SIX DATA POINTS ABOUT THE CIA DRAGNET

Last week, Ron Wyden and Martin Heinrich released a declassified letter they wrote last April, describing a CIA bulk program that had not been fully briefed to the Intelligence Committees, which violated the spirit and understanding of efforts to shut down bulk collection.

> This history demonstrates Congress's clear intent, expressed over many years and through multiple pieces of legislation, to limit, and in some cases, prohibit the warrantless collection of Americans' records, as well as the public's intense interest in and support for these legislative efforts. And yet, throughout this period, the CIA has secretly conducted it own bulk program [redacted]. It has done so entirely outside the statutory framework that Congress and the public believe govern this collection, and without any of the judicial, congressional or even executive branch oversight that comes with FISA collection.

I've been hesitating writing about it. That's true, because it's not the least little surprise to me. I've written a series of pieces describing how the self-congratulatory pieces claiming legislation passed in the wake of Snowden's leaks won't do what they say. I pointed out some of what PCLOB was likely to find when they started this review.

> Then there's bullet 4, which suggests CIA and/or NSA are collecting "within the United States or from U.S. companies."
>
> With regards collection "within the US," Mayer's post is helpful here too,

> pointing to loopholes for wireless and satellite communication.
>
> > The law that results is quite counterintuitive. If a communication is carried by radio waves, and it's one-end foreign, it falls under Executive Order 12333. If that same communication were carried by a wire, though, it would fall under FISA. (Specifically, the Section 702 upstream program.)
> >
> > As for how this Executive Order 12333 authority might be used beyond satellite surveillance, I could only speculate. Perhaps intercepting cellphone calls to or from foreign embassies?[12] Or along the national borders? At any rate, the FISA-free domestic wireless authority appears to be even broader than the Transit Authority.
>
> As far as collection outside the US, this may simply be a reference to providers voluntarily providing data under 18 U.S.C. § 2511(2)(f), as we know at least some of the telecoms do.

I pointed out that a consideration of the risks of surveillance under EO 12333 to US persons had to consider CIA's use of it (then got yelled at because I pointed out enormous blindspots in "expert" reports). I noted that when cautioning about the dragnet Donald Trump would wield, you had to consider EO 12333.

I mean, there's been a whole lot of self-congratulation since Snowden. And it has all been just that, something to brag to donors about. Because EO 12333 was always out there, and it was always possible to do virtually all

of what Snowden exposed in the Section 215 program via EO 12333.

Add that to the list of unpopular things I have said over the years that leads “experts” to prefer to ignore me.

So I assume this will be ignored like all those other warnings of precisely this moment.

Here’s where I would propose to go find the CIA dragnet.

CIA always wanted to restore its Stellar Wind component

First, remember there was a CIA component to Stellar Wind, the first dragnet set up for counterterrorism (which this program is). CIA had to do its own IG Report on Stellar Wind.

Remember that one of Bill Binney’s gripes about how NSA repurposed his surveillance was that they eliminated the encryption hiding US person identifiers, effectively making it easy to spy on US persons.

Now consider that on July 20, 2004, the CIA took the lead on pushing for the adoption of “supplemental procedures” allowing the analysis of US person metadata under EO 12333. July 20, 2004 was days after Jack Goldsmith, who had shut down parts of Stellar Wind, resigned, and the agencies immediately moved to start turning all the programs he had shut down (including both surveillance and torture) back on.

It took years to restore that access to US person data (I have a theory that Alberto Gonzales was fired because he refused to reauthorize it). But starting in 2007, expanding in 2009 (at a time when the Section 215 program was under threat), and then fully implementing in 2011 (after NSA had to shut down the PRTT program knowing full well it violated John Bates upstream order), SPCMA was rolled

out.This meant that, so long as data was collected via whatever means overseas, US person metadata could be included in the analysis.

The government has been preserving its ability to use 18 U.S.C. § 2511(2)(f)

Over a series of IG Reports written by Glenn Fine, I honed in a memo that David Barron (the OLC head who, under Obama, played a similar role as John Yoo did for George Bush) wrote seemingly authorizing using 18 U.S.C. § 2511(2)(f) to get "international" data from telecoms provided voluntarily. In 2013, David Kris confirmed that that had been happening.

In March 2021 — so before he wrote the letter just declassified but after he was briefed by PCLOB on the report on the CIA dragnet — the Congressional Research Service wrote a report on 18 U.S.C. § 2511(2)(f) for Senator Wyden. It describes how it works as an exception to FISA and other criminal laws.

> Accordingly, Section 2511(2)(f) identifies two broad categories of government activities that are exempt from Title III, the SCA, the Pen Register statute, and section 705 of the Communications Act of 1934:27 (1) the "acquisition by the United States Government of foreign intelligence information from international or foreign communications"; and (2) "foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system." These two categories are further qualified so that the exception only applies if: (3) the acquisition or the foreign intelligence activity is not "electronic surveillance" as defined

> under FISA; and (4) an "exclusivity" clause states that ECPA, the SCA, and FISA shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, and electronic communications may be conducted. Each of these clauses is discussed in more detail below.

It describes that some things don't count as an "acquisition" under FISA, such as something obtained from a telephone instrument being used in the ordinary course of business.

