I CON THE RECORD TRANSPARENCY BINGO PART ONE: CONSIDER THE FULL SURVEILLANCE PLAYING HAND

Several weeks ago, the government released its yearly transparency reports:

- FISA Court's report: This provides a very useful description of approvals viewed from the FISA Court's perspective. While it is the least deceptive report, FISC has only released one full year (2016) and one partial year (2015) report before, so it can't be used to study trends or history.
- DOJ report: This is the mostly useless report, told from the government's standpoint, reflecting how many final applications get approved. While it isn't very useful for nuance, it is the only measure we can use to compare last year with the full history of FISA.
- DNI report: This is the report started in the wake of the Snowden leaks and codified in the USA Freedom Act and last year's FISA

> Amendments Act. Parts of this report are very useful, parts are horribly misleading (made worse by new reporting requirements pass in the FAA reauthorization). But it requires more kinds of data than the other two reports.

I've been meaning to write more on the transparency reports released some weeks ago (see this post debunking the claim that we can say the FISA Court has rejected more applications than in the past). But given some misunderstandings in this post, I thought it better to lay out some general principles about how to understand what the transparency reports show us.

Consider the full surveillance playing hand

FISA is just one way that the government can collect data used for national security investigations, and because it involves a secret court, it attracts more attention than the many other ways. Worse, it often attracts the focus *in isolation* from other surveillance methods, meaning even experts fail to consider how authorities work together to provide different parts of the government all the kinds of data they might want. Additionally, an exclusive focus on FISA may blind people to how new restrictions or permissions in one authority may lead to changes in how the government uses another authority.

National security surveillance currently includes at least the following:

- FISA, including

individualized orders, 702, and metadata collection
- NSLs, providing some kind of metadata with little (albeit increasing) court oversight
- Criminal investigative methods, collecting content, metadata, and business records; in 2016 this came to include Rule 41 hacking
- Other means to collect business records, such as private sector contractors or mandated bank reporting
- The Cybersecurity Information Sharing Act, permitting the private sector to share cyber data "voluntarily" with the government
- EO 12333: spying conducted overseas under Article II authority; in 2017, the Obama Administration permitted the sharing of raw data within the intelligence community (which includes FBI)

Two examples of how FISA interacts with other authorities may help to demonstrate the importance of considering all these authorities together.

The Internet dragnet moves to PRISM and SPCMA

For virtually the entirety of the time the government collected Internet metadata as metadata domestically, it was breaking the law (because the concepts of metadata and content

don’t apply neatly to packet based collection). From 2009 to 2011, the government tried to fake their way through this (in part by playing games with the distinction between collection and access). By the end of 2011, however, that game became legally untenable. Plus, the restrictions the FISA Court imposed on dissemination rules and purpose (NSA was only permitted to collect this data for counterterrorism purposes) made the program less useful. As a result, the government moved the function of chaining on Internet metadata to two different areas: metadata collected under PRISM (which because it was collected as content avoided the legal problems with Internet metadata collection) and metadata collected under EO 12333 and made accessible to analysts under Special Procedures approved in 2008 and extended throughout NSA in early 2011.

Some location collections moves to criminal context

As I’ve laid out, the FISC actually takes notice of rulings in the criminal context — even at the magistrate level — and adjusts FISC rulings accordingly. They’ve done this with both Post Cut Through Dialed Digits and location data. When the FISC adopted a highest common denominator for location collection, it meant that, in jurisdictions where FBI could still obtain location data with a d order, they might do that for national security purposes rather than obtain a PRTT under FISA (to say nothing of the additional paperwork). More recently, we’ve gotten hints that FBI had ways to access cell phones in a national security realm that were unavailable in a criminal realm.

This probably goes on all the time, as FBI Agents make trade offs of secrecy, notice to defendants, paperwork and oversight, and specific collection techniques to pursue national security investigations. We don’t get great numbers for FBI collection in any case, but what we do get will be significantly affected by these granular decisions made in

secret.

Understand why surveillance law changes

Additionally, it's important to understand why surveillance laws get passed.

CISA, for example, came about (among many other reasons) because Congress wouldn't permit the government to conduct upstream collection using Section 702 for all cybersecurity purposes. Engaging in "voluntary" sharing with backbone providers gave the government data from all kinds of hostile actors (not just nation states), with fewer restrictions on sharing, no court oversight, and no disclosure requirements.

Similarly, to this day, many privacy activists and journalists misunderstand why the government was willing (nay, happy!) to adopt USA Freedom Act. It's not that the government didn't collect mobile data. On the contrary, the government had been obtaining cell data from AT&T since 2011, and that was probably a resumption of earlier collection incorporating FISA changed rules on location collection. Nor was it about calling card data; that had been explicitly permitted under the old program. Rather, USAF gave the government the ability to require assistance, just as it can under Section 702. While that was instrumental in getting access to Verizon cell data (which had avoided complying because it did not retain business records in the form that complied with FISA collection rules), that also gave the ability to get certain kinds of data under the "session identifier" definition of call records in the law.

Here's a post on all the other goodies the government got with USA Freedom Act.

One more important detail virtually unmentioned in coverage of this authority: the 215 dragnet (both the old one and the USAF one) intersect

with a far vaster dragnet of metadata collected under 12333. The “bulk” is achieved — and has been since 2009! — using EO 12333 data, data which doesn’t have the same restrictions on things like location data that FISA data does. Section 215 is about getting records (and correlations) that aren’t available overseas, effectively filling in the holes in data collected overseas.

All that is necessary background to understanding numbers that track just FISA (and NSL authorities). FISA is just one part of the always evolving national security collection the government does. And as permissive as a lot of people think FISA is, in many ways it is the most closely regulated part of national security collection.