

THE IRONIES OF THE EO 12333 SHARING EXPANSION FOR OBAMA AND TRUMP

In one of his first acts as leader of the Democratic party in 2008, Barack Obama flipped his position on telecom immunity under FISA Amendments Act, which cleared the way for its passage. That was a key step in the legalization of the Stellar Wind dragnet illegally launched by George Bush in 2001, the normalization of turnkey surveillance of the rest of the world, surveillance that has also exposed countless Americans to warrantless surveillance.

Bookends of the Constitutional law president's tenure: codifying and expanding Stellar Wind

So it is ironic that, with one of his final acts as President, Obama completed the process of normalizing and expanding Stellar Wind with the expansion of EO 12333 information sharing.

As I laid out some weeks ago, on January 3, Loretta Lynch signed procedures that permit the NSA to share its data with any of America's other 16 intelligence agencies. This gives CIA direct access to NSA data, including on Americans. It gives all agencies who jump through some hoops that ability to access US person metadata available overseas for the kind of analysis allegedly shut down under USA Freedom Act, with far fewer limits in place than existed under the old Section 215 dragnet exposed by Edward Snowden.

And it did so just as an obvious authoritarian

took over the White House.

I've was at a privacy conference in Europe this week (which is my partial explanation for being AWOL all week), and no one there, American or European, could understand why the Obama Administration would give Trump such powerful tools.

About the only one who has tried to explain it is former NSA lawyer Susan Hennessey in this Atlantic interview.

12333 is not constrained by statute; it's constrained by executive order. In theory, a president could change an executive order—that's within his constitutional power. It's not as easy as just a pen stroke, but it's theoretically possible.

[snip]

When they were in rewrites, they were sort of vulnerable. There was the possibility that an incoming administration would say, "Hey! While you're in the process of rewriting, let's go ahead and adjust some of the domestic protections." And I think a reasonable observer might assume that while the protections the Obama administration was interested in putting into place increased privacy protections—or at the very least did not reduce them—that the incoming administration has indicated that they are less inclined to be less protective of privacy and civil liberties. So I think it is a good sign that these procedures have been finalized, in part because it's so hard to change procedures once they're finalized.

[snip]

I think the bottom line is that it's comforting to a large national-security community that these are procedures that

are signed off by Director of National Intelligence James Clapper and Attorney General Loretta Lynch, and not by the DNI and attorney general that will ultimately be confirmed under the Trump Administration.

Hennessey's assurances ring hollow. That's true, first of all, because it is actually *easier* to change an EO – and EO 12333 specifically – than “a pen stroke.” We know that because John Yoo did just that, in authorizing Stellar Wind, when he eliminated restrictions on SIGINT sharing without amending EO 12333 at all. “An executive order cannot limit a President,” Yoo wrote in the 2001 memo authorizing Stellar Wind. “There is no constitutional requirement for a President to issue a new executive order whenever he wishes to depart from the terms of a previous executive order. Rather than violate an executive order, the President has instead modified or waived it.” And so it was that the NSA shared Stellar Wind data with CIA, in violation of the plain language of EO 12333 Section 2.3, until that sharing was constrained in 2004.

Yes, in 2008, the Bush Administration finally changed the language of 2.3 to reflect the SIGINT sharing it had started to resume in 2007-2008. Yes, this year the Obama Administration finally made public these guidelines that govern that sharing. But recent history shows that no one should take comfort that EOs can bind a president. They cannot. The Executive has never formally retracted that part of the 2001 opinion, which in any case relies on a 1986 OLC opinion on Iran-Contra arguing largely the same thing.

**No statutorily
independent oversight**

over vastly expanded information sharing

Which brings us to whether the E0 sharing procedures, as released, might bind Trump anymore than E0 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.

Obama vastly expanded information sharing with these procedures without implementing the most obvious and necessary oversight over that sharing, statutorily independent oversight.

Limits on using the dragnet to affect political processes

There is just one limit in the new procedures that I think will have any effect whatsoever – but I think Trump may have already moved to undercut it.

The procedures explicitly prohibit what everyone should be terrified about under Trump – that he'll use this dragnet to persecute his political enemies. Here's that that prohibition looks like.

Any IC element that obtains access to raw SIGINT under these Procedures will:

[snip]

Political process in the United States.

Not engage in any intelligence activity authorized by these Procedures,

including disseminations to the White House, for the purpose of affecting the political process in the United States.

The IC element will comply with the guidance applicable to NSA regarding the

application of this prohibition. Questions about whether a particular activity falls within this prohibition will be resolved in consultation with the element's legal counsel and the General Counsel of the Office of the Director of National Intelligence (ODNI) (and the DoD's Office of the General Counsel in the case of a DoD IC element).

If you need to say the IC should not share data with the White House for purposes of affecting the political process, maybe your info sharing procedures are too dangerous?

Anyway, among the long list of things the IC is not supposed to do, this is the only one that I think is so clear that it would likely elicit leaks if it were violated (though obviously that sharing would have to be discovered by someone inclined to leak).

All that said, note who is in charge of determining whether something constitutes affecting political processes? The IC agency's and ODNI's General Counsel (the latter position is vacant right now). Given that the Director of National Intelligence is one of the positions that just got excluded from de facto participation in Trump's National Security Council (in any case, Republican Senator Dan Coats has been picked for that position, which isn't exactly someone you can trust to protect Democratic or even democratic interests), it would be fairly easy to hide even more significant persecution of political opponents.

FBI and CIA's expanded access to Russian counterintelligence information

There is, however, one aspect of these sharing

guidelines that may have work to limit Trump's power.

In the procedures, the conditions on page 7 and 8 under which an American can be spied on under EO 12333 are partially redacted. But the language on page 11 (and in some other parallel regulations) make it clear one purpose under which such surveillance would be acceptable, as in this passage.

Communications solely between U.S. persons inadvertently retrieved during the selection of foreign communications will be destroyed upon recognition, except:

When the communication contains significant foreign intelligence or counterintelligence, the head of the recipient IC element may waive the destruction requirement and subsequently notify the DIRNSA and NSA's OGC;

Under these procedures generally, communications between an American and a foreigner can be read. But communications between Americans must be destroyed except if there is significant foreign intelligence *or counterintelligence* focus. This EO 12333 sharing will be used not just to spy on foreigners, but also to identify counterintelligence threats (which would presumably include leaks but especially would focus on Americans serving as spies for foreign governments) within the US.

Understand: On January 3, 2017, amid heated discussions of the Russian hack of the DNC and public reporting that at least four of Trump's close associates may have had inappropriate conversations with Russia, conversations that may be inaccessible under FISA's probable cause standard, Loretta Lynch signed an order permitting the bulk sharing of data to (in part) find counterintelligence threats in the US.

This makes at least five years of information collected on Russian targets available, with few

limits, to both the CIA and FBI. So long as the CIA or FBI were to tell DIRNSA or NSA's OGC they were doing so, they could even keep conversations *between Americans* identified "incidentally" in this data.

I still don't think giving the CIA and FBI (and 14 other agencies) access to NSA's bulk SIGINT data with so little oversight is prudent.

But one of the only beneficial aspects of such sharing might be if, before Trump inevitably uses bulk SIGINT data to persecute his political enemies, CIA and FBI use such bulk data to chase down any Russian spies that may have had a role in defeating Hillary Clinton.