EXHIBIT 15

future tense ASU | NEW AMERICA | SLATE

FUTURE TENSE | THE CITIZEN'S GUIDE TO THE FUTURE | OCT. 19 2012 4:00 PM

FBI Accused of Dragging Feet on Release of Info About "Stingray" Surveillance Technology

By Ryan Gallagher

The FBI is reluctant to share information about "stingray" technology

Photo by MANDEL NGAN/AFP/Getty Images

Tracking cell phones by tricking them into operating on a bogus network is a law enforcement tactic shrouded in secrecy. Now the FBI is under pressure to release information about it—but the bureau doesn't want to let go of 25,000 pages of documents on sophisticated cell surveillance technology.

In an Arizona court case last year (*U.S. v. Rigmaiden*), it emerged the FBI had used a "cell-site simulator" in order to track down a suspect. The portable equipment, sometimes described as either an "IMSI catcher" or a "Stingray," covertly sends out a signal that dupes all phones within a specific area into hopping onto a fake network. The spy tool can force targeted phones to release unique identity codes that can then be used to track a person's movements in real time.

Now, the Electronic Privacy Information Center is attempting to obtain internal FBI documents relating to the technology. EPIC is taking legal action to force the prompt disclosure of records concerning Stingray devices or other cell site simulator technologies, alleging that the FBI has "failed to comply with statutory deadlines" by not handing them over quickly enough following a freedom of information request made in February. The FBI has found 25,000 pages of documents that relate to the request, about 6,000 of which are classified—but says it may need up to three years to process the files before they can be released.

In a bid to appease EPIC's grumbles about timescale, earlier this month the bureau released a 0.3 percent slither of the 25,000. The meager 67 pages were heavily redacted—containing only a glossary of jargon that related to cell networks along with blanked out copies of an internal manual called "GSM cell phone tracking for dummies." EPIC's Alan Butler told me the FBI has promised to assess 1,000 documents per month, drip-releasing the portions it has deemed suitable for public consumption. But EPIC is asking that a district judge force the feds to disclose all of the non-classified documents within 60 days, with the 6,000 classified documents assessed for release within six months.

One reason stingray technology is particularly contentious is because by design they result in "collateral" snooping. During the Arizona court case, FBI special agent Bradley Morrison stated in an affidavit that "all wireless devices in the immediate area of the FBI device that subscribe to a particular provider may be incidentally recorded, including those of innocent, non-target devices." (The FBI has insisted that the information it gathers using the tracking tools is routinely deleted, with a spokesperson telling the *Wall Street Journal* last year that "our policy since the 1990s has been to purge or 'expunge' all information obtained during a location operation.")

There are also questions about the constitutionality of how the technology is used. According to EPIC, the devices are sometimes deployed with no warrant—possibly rendering their use a violation of the Fourth Amendment, which prohibits unreasonable searches and seizures. The Supreme Court in January ruled that the use of GPS trackers constituted a "search," but when it comes to mobile phone tracking the government has continued to argue that Americans should have no reasonable expectation of privacy over their location data.

Though more advanced versions of Stingray-style technology can intercept text messages and phone calls, the focus on the FBI's use of the technology has predominantly concerned location tracking. The 25,000 documents held by the FBI likely contain sensitive and controversial details about the full capabilities of its cell surveillance gear—which could partially explain the bureau's aversion to full disclosure.

But this isn't just a federal-level issue. According to a report by *LA Weekly* last month, state cops in California, Florida, Texas, and Arizona have also used Stingray technology. Farther afield, in the Czech Republic, there are concerns that similar devices may be in the hands of criminals. And DIY Stingrays can be built by anyone with $1,500 to burn and a bit of hacker savvy. One way to help protect yourself is to use encryption. Another is to revert back to a 1980s mindset by scrapping your cell phone and sticking to landlines.