A DRAGNET OF EMPTYWHEEL'S MOST IMPORTANT POSTS ON SURVEILLANCE, 2007 TO 2017

Happy Birthday to me! To us! To the emptywheel community!

On December 3, 2007, emptywheel first posted as a distinct website. That makes us, me, we, ten this week.

To celebrate, the emptywheel team has been sharing some of our favorite work from the last decade. This is my massive dragnet of surveillance posts.

For years, we've done this content ad free, relying on donations and me doing freelance work for others to fund the stuff you read here. I would make far more if I worked for some free-standing outlet, but I wouldn't be able to do the weedy, iterative work that I do here, which would amount to not being able to do my best work.

If you've found this work valuable — if you'd like to ensure it remains available for the next ten years — please consider supporting the site.

2007

Whitehouse Reveals Smoking Gun of White House Claiming Not to Be Bound by Any Law

Just days after opening the new digs, I noticed Sheldon Whitehouse entering important details into the Senate record — notably, that John Yoo

had pixie dusted EO 12333 to permit George Bush to authorize the Stellar Wind dragnet. In the ten years since, both parties worked to gradually expand spying on Americans under EO 12333, only to have Obama permit the sharing of raw EO 12333 data in its last days in office, completing the years long project of restoring Stellar Wind's functionalities. This post, from 2016, analyzes a version of the underlying memo permitting the President to change EO 12333 without providing public notice he had done so.

2008

McConnell and Mukasey Tell Half Truths

In the wake of the Protect America Act, I started to track surveillance legislation as it was written, rather than figure out after the fact how the intelligence community snookered us. In this post, I examined the veto threats Mike McConnell and Michael Mukasey issued in response to some Russ Feingold amendments to the FISA Amendments Act and showed that the government intended to use that authority to access Americans' communication via both what we now call back door searches and reverse targeting. "That is, one of the main purposes is to collect communications in the United States."

9 years later, we're still litigating this (though, since then FISC has permitted the NSA to collect entirely domestic communications under the 2014 exception).

2009

FISA + EO 12333 + [redacted] procedures =

No Fourth Amendment

The Government Sez: We Don’t Have a Database of All Your Communication

After the FISCR opinion on what we now know to be the Yahoo challenge to Protect American Act first got declassified, I identified several issues that we now have much more visibility on. First, PAA permitted spying on Americans overseas under EO 12333. And it didn’t achieve particularity through the PAA, but instead through what we know to be targeting procedures, including contact chaining. Since then we’ve learned the role of SPCMA in this.

In addition, to avoid problems with back door searches, the government claimed it didn’t have a database of all our communication — a claim that, narrowly parsed might be true, but as to the intent of the question was deeply misleading. That claim is one of the reasons we’ve never had a real legal review of back door searches.

Bush’s Illegal Domestic Surveillance Program and Section 215

On PATRIOTs and JUSTICE: Feingold Aims for Justice

During the 2009 PATRIOT Act reauthorization, I continued to track what the government hated most as a way of understanding what Congress was really authorizing. I understood that Stellar Wind got replaced not just by PAA and FAA, but

also by the PATRIOT authorities.

> All of which is a very vague way to say we probably ought to be thinking of four programs—Bush's illegal domestic surveillance program and the PAA/FAA program that replaced it, NSLs, Section 215 orders, and trap and trace devices—as one whole. As the authorities of one program got shut down by exposure or court rulings or internal dissent, it would migrate to another program. That might explain, for example, why Senators who opposed fishing expeditions in 2005 would come to embrace broadened use of Section 215 orders in 2009.

I guessed, for example, that the government was bulk collecting data and mining it to identify targets for surveillance.

> We probably know what this is: the bulk collection and data mining of information to select targets under FISA. Feingold introduced a bajillion amendments that would have made data mining impossible, and each time Mike McConnell and Michael Mukasey would invent reasons why Feingold's amendments would have dire consequences if they passed. And the legal information Feingold refers to is probably the way in which the Administration used EO 12333 and redacted procedures to authorize the use of data mining to select FISA targets.

Sadly, I allowed myself to get distracted by my parallel attempts to understand how the government used Section 215 to obtain TATP precursors. As more and more people confirmed that, I stopped pursuing the PATRIOT Act ties to 702 as aggressively.

2010

Throwing our PATRIOT at Assange

This may be controversial, given everything that has transpired since, but it is often forgotten what measures the US used against Wikileaks in 2010. The funding boycott is one thing (which is what led Wikileaks to embrace Bitcoin, which means it is now in great financial shape). But there's a lot of reason to believe that the government used PATRIOT authorities to target not just Wikileaks, but its supporters and readers; this was one hint of that in real time.

2011

The March–and April or May–2004 Changes to the Illegal Wiretap Program

When the first iteration of the May 2004 Jack Goldsmith OLC memo first got released, I identified that there were multiple changes made and unpacked what some of them were. The observation that Goldsmith newly limited Stellar Wind to terrorist conversations is one another reporter would claim credit for "scooping" years later (and get the change wrong in the process). We're now seeing the scope of targeting morph again, to include a range of domestic crimes.

Using Domestic Surveillance to Get Rapists to Spy for

America

Something that is still not widely known about 702 and our other dragnets is how they are used to identify potential informants. This post, in which I note Ted Olson's 2002 defense of using (traditional) FISA to find rapists whom FBI can then coerce to cooperate in investigations was the beginning of my focus on the topic.

2012

FISA Amendments Act: "Targeting" and "Querying" and "Searching" Are Different Things

During the 2012 702 reauthorization fight, Ron Wyden and Mark Udall tried to stop back door searches. They didn't succeed, but their efforts to do so revealed that the government was doing so. Even back in 2012, Dianne Feinstein was using the same strategy the NSA currently uses — repeating the word "target" over and over — to deny the impact on Americans.

Sheldon Whitehouse Confirms FISA Amendments Act Permits Unwarranted Access to US Person Content

As part of the 2012 702 reauthorization, Sheldon Whitehouse said that requiring warrants to access the US person content collected incidentally would "kill the program." I took that as confirmation of what Wyden was saying: the government was doing what we now call back

door searches.

2013

20 Questions: Mike Rogers' Vaunted Section 215 Briefings

After the Snowden leaks started, I spent a lot of time tracking bogus claims about oversight. After having pointed out that, contrary to Administration claims, Congress did not have the opportunity to be briefed on the phone dragnet before reauthorizing the PATRIOT Act in 2011, I then noted that in one of the only briefings available to non-HPSCI House members, FBI had lied by saying there had been no abuses of 215.

John Bates' TWO Wiretapping Warnings: Why the Government Took Its Internet Dragnet Collection Overseas

Among the many posts I wrote on released FISA orders, this is among the most important (and least widely understood). It was a first glimpse into what now clearly appears to be 7 years of FISA violation by the PRTT Internet dragnet. It explains why they government moved much of that dragnet to SPCMA collection. And it laid out how John Bates used FISA clause 1809(a)(2) to force the government to destroy improperly collected data.

Federated Queries and EO 12333 FISC

Workaround

In neither NSA nor FBI do the authorities work in isolation. That means you can conduct a query on federated databases and obtain redundant results in which the same data point might be obtained via two different authorities. For example, a call between Michigan and Yemen might be collected via bulk collection off a switch in or near Yemen (or any of the switches between there and the US), as well as in upstream collection from a switch entering the US (and all that's assuming the American is not targeted). The NSA uses such redundancy to apply the optimal authority to a data point. With metadata, for example, it trained analysts to use SPCMA rather than PATRIOT authorities because they could disseminate it more easily and for more purposes. With content, NSA appears to default to PRISM where available, probably to bury the far more creative collection under EO 12333 for the same data, and also because that data comes in structured form.

Also not widely understood: the NSA can query across metadata types, returning both Internet and phone connection in the same query (which is probably all the more important now given how mobile phones collapse the distinction between telephony and Internet).

This post described how this worked with the metadata dragnets.

The Purpose(s) of the Dragnet, Revisited

The government likes to pretend it uses its dragnet only to find terrorists. But it does far more, as this analysis of some court filings lays out.

2014

The Corporate Store: Where NSA Goes to Shop Your Content and Your Lifestyle

There’s something poorly understood about the metadata dragnets NSA conducts. The contact-chaining isn’t the point. Rather, the contact-chaining serves as a kind of nomination process that puts individuals’ selectors, indefinitely, into the “corporate store,” where your identity can start attracting other related datapoints like a magnet. The contact-chaining is just a way of identifying which people are sufficiently interesting to submit them to that constant, ongoing data collection.

SPCMA: The Other NSA Dragnet Sucking In Americans

I’ve done a lot of work on SPCMA — the authorization that, starting in 2008, permitted the NSA to contact chain on and through Americans with EO 12333 data, which was one key building block to restoring access to EO 12333 analysis on Americans that had been partly ended by the hospital confrontation, and which is where much of the metadata analysis affecting Americans has long happened. This was my first comprehensive post on it.

The August 20, 2008 Correlations Opinion

A big part of both FBI and NSA’s surveillance involves correlating identities — basically, tracking all the known identities a person uses

on telephony and the Internet (and financially, though we see fewer details of that), so as to be able to pull up all activities in one profile (what Bill Binney once called "dossiers"). It turns out the FISC opinion authorizing such correlations is among the documents the government still refuses to release under FOIA. Even as I was writing the post Snowden was explaining how it works with XKeyscore.

A Yahoo! Lesson for USA Freedom Act: Mission Creep

This is another post I refer back to constantly. It shows that, between the time Yahoo first discussed the kinds of information they'd have to hand over under PRISM in August 2007 and the time they got directives during their challenge, the kinds of information they were asked for expanded into all four of its business areas. This is concrete proof that it's not just emails that Yahoo and other PRISM providers turn over — it's also things like searches, location data, stored documents, photos, and cookies.

FISCR Used an Outdated Version of EO 12333 to Rule Protect America Act Legal

Confession: I have an entire chapter of the start of a book on the Yahoo challenge to PRISM. That's because so much about it embodied the kind of dodgy practices the government has, at the most important times, used with the FISA Court. In this post, I showed that the documents that the government provided the FISCR hid the fact that the then-current versions of the documents had recently been modified. Using the active documents would have shown that Yahoo's key argument — that the government could change

the rules protecting Americans anytime, in secret — was correct.

2015

Is CISA the Upstream Cyber Certificate NSA Wanted But Didn't Really Get?

Among the posts I wrote on CISA, I noted that because the main upstream 702 providers have a lot of federal business, they'll "voluntarily" scan on any known cybersecurity signatures as part of protecting the federal government. Effectively, it gives the government the certificate it wanted, but without any of the FISA oversight or sharing restrictions. The government has repeatedly moved collection to new authorities when FISC proved too watchful of its practices.

The FISA Court's Uncelebrated Good Points

Many civil libertarians are very critical of the FISC. Not me. In this post I point out that it has policed minimization procedures, conducted real First Amendment reviews, taken notice of magistrate decisions and, in some cases, adopted the highest common denominator, and limited dissemination.

How the Government Uses Location Data from Mobile Apps

Following up on a Ron Wyden breadcrumb, I

figured out that the government — under both FISA and criminal law — obtain location data from mobile apps. While the government still has to adhere to the collection standard in any given jurisdiction, obtaining the data gives the government enhanced location data tied to social media, which can implicate associates of targets as well as the target himself.

The NSA (Said It) Ate Its Illegal Domestic Content Homework before Having to Turn It in to John Bates

I'm close to being able to show that even after John Bates reauthorized the Internet metadata dragnet in 2010, it remained out of compliance (meaning NSA was *always* violating FISA in obtaining Internet metadata from 2002 to 2011, with a brief lapse). That case was significantly bolstered when it became clear NSA hastily replaced the Internet dragnet with obtaining metadata from upstream collection after the October 2011 upstream opinion. NSA hid the evidence of problems on intake from its IG.

FBI Asks for at Least Eight Correlations with a Single NSL

As part of my ongoing effort to catalog the collection and impact of correlations, I showed that the NSL Nick Merrill started fighting in 2004 asked for eight different kinds of correlations before even asking for location data. Ultimately, it's these correlations as much as any specific call records that the government appears to be obtaining with NSLs.

2016

What We Know about the Section 215 Phone Dragnet and Location Data

During the lead-up to the USA Freedom Debate, the government leaked stories about receiving a fraction of US phone records, reportedly because of location concerns. The leaks were ridiculously misleading, in part because they ignored that the US got redundant collection of many of exactly the same calls they were looking for from EO 12333 collection. Yet in spite of these leaks, the few figured out that the need to be able to force Verizon and other cell carriers to strip location data was a far bigger reason to pass USAF than anything Snowden had done. This post laid out what was known about location data and the phone dragnet.

While It Is Reauthorizing FISA Amendments Act, Congress Should Reform Section 704

When Congress passed FISA Amendments Act, it made a show of providing protections to Americans overseas. One authority, Section 703, was for spying on people overseas with help of US providers, and another was for spying on Americans overseas without that help. By May 2016, I had spent some time laying out that only the second, which has less FISC oversight, was used. And I was seeing problems with its use in reporting. So I suggested maybe Congress should look into that?

