IT'S NOT JUST THE FISA COURT, IT'S THE GAME OF SURVEILLANCE WHACK-A-MOLE

In response to this post from Chelsea Manning, the other day I did the first in what seems to have become a series of posts arguing that we should eliminate the FISA Court, but that the question is not simple. In that post, I laid out the tools the FISC has used, with varying degrees of success, in reining in Executive branch spying, especially in times of abuse.

In this post, I want to lay out how reining in surveillance isn't just about whether the secret approval of warrants and orders would be better done by the FISC or a district court. It's about whack-a-mole.

That's because, right now, there are four ways the government gives itself legal cover for expansive surveillance:

- FISC, increasingly including programs
- EO 12333, including SPCMA
- Magistrate warrants and orders without proper briefing
- Administrative orders and/or voluntary cooperation

FISA Court

The government uses the FISA court to get individualized orders for surveillance in this country and, to a less clear extent, surveillance of Americans overseas. That's the old-fashioned stuff that could be done by a district court. But it's also one point where egregious source information — be it a foreign

partner using dubious spying techniques, or, as John Brennan admitted in his confirmation hearing, torture — gets hidden. No defendant has ever been able to challenge the basis for the FISA warrant used against them, which is clearly not what Congress said it intended in passing FISA. But given that's the case, it means a lot of prosecutions that might not pass constitutional muster, because of that egregious source information, get a virgin rebirth in the FISC.

In addition, starting 2004, the government started using the FISA Court to coerce corporations to continue domestic collection *programs* they had previously done voluntarily. As I noted, while I think the FISC's oversight of these programs has been mixed, the FISC *has* forced the government to hew closer (though not at) the law.

EO 12333, including SPCMA

The executive branch considers FISA just a subset of EO 12333, the Reagan Executive Order governing the intelligence community — a carve out of collection requiring more stringent rules. At times, the Intelligence Community have operated as if EO 12333 is the only set of rules they need to follow — and they've even secretly rewritten it at least once to change the rules. The government will always assert the right to conduct spying under EO 12333 if it has a technical means to bypass that carve out. That's what the Bush Administration claimed Stellar Wind operated under. And at precisely the time the FISC was imposing limits on the Internet dragnet, the Executive Brach was authorizing analysis of Americans' Internet metadata collected overseas under SPCMA.

EO 12333 derived data does get used against defendants in the US, though it appears to be laundered through the FISC and/or parallel constructed, so defendants never get the opportunity to challenge this collection.

Magistrate warrants and orders

Even when the government goes to a Title III court — usually a magistrate judge — to get an order or warrant for surveillance, that surveillance often escapes real scrutiny. We've seen this happen with Stingrays and other location collection, as well as FBI hacking; in those cases, the government often didn't fully brief magistrates about what they're approving, so the judges didn't consider the constitutional implications of it. There are exceptions, however (James Orenstein, the judge letting Apple challenge the use of an All Writs Act to force it to unlock a phone, is a notable one), and that has provided periodic checks on collection that should require more scrutiny, as well as public notice of those methods. That's how, a decade after magistrates first started to question the collection of location data using orders, we're finally getting circuit courts to review the issue. Significantly, these more exotic spying techniques are often repurposed foreign intelligence methods, meaning you'll have magistrates and other TIII judges weighing in on surveillance techniques being used in parallel programs under FISA. At least in the case of Internet data, that may even result in a higher standard of scrutiny and minimization being applied to the FISA collection than the criminal investigation collection.

Administrative orders and/or voluntary cooperation

Up until 2006, telecoms willing turned over metadata on Americans' calls to the government under Stellar Wind. Under Hemisphere, AT&T provides the government call record information — including results of location-based analysis, on all the calls that used its networks, not just AT&T customers — sometimes without an order. For months after Congress was starting to

find a way to rein in the NSA phone dragnet with USA Freedom Act, the DEA continued to operate its own dragnet of international calls that operated entirely on administrative orders. Under CISA, the government will obtain and disseminate information on cybersecurity threats that it wouldn't be able to do under upstream 702 collection; no judge will review that collection. Until 2009, the government was using NSLs to get all the information an ISP had on a user or website, including traffic information. AT&T still provides enhanced information, including the call records of friends and family co-subscribers and (less often than in the past) communities of interest.

These six examples make it clear that, even with Americans, even entirely within the US, the government conducts a lot of spying via administrative orders and/or voluntary cooperation. It's not clear this surveillance had any but internal agency oversight, and what is known about these programs (the onsite collaboration that was probably one precursor to Hemisphere, the early NSL usage) makes it clear there have been significant abuses. Moreover, a number of these programs represent individual (the times when FBI used an NSL to get something the FISC had repeatedly refused to authorize under a Section 215 order) or programmatic collection (I suspect, CISA) that couldn't be approved under the auspices of the FISC.

All of which is to say the question of what to do to bring better oversight over expansive surveillance is not limited to the short-comings of the FISC. It also must contend with the way the government tends to move collection programs when one method proves less than optimal. Where technologically possible, it has moved spying offshore and conducted it under EO 12333. Where it could pay or otherwise bribe and legally shield providers, it moved to voluntary collection. Where it needed to use traditional courts, it often just obfuscated about what it was doing. The primary limits here are not *legal*, except insofar as legal niceties and

the very remote possibility of transparency raise corporate partner concerns.

We need to fix or eliminate the FISC. But we need to do so while staying ahead of the game of whack-a-mole.