EXHIBIT 3

Politics : Online Rights

FBI E-Mail Shows Rift Over Warrantless Phone Record Grabs

By Ryan Singel 12.20.07

By now it's well known that FBI agents can't always be troubled to get a court order before going after a surveillance target's telephone and internet records. But newly released FBI documents show that aggressive surveillance tactics have even caused friction within the bureau.

"We deal mostly with the fugitive squad here, and, like in many other offices, these guys have a reputation for cutting corners," a surveillance specialist at the FBI's Minneapolis field office complained in an internal e-mail last year. "I'm not bashing them; it's the way they do business. Getting a court order is the absolute last step, if they have to.

"Before I had a blowup with a particular agent ... we were constantly asked to call our contacts at service providers to see if we could get various information without having to get a court order," the message continues. "This gets old, believe me. ... Doing this once or twice to help out turns into SOP (standard operating procedure) ... It's expected, and you're criticized as a tech agent if you refuse to do this later on."

The revelation is the second this year showing that FBI employees bypassed court order requirements for phone records. In July, the FBI and the Justice Department Inspector General revealed the existence of a joint investigation into an FBI counter-terrorism office, after an audit found that the Communications Analysis Unit sent more than 700 fake emergency letters to phone companies seeking call records. An Inspector General spokeswoman declined to provide the status of that investigation, citing agency policy.

The June 2006 e-mail (.pdf) was buried in more than 600-pages of FBI documents obtained by the Electronic Frontier Foundation, in a Freedom of Information Act lawsuit.

The message was sent to an employee in the FBI's Operational Technology Division by a technical surveillance specialist at the FBI's Minneapolis field office -- both names were redacted from the documents. The e-mail describes widespread attempts to bypass court order requirements for cellphone data in the Minneapolis office.

Remarkably, when the technical agent began refusing to cooperate, other agents began calling telephone carriers directly, posing as the technical agent to get customer cellphone records.

Federal law prohibits phone companies from revealing customer information unless given a court order, or in the case of an emergency involving physical danger.

The documents are the second batch released by the EFF after winning a Freedom of Information Act lawsuit last May. The first set of documents shed light on the breadth and sophistication of the FBI's national wiretapping system, which is wired into telecom switches around the United States under the terms of the 1994 Communications Assistance for Law Enforcement Act -- a law that was extended to broadband internet switches in May of this year.

The new documents detail how a little-known FBI telephone intercept unit has developed a powerful cellphone tracking technology that agents use to monitor the physical movements of surveillance targets, even on phones that are not GPS equipped.

Originally developed to capture and arrest computer hacker Kevin Mitnick in 1995, the system today relies on a mobile FBI van that has access to a wireless carrier's cell site tracking information in real time. A special surveillance unit called the Wireless Intercept and Tracking Team (WITT) operates the van, using the cell site location to get to the approximate location of the cellphone customer, then uses direction-finding gear to zero in on the target.

The technical agent complained in the e-mail that FBI agents looking for a suspect tend to skip gumshoe investigative techniques in favor of the slick tracking van. "These guys always want to take the WITT vehicle out and drive around half of town (sic) to find the guy," the agent wrote.

The tracking system is part of the FBI's Digital Collection System, or DCS, a suite of software packages used for criminal and intelligence phone taps, which relies on a massive interlinked fiber-optic network that connects surveillance terminals around the country.

In brief, the mobile tracking system works as follows:

1. FBI agents investigating a case prepare a court order saying a cellphone number is likely relevant to an ongoing investigation, and a judge signs off on it.
2. The court order is faxed to a mobile carrier, which then turns on surveillance in its switches, and begins delivering call data and cell site information to the FBI's DCS 3000 software.
3. That software keeps track of which cellphone towers a phone uses or pings. A central FBI database translates a mobile carrier's cell tower code to latitude and longitude coordinates.
4. The software sends the coordinates to the agents and technical personnel in the mobile unit who then drive to the general area. But since cell tower information is not precise, agents in the van use antenna array connected to tracking software to zero in on the cellphone.