It turns out that at precisely that moment, NSA was wildly scrambling to get a hold on its 704 collection, having had an IG report earlier in the year showing they couldn't audit it, find it all, or keep it within legal boundaries. This would be the source of the delay in the 702 reauthorization in 2016, which led to the prohibition on about searches.

The Yahoo Scan: On Facilities and FISA

The discussion last year of a scan the government asked Yahoo to do of all of its users was muddled because so few people, even within the privacy community, understand how broadly the NSA has interpreted the term "selector" or "facility" that it can target for collection. The confusion remains to this day, as some in the privacy community claim HPSCI's use of facility based language in its 702 reauthorization bill reflects *new* practice. This post attempts to explain what we knew about the terms in 2016 (though the various 702 reauthorization bills have offered some new clarity about the distinctions between the language the government uses).

2017

Ron Wyden's History of Bogus Excuses for Not Counting 702 US Person Collection

Ron Wyden has been asking for a count of how many Americans get swept up under 702 for years. The IC has been inventing bogus explanations for why they can't do that for years. This post chronicles that process and explains why the debate is so important.

The Kelihos Pen Register: Codifying an Expansive Definition of DRAS?

When DOJ used its new Rule 41 hacking warrant against the Kelihos botnet this year, most of the attention focused on that first-known usage. But I was at least as interested in the accompanying Pen Register order, which I believe may serve to codify an expansion of the dialing, routing, addressing, and signaling information the government can obtain with a PRTT. A similar codification of an expansion exists in the HJC and Lee-Leahy bills reauthorizing 702.

The Problems with Rosemary Collyer's Shitty Upstream 702 Opinion

The title speaks for itself. I don't even consider Rosemary Collyer's 2017 approval of 702 certificates her worst FISA opinion ever. But it is part of the reason why I consider her the worst FISC judge.

It Is False that Downstream 702 Collection Consists Only of To and From Communications

I pointed out a number of things not raised in a panel on 702, not least that the authorization of EO 12333 sharing this year probably replaces some of the "about" collection function. Most of all, though, I reminded that in spite of what often gets claimed, PRISM is far more than just

communications to and from a target.

UNITEDRAKE and Hacking under FISA Orders

A document leaked by Shadow Brokers reveals a bit about how NSA uses hacking on FISA targets. Perhaps most alarmingly, the same tools that conduct such hacks can be used to impersonate a user. While that might be very useful for collection purposes, it also invites very serious abuse that might create a really nasty poisonous tree.

A Better Example of Article III FISA Oversight: Reaz Qadir Khan

In response to Glenn Gerstell's claims that Article III courts have exercised oversight by approving FISA practices (though the reality on back door searches is not so cut and dry), I point to the case of Reaz Qadir Khan where, as Michael Mosman (who happens to serve on FISC) moved towards providing a CIPA review for surveillance techniques, Khan got a plea deal.

The NSA's 5-Page Entirely Redacted Definition of Metadata

In 2010, John Bates redefined metadata. That five page entirely redacted definition became codified in 2011. Yet even as Congress moves to reauthorize 702, we don't know what's included in that definition (note: location would be included).

FISA and the Space-Time Continuum

This post talks about how NSA uses its various authorities to get around geographical and time restrictions on its spying.

The Senate Intelligence Committee 702 Bill Is a Domestic Spying Bill

This is one of the most important posts on FISA I've ever written. It explains how in 2014, to close an intelligence gap, the NSA got an exception to the rule it has to detask from a facility as soon as it identifies Americans using the facility. The government uses it to collect on Tor and, probably VPN, data. Because the government can keep entirely domestic communications that the DIRNSA has deemed evidence of a crime, the exception means that 702 has become a domestic spying authority for use with a broad range of crimes, not to mention anything the Attorney General deems a threat to national security.

"Hype:" How FBI Decided Searching 702 Content Was the Least Intrusive Means

In a response to a rare good faith defense of FBI's back door searches, I pointed out that the FBI is obliged to consider the least intrusive means of investigation. Yet, even while it admits that accessing content like that obtained via 702 is extremely intrusive, it nevertheless uses the technique routinely at the assessment level.

Other Key Posts Threads

10 Years of emptywheel: Key Non-Surveillance Posts 2008-2010

10 Years of emptywheel: Key Non-Surveillance Posts 2011-2012

10 Years of emptywheel: Key Non-Surveillance Posts 2013-2015

10 Years of emptywheel: Key Non-Surveillance Posts 2016-2017

10 Years of emptywheel: Jim’s Dimestore