MORE VISIBILITY ON STINGRAYS

On New Year's Eve, Chuck Grassley released details of ongoing discussions he and Patrick Leahy have had with the FBI about its use of Stingray (or IMSI catcher) technology, which the FBI and other agencies use to identify cell phone location. Also early last month, the Minneapolis Star-Tribune liberated copies of the documents Minnesota's Bureau of Criminal Apprehension had to sign to get a Stingray (which is less redacted than an NDA released by the Tacoma Police Department to Muckrock in September). Together the documents provide new insight onto how the FBI manages the use of Stingrays around the country.

In his release on Stingrays, Grassley revealed that FBI had recently changed its policy on Stingray use — though the "changed" policy probably affects very little Stingray use.

> [W]e understand that the FBI's new policy requires FBI agents to obtain a search warrant whenever a cell-site simulator is used as part of a FBI investigation or operation, unless one of several exceptions apply, including (among others): (1) cases that pose an imminent danger to public safety, (2) cases that involve a fugitive, or (3) cases in which the technology is used in public places or other locations at which the FBI deems there is no reasonable expectation of privacy.
>
> We have concerns about the scope of the exceptions. Specifically, we are concerned about whether the FBI and other law enforcement agencies have adequately considered the privacy interests of other individuals who are not the targets of the interception, but whose information is nevertheless being collected when these devices are being

> used. We understand that the FBI believes that it can address these interests by maintaining that information for a short period of time and purging the information after it has been collected. But there is a question as to whether this sufficiently safeguards privacy interests.

I say this probably doesn't affect much Stingray use because we already know the US Marshal Service makes up a lot of the known Federal use of Stingrays (at least that use that obtains Pen Registers to use the Stingrays). They would presumably be hunting fugitives, which is one of the overly broad exceptions in FBI's "new" policy. We discovered last year just how elastic the federal government's interpretation of "imminent danger" can be. And the most common — and troubling — known use of Stingrays are in public spaces (like legal protests) to track participants.

Indeed, in the one known example where a Stingray was used to discover the identity of a suspect, Daniel Rigmaiden, the government got a warrant for its use, albeit one obtained without fully explaining how it works.

So it's not clear that this "new" policy will change all that much. Moreover, Grassley is focused on federal use of the technology, and not the way federal use intersects with and controls local use.

Now couple that with this non-disclosure agreement (pages 10-15, h/t SanLeandroPrivacy) sent in June 2012. The NDA explains that,

> Disclosing the existence of and the capabilities provided by such equipment/technology to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation wherein this

> equipment/technology is used to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations.

If that's such a big worry, then maybe it shouldn't be so widely available in the first place? Also, I see how seamlessly the FBI moves from law enforcement to national security functions…

The NDA then goes onto tell the BCA the following (among other things):

- BCA should only use it for "public safety operations or criminal investigations."
- BCA accepts liability for violations of Federal law, irrespective of the FBI approval, if any, of [redacted].
- The BCA will [redacted] to ensure deconfliction of respective missions.

Then there's a very long paragraph laying out something else the BCA "shall not" do.

So over the course of the NDA, we got from "law enforcement" purposes, to national security investigations, to "public safety operations." The NDA clearly envisions FBI approval of some use of this technology, suggesting an ongoing relationship with this local agency. That is further established by FBI's concern about "deconfliction of respective missions," meaning FBI expects BCA to communicate about how it will use its Stingray with out agencies who might be using their Stingrays (or BCA's Stingray?) in

ways that might set off a turf war. Plus whatever that “shall not” paragraph says.

The point is, the FBI is not just demanding that BCA not tell anyone that it has a Stingray and how Stingray’s use (see this Chris Soghoian and Stephanie Pell paper for why that’s a futile fight anymore anyway). It is also demand certain things about cooperation between agencies. And while that makes sense from a bureaucratic standpoint, it also may suggest there’s more reason to keep FBI involved in these local operations than just secrecy. After all, as more and more local police departments get Stingrays and sign these agreements with FBI, the FBI is assured there’s a network of Stingrays across the country that will be deployed if necessary. Given the inclusion of national security investigations in this NDA (which, after all, is all that FBI thought it needed to get NSA to collect all our phone records), it at least introduces the possibility of a more systematic FBI program for which the FBI relies on local Stingrays.

That’s just a latent concern of mine — we don’t yet have the proof of it (we’ll have to liberate far more NDAs to get it). But it does seem logical, given the role FBI is playing in this process, all in the guise of futile secrecy.