The FBI's technology office trumpeted the tracking function of the DCS 3000 software in a letter to the FBI director, boasting that it was used after a December 2005 North Carolina kidnapping to help find the victim unharmed.

Justice Department spokesman Dean Boyd says the department's policy allows the FBI to get cell tower information using under the low legal standard that applies to monitoring the digits a phone customer dials. Under that "pen register" standard, the FBI need only assert that the surveillance is relevant to an investigation -- the target need not be suspected of a crime.

When GPS-level data is wanted, law enforcement agents still need to show probable cause to a judge, said Boyd, who deferred questions about the Minneapolis agent's e-mail to the FBI.

FBI spokesman Paul Bresson cautioned against drawing conclusions from redacted government documents, and claimed that the FBI follows the law. "FBI agents are trained to enforce the law using all available legal tools," Bresson said. "Absent an emergency circumstance involving danger or death or serious physical injury, the FBI does not request, nor do service providers give, any records without a court order."

The FBI tech agent's critical e-mail is best understood in light of the bureau's ongoing courtroom attempts to get cellphone location information without having to show probable cause, according to EFF lawyer Marcia Hofmann.

"For years the government has made dubious legal claims to justify tracking people's locations with minimal oversight," Hofmann said. "These docs show that the government hasn't satisfied its own weak standards in some cases."

Other revelations in the document include:

- National security wiretaps in a Florida investigation captured more than 1,800 phone conversations, and led to 50 international terrorism advisories. Though details are redacted from the document, that case appears to be the so-called Liberty City Seven. Prosecutors initially trumpeted that the seven men were plotting to blow up the Sears Tower, though a government official later admitted the group was "more aspirational than operational." Last week a Florida jury acquitted one man and failed to reach a verdict on the other six.
- In 2006, DCS 5000, the FBI's national security wiretapping software, captured 27,728,675 communication sessions. The document does not define what a "session" consists of. That year the FBI reported winning 2,176 FISA, or Foreign Intelligence Surveillance Act, warrants from a secret court.
- By 2003 one cellphone carrier, Richmond, Virginia-based Triton PCS, was handling some 1,800 subpoenas and court orders a year. With 800,000 customers, that represented one records demand for every 444 customers.
- The FBI uses a Raytheon-developed tool known as the Digital Multimedia Watchdog to record and store phone calls and internet communications between informants and targets of an investigation. That tool can "collect, process and store large amounts of multimedia data, including voice, fax, data and video."
- DCS 3000 -- the FBI's tool for recording the phone numbers a target calls, or is called from -- was set loose on 5,300 phones in 2005, at a cost of $320 per targeted number. Those costs did not include payments to telecoms for the intercepts. The software is maintained by Booz Allen Hamilton and contained more than 490,000 lines of code as of 2005.
- The three software components of the FBI's phone surveillance system cost $38.7 million in 2003 and $39 million in 2004. Computers running these software packages at FBI offices and surveillance locations are connected through a Sprint-run closed fiber-optic network that allows surveillance to continue even when offices are destroyed, as happened during Sept. 11 and Hurricane Katrina.

Quick Links: Contact Us | Login/Register | Newsletter | RSS Feeds | Tech Jobs | Wired Mobile | FAQ | Sitemap

See Also:

Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates
FBI Employees Face Criminal Probe Over Patriot Act Abuse
Threat Level: Monday is Wiretap the Internet Day
Threat Level: AT&T, Verizon: We Obeyed FBI 'Emergency' Requests -- 739 of Them
FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats

Search Wired
Top Stories
GO
Related Topics:

Sitemap | FAQ | Contact Us | WIRED Staff | Advertising | Press Center | Subscription Services | Newsletter | RSS Feeds

Condé Nast Web Sites:

Webmonkey | Reddit | ArsTechnica | Details | Golf Digest | GQ | New Yorker

Subscribe to a | Condé Nast web sites: | International Sites: