephone company. Now, that same data can also be gathered directly by the cops themselves through the use of a stingray. In some cases, police have gone to judges asking for such a device or have falsely claimed the existence of a confidential informant while in fact deploying this particularly sweeping and invasive surveillance tool.

Most judges are likely to sign off on a pen register application not fully understanding that police are actually asking for permission to use a stingray. Under federal law and New York state law, pen registers are granted under a very low standard: authorities must simply show that the information obtained from the pen register is "relevant to an ongoing criminal investigation."

That is a far lower standard than being forced to show probable cause for a search warrant or wiretap order. A wiretap requires law enforcement to not only specifically describe the alleged crimes but also to demonstrate that all other means of investigation have been exhausted or would fail if they were attempted.

Hirose reveled in her organization's judicial win: "Just because the FBI and the ECSO agree that these documents are confidential doesn't mean that they're confidential under the law."

Promoted Comments

Chris FOM / Ars Tribunus Angusticlavius JUMP TO POST

Eventually we're going to find out something really scary about Stingrays. The amount of secrecy they've been shrouded in and the incredible lengths law enforcement at every level is going through to conceal even the smallest detail of their use just doesn't make sense for something that "only" tracks the location of a cell phone or even can intercept what that phone is doing. There's got to be something else at play to explain the extreme secrecy.

7534 posts | registered Jan 26, 2005

Vidi Vici Veni / Ars Centurion JUMP TO POST

> milski wrote:
> So what is the worst case here? Let's say that these are deployed without a warrant and are capable of recording any voice calls, text messages and data exchanged by all cell phones in range. Would that be something deserving the amount of efforts spend on keeping the capability secret? After all, it only seems quite possible that the devices could do any of these, just based on the general description of what they do.What *else* could they possibly do to justify all the secrecy?

How about inject code into the baseband receiver of your phone ?

293 posts | registered Nov 14, 2013