> Therefore, some intelligence activities that qualify as "acquisitions" for purposes of Section 2511(2)(f) may not qualify as "electronic surveillance" under FISA because the acquisition is not accomplished through an electronic, mechanical, or other surveillance device. Although FISA does not define this phrase, ECPA provides a definition of "electronic, mechanical, or other device" to mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication."46 However, this definition expressly excludes "any telephone or telegraph instrument, equipment or facility, or any component thereof" that is "being used by a provider of wire or electronic communication service in the ordinary course of its business."47

This is the kind of language that was used to treat bulk metadata as a mere business record under Section 215 after the government stopped relying exclusively on voluntary production. The bulk telephony data of all Americans was just a business record.

The report written for Ron Wyden during the same period he was writing the now unclassified letter also notes that "exclusivity" only applies to "domestic" communications, not stuff

acquired overseas.

> The exclusivity clause is first directed at interception of domestic communications, which would not appear to be affected by the previous disclaimers regarding acquisition of foreign and international communications or foreign intelligence activities directed at foreign electronic communications systems.

In other words, if telephone companies want to voluntarily give the records they otherwise keep to the IC for the purpose of foreign intelligence, it fits in this loophole. And given the realities of telecommunication, a huge percentage of "domestic" communications can be obtained overseas.

In 2013, NYT reported that AT&T was providing CIA call records

In 2013, as a bunch of different dragnets were being disclosed while everyone was looking exclusively at Section 215 and right after Kris had confirmed this application of 18 U.S.C. § 2511(2)(f), Charlie Savage described that the CIA had its own dragnet based on telephone records purchased from AT&T.

> The C.I.A. is paying AT&T more than $10 million a year to assist with overseas counterterrorism investigations by exploiting the company's vast database of phone records, which includes Americans' international calls, according to government officials.
>
> The cooperation is conducted under a voluntary contract, not under subpoenas or court orders compelling the company to participate, according to the officials. The C.I.A. supplies phone

> numbers of overseas terrorism suspects, and AT&T searches its database and provides records of calls that may help identify foreign associates, the officials said. The company has a huge archive of data on phone calls, both foreign and domestic, that were handled by its network equipment, not just those of its own customers.

Legally, this dragnet would fit solidly in the 18 U.S.C. § 2511(2)(f) loophole.

Obama's codification of EO 12333 in his final days

Insanely, Obama finished the process of reconstituting the Stellar Wind program in his final days. He did so, I've been told, in an effort to put guidelines in place (for example, Loretta Lynch adopted rules that you couldn't use EO 12333 data for political purposes, as if that would restrain Donald Trump). But I emphasized then precisely what Wyden and Heinrich are emphasizing now. There's no oversight.

> Which brings us to whether the EO sharing procedures, as released, might bind Trump anymore than EO 12333 bound Bush in 2001.
>
> In general, the sharing procedures are not even as stringent as other surveillance documents from the Obama Administration. The utter lack of any reasonable oversight is best embodied, in my opinion, by the oversight built into the procedures. A key cog in that oversight is the Department of National Intelligence's Privacy and Civil Liberties Officer – long inhabited by a guy, Alex Joel, who had no problem with Stellar Wind. That role will lead

> reviews of the implementation of this data sharing. In addition to DNI's PCLO, NSA's PCLO will have a review role, along with the General Counsels of the agencies in question, and in some limited areas (such as Attorney Client communications), so will DOJ's National Security Division head.
>
> What the oversight of these new sharing procedures does not include is any statutorily independent position, someone independently confirmed by the Senate who can decide what to investigate on her own. Notably, there is not a single reference to Inspectors General in these procedures, even where other surveillance programs rely heavily on IGs for oversight.
>
> There is abundant reason to believe that the PATRIOT Act phone and Internet dragnets violated the restrictions imposed by the FISA Court for years in part because NSA's IG's suggestions were ignored, and it wasn't until, in 2009, the FISC mandated NSA's IG review the Internet dragnet that NSA's GC "discovered" that every single record ingested under the program violated FISC's rules after having not discovered that fact in 25 previous spot checks. In the past, then, internal oversight of surveillance has primarily come when IGs had the independence to actually review the programs.
>
> Of course, there won't be any FISC review here, so it's not even clear whether explicit IG oversight of the sharing would be enough, but it would be far more than what the procedures require.
>
> I'd add that the Privacy and Civil Liberties Oversight Board, which provided key insight into the Section 215 and 702 programs, also has no role —

> except that PCLOB is for all intents and purposes defunct at this point, and there's no reason to believe it'll become operational under Trump.

I guess I was wrong about PCLOB. It did get reconstituted, and seven years after the EO 12333 review started we're getting dribbles about what it found!

And in fact if this whole discussion didn't make me crabby, I'd point out details from the PCLOB report that suggest things aren't as bad as I thought they'd get in 2017, when this dragnet was handed over to Donald Trump.

So I'm not entirely a pessimist!

PCLOB only has authority over counterterrorism programs

The only problem with being proven wrong about PCLOB, however, is even though there were efforts to expand its mandate during the Trump years, those efforts failed.

It can only look at counterterrorism programs.

So there could be a parallel program used for counterintelligence (indeed, the sharing rules make it quite clear there's a CI purpose for it), and we'd never get oversight over it. So Wyden and Heinrich should be pushing to get a full briefing on the CI version of this, because it's there, I would bet you a lot of money.

Anyway, if you want to find the CIA dragnet, you can look at my warnings over the last 9 years (or Charlie Savage's report on it from 2013). Or you can look at the loophole that 18 U.S.C. § 2511(2)(f) creates, Ron Wyden was exploring closely when he was writing this letter. Another place you might look is AT&T's earnings

statements.