THE LOOPHOLES IN DOJ'S NEW STINGRAY POLICY

DOJ just announced a new policy on use of Stingrays which requires a warrant and minimization of incidentally-collected data. It's big news and an important improvement off the status quo.

But there are a few loopholes.

Exigent and emergency uses

First, the policy reserves exigent uses. The exigent uses include most of DOJ Agencies known uses of Stingrays now.

> These include the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.
>
> [snip]
>
> In addition, in the subset of exigent situations where circumstances necessitate emergency pen register authority pursuant to 18 U.S.C. § 3125 (or the state equivalent), the emergency must be among those listed in Section 3125: immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year.

We know the US Marshals constitute the most

frequent users of admitted Stingray use — they'd be covered in prevention of escape by a fugitive. DEA seems to use them a lot (though I think more of that remains hidden). That'd include "conspiratorial activities characteristic of organized crime." And it's clear hackers are included here, which includes the first known use, to capture Daniel Rigmaiden.

And I'm not sure whether the exigent/emergency use incorporates the public safety applications mentioned in the non-disclosure agreements localities sign with the FBI, or if that's included in this oblique passage.

> There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. In such cases, which we expect to be very limited, agents must first obtain approval from executive-level personnel at the agency's headquarters and the relevant U.S. Attorney, and then from a Criminal Division DAAG. The Criminal Division shall keep track of the number of times the use of a cell-site simulator is approved under this subsection, as well as the circumstances underlying each such use.

In short, many, if not most, known uses are included in exceptions to the new policy.

Notice to defendants

The many known uses of Stingrays where warrants would not be necessary — and where DOJ would therefore just be using a PRTT — are of particular importance given the way new disclosure requirements work. There are, to be sure, admirable new requirements to tell judges what the fuck they're approving and what it means. But nothing explicitly says defendants

will not get noticed. DOJ has said no past or current usage of Stingrays will get noticed to defendants. And all these non-warrant uses of Stingrays will be noticed either, probably. In other words, this returns things to the condition where defendants won't know — because they would normally expect to see a warrant that wouldn't exist in these non-warrant uses.

Sharing with localities

The policy doesn't apply to localities, which increasingly have their own Stingrays they permit federal agencies to use. Curiously, the language applying this policy to federal cooperation with localities would suggest the federal rules only apply if the Feds are supporting localities, not if the reverse (FBI borrowing Buffalo's Stingray, for example) is the case.

> The Department often works closely with its State and Local law enforcement partners and provides technological assistance under a variety of circumstances. This policy applies to all instances in which Department components use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies.

Thus, it may leave a big out for the kind of cooperation we know to exist.

National security uses

Then, of course, the policy only applies in the criminal context, though DOJ claims it will adopt a policy "consistent" with this one on the FISC side.

> This policy applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations. When acting pursuant to the Foreign

> Intelligence Surveillance Act, Department of Justice components will make a probable-cause based showing and appropriate disclosures to the court in a manner that is consistent with the guidance set forth in this policy.

BREAKING! FBI has been using Stingrays in national security investigations! (Told ya!)

This language is itself slippery. FISC use of Stingrays probably won't be consistent on the FISC side (even accounting for the many ways exigent uses could be claimed in national security situations), because we know that FISC *already* has different rules for PRTT on the FISC side, in that it permits collection of post cut through direct dialed numbers — things like extension numbers — so long as that gets minimized after the fact. The section on minimization here emphasizes the "law enforcement" application as well. So I would assume that not only will national security targets of Stingrays not get noticed on it, but they may use different minimization rules as well (especially given FBI's 30 year retention for national security investigation data).

Other agencies use of Stingrays for content

DOJ suggests that DOJ never collects content using Stingrays by stating that its Stingrays always get set not to collect content.

> Moreover, cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site

> simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

But the rest of the policy makes it clear that department agents will work with other agencies on Stingray use. Some of those — such as JSOC — not only would have Stingrays that get content, but can even partner within the US with FBI. So DOJ hasn't actually prohibited its agencies from getting content from a Stingray (domestically — it goes without saying they're permitted to do so overseas), just that it won't do so using its own Stingrays.

Funny definitional games

Finally, while not necessarily a loophole (or at least not one I completely understand yet), I'm interested in this definition.

> In the context of this policy, the terms "collection" and "retention" are used to address only the unique technical process of identifying dialing, routing, addressing, or signaling information, as described by 18 U.S.C. § 3 I 27(3), emitted by cellular devices. "Collection" means the process by which unique identifier signals are obtained; "retention" refers to the period during which the dialing, routing, addressing, or signaling information is utilized to locate or identify a target device, continuing until tlle point at whic!h such information is deleted.

This definition (which only applies to this policy and therefore perhaps not to national security uses of Stingrays) employs an entirely different definition for collection and retention than other collection that relies on collection then software analysis. Under upstream collection, for example, the government

calls this definition of “retention” something closer to “collection.” Don’t get me wrong — this is probably a better definition than that used in other contexts. But I find it funny that FBI employs such different uses of these words in very closely connected contexts.

So, in sum, this is a real victory, especially the bit about actually telling judges what they’re approving when they approve it.

But there are some pretty obvious loopholes here….

Update: ACLU also welcomes this while pointing to some of the limits of the policy.

Update: Here are some of my posts on the FISA uses of PRTT, including (we now know) Stingrays.

> DOJ IG: FBI’s Secret Applications of PRTT Are Even More Secret than Its Secret Applications of Section 215

> FBI’s Pen Registers without Any Call Records

> The Loss of PRTT Minimization Review in USA F-ReDux

https://www.emptywheel.net/2015/03/17/is-there-a-programmatic-stingray/