IS THERE A PROGRAMMATIC STINGRAY?

The NYT yesterday had a story on the secrecy surrounding Stingrays including these admissions from an FBI affidavit to explain the secrecy.

> 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 response, a bunch of smart people had an

interesting conversation today about why the government is so secretive about them (start at this tweet).

My wildarseguess is that they're hiding some kind of programmatic Stingray program. I think so for three reasons:

- Any programmatic Stingray program would (have) been hidden by carve-outs in USA Freedom Act's transparency provisions
- At least one of the liberated non-disclosure agreements suggests ongoing obligations between localities and the FBI
- FISC appears to have permitted more expansive versions of criminal PRTT programs

In past legislative debates the Intelligence Community revealed secret programs by defending them

I believe one of the best ways to see vague outlines of undisclosed domestic surveillance is to watch where the Intelligence Community is most intransigent on legislation.

When Michaels Mukasey and McConnell wrote a transparently bullshit response to a Russ Feingold effort to segregate incidentally collected US person data under FISA Amendments Act in early 2008, I guessed they were doing back door searches of that data. 4 and 5 years later (with the report on the reauthorization and Snowden disclosures, respectively), that was

proven correct.

When the IC repeatedly and successfully defeated efforts to require some real connection between a target and the records collected using Section 215 in 2009 all while boasting they had used it in the Najibullah Zazi investigation, I guessed they were using Section 215 to collect bulky data. I even guessed that they had migrated Bush's illegal wiretap program to Section 215 and PRTT (though a former prosecutor friend soon dissuaded me from pushing my PRTT analysis because, she pointed out, there was no way in hell PRTT could authorize a dragnet).

There were 3 parts of the USA Freedom Act which struck me as particularly notable in the same way. First, the government's insistence on expanding the chaining process to include "connections" in addition to contacts; I strongly believe that indicates they ask cell companies to match up the various identities with a particular handset.

Then there were two kinds of programmatic collection that would not only not be shut down by the prohibition on bulk collection in the bill, but which were specifically excluded from individualized transparency reporting (in addition to back door searches and upstream domestic collection, but we already knew about both of those), because transparency in the bill only covered "communications." The first is any kind of dragnet tied to a non-communication corporate name, such as a financial dragnet or hotel records. See this post for an explanation. USAF would not require individualized reporting on this collection at all. Particularly given that the bill would permit using corporate names as identifiers and would exclude that from transparency, I think reasonable people should assume that kind of bulky collection would continue unabated.

More interesting, though, the transparency provisions also appear to exempt tracking device collection from individualized reporting, because those aren't considered "communications"

from individualized transparency reporting (I believe it would also exempt cloud data but I don't understand what this is yet). I don't think the government could use "Harris Corporation" as a identifier (they wouldn't need to anyway, because the FBI would be using the tool not collecting all of Harris' data). But they could collect the tracking data on 310 million people and only need to report targets (which currently number in the hundreds, though there already is some gaming of the required US person target reporting).

Like a Stingray, which looks for one phone, but obtains the records of everyone in a cell area.

Which is why I love this quote from the NYT article:

> 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."

The government currently collects phone records of some significant subset of 310 million Americans for the purposes of "specific investigations." It's just that they consider enterprise investigations to be "specific" and therefore every American to be "relevant." The same may well apply to location data.

FBI's non-disclosure agreement(s) suggests ongoing cooperation between local and federal law enforcement

We've already seen plenty of evidence that local law enforcement retain their ties and obligations to federal law enforcement, largely in the demands the Marshal service puts on secrecy.

But as I lay out in this post, that seems to involve ongoing cooperation using the Stingray. An NDA liberated in MN specifically requires deconfliction of missions, indicating that multiple entities would use one Stingray at once.

That all seems to suggest a key part of this top-down hierarchical non-disclosure requirement involves that kind of mission-sharing.

Which is another way of saying that FBI probably relies on these local Stingrays.

FISC appears to permit more expansive PRTT programs than in criminal context

In this post and this one, I showed that the FISC-authorized use of PRTT relates the criminal context but may not be bound by it. That's significant, because we know where the government has obtained permission for Stingray use in the criminal context, they've often relied on PRTT.

In both the use of combined PRTT/215 orders to get location data and in the collection of Post-Cut Through Dialed Digits, FISC has reconsidered PRTT orders after magistrates challenged similar criminal uses. At least in the latter example, FISC permitted FBI to continue a more expansive collection even after it was prohibited in the criminal context, requiring only that FBI comply with Fourth Amendment protections using minimization (as I'll show when I finally write up the remainder of the FISC opinions, this practice has early foundation in other FISC applications).

> What becomes clear reviewing the public records (these reports say this explicitly) is that the 2002 DOJ directive against retaining PCTDD applies to the criminal context, not the FISA context. When judges started challenging FBI's authority to retain

> PCTDD that might include content under criminal authorities, FBI fought for and won the authority to continue to treat PCTDD using minimization procedures, not deletion. And even the standard for retention of PCTDD that counts as content permits the affirmative investigative use of incidentally collected PCTDD that constitutes content in cases of "harm to the national security."
>
> Whateverthefuck that is.
>
> Which is, I guess, how FBI still has 7 uses of PCTDD, including one new one since 2008.

In other words, the Stingray use we see glimpses of in the criminal and fugitive context may be far short of what FISC has permitted in the national security context, if it tracks other practice. And accused terrorists (or spies) would not get notice of any such PRTT use so long as it wasn't entered into a criminal proceeding (there have been several instances where the government has seemed to suggest PRTT was used, but evidence from it not entered into evidence).

All of this, of course, is speculative.

But there's some reason the government is insisting on its expansive NDAs even while more and more people are discussing them. Hiding a more comprehensive program targeted at national security targets (terrorists and spies) might explain why the government is increasingly willing to forgo prosecutions of alleged criminals to keep what they're doing with dragnets secret.

Update: Meanwhile, in NY, a judge has ordered the Erie County Sheriff to come clean on its Stingray use.