

SECTION 309: A BAND-AID FOR A GAPING WOUND IN DEMOCRACY



Metadata: Someone surveilling our conversation “connection chained” Bob Litt and me chatting about spying on Americans in the Hayek Auditorium at CATO on 12/12/14.

On Friday, officials from James Clapper’s office confirmed in a number of different ways that the government obtains “vast troves” of Americans’ communication overseas. And rather than enforce Dianne Feinstein and Mark Udall’s suggestion that the intelligence community treat it under FISA – as the spirit of FISA Amendment Acts, which extended protection to Americans abroad, would support – Congress instead passed Section 309, a measure to impose limited protections on vast unregulated spying on Americans.

This all happened at CATO’s conference on surveillance, an awesome conference set up by Julian Sanchez.

My panel (moderated very superbly by Charlie

Savage) revisited at length the debate between former State Department whistleblower John Napier Tye and Director of National Intelligence Civil Liberties Officer Alex Joel (into which I stuck my nose). As he did in his Politico post responding to Tye's alarms about the risk of EO 123333 collection against Americans to democracy, Joel pointed to the topical limits on bulk collection Obama imposed in his Presidential Policy Directive 28, which read,

The United States must consequently collect signals intelligence in bulk in certain circumstances in order to identify these threats. Routine communications and communications of national security interest increasingly transit the same networks, however, and the collection of signals intelligence in bulk may consequently result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value. The United States will therefore impose new limits on its use of signals intelligence collected in bulk. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside.

In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S

or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.

I noted – as I did in my Salon piece on the topic – that bulk collection for even just one topic means the collection of everything, as counterterrorism serves as the excuse to get all phone records in the US in the phone dragnet. Joel did not dispute that, explaining that PPD-28 only limits the *use* of data that has been bulk collected to these six purposes. PPD-28 does nothing to limit bulk collection itself. Though the fact that these limitations have forced a change in how the NSA operates is testament that they were using data collected in bulk for even more reasons before January.

The NSA is, then, aspiring to collect it all, around the world.

Which was a point confirmed in an exchange between Joel and Tye. Joel claimed we weren't collecting nearly all of the Internet traffic out there, saying it was just a small fraction. Tye said that was disingenuous, because 80% of Internet traffic is actually things like Netflix. Tye stated that the NSA does collect a significant percentage of the remainder (he implied most, but I'd want to see the video before I characterize how strongly he said that).

Again, collect it all.

Our panel didn't get around to talking about Section 309 of the Intelligence Authorization, which I examined here. The Section imposes a 5 year retention limit on US person data except for a number of familiar purposes – foreign intelligence, evidence of a crime, encryption, all foreign participants, tech assurance or compliance, or an Agency head says he needs to retain it longer (which requires notice to Congress). Justin Amash had argued, in an

unsuccessful attempt to defeat the provision, that the measure provides affirmative basis for sharing US person content collected under EO 12333.

In a later panel at the CATO conference, DNI General Counsel Bob Litt said that the measure doesn't change anything about what the IC is already doing. Rather, it just imposes new limits, and the IC didn't want the measure (my guess is it will be most onerous because it demands affirmative determinations of either foreign intelligence purpose or all-foreign participants in communications, which will require the IC to do more work or broader purging, including of non-US person data, with the data they obtain).

When I asked a question during Q&A (about FBI oversight) he asked if his comments about 309 had convinced me, and we continued the discussion after the panel (he made it clear Joel had told him during the day we hadn't talked about it – we ran out of time on our panel). And I noted, first, that the many non-credible claims the Executive had made that Congress had ratified the phone dragnet with its extensions of the PATRIOT Act – which I noted was aggressive lawyering on Litt and others' part – had damaged their credibility on claims like this. I then asked, whether this just dealt with the "vast trove" of data Mark Udall had described in February.

Udall: I want to talk about Executive Order 12333, with which you're familiar. I understand that the collection, retention, or dissemination of information about US persons is prohibited under Executive Order 12333 except under certain procedures approved by the Attorney General. But this doesn't mean that US person information isn't mistakenly collected or obtained and then disseminated outside these procedures, so take this example. Let's say the NSA's conducting what it

believes to be foreign to foreign collection under EO 12333 but discovers in the course of this collection that it also incidentally collected a vast trove of US person information. That US person collection should now have FISA protections. What role does the NSD have in overseeing any collection, retention, or dissemination of US person information that might occur under that executive order?

While Litt made it clear it dealt with all incidentally collected content, including from other authorities, and he definitely said nothing like, "I am affirmatively confirming that that 'vast trove' Udall raised hypothetically exists in actual fact," he did agree that's what this is about. As I noted, both the spirit of FISA Amendments Act, which rules that US persons should be protected overseas as well as in the US, and both Udall and Dianne Feinstein, suggested this should be afforded the protections of FISA. In our conversation, Litt claimed Congress had affirmatively declined to include such materials in 1978, which I noted was a time when such bulk collection of US data was not possible overseas.

But instead of extending FISA (which is already inadequate to the technology of bulk collection), Congress instead moved to impose some retention limits *but not use limits* on this data. Indeed, the permitted reasons for retention, and Litt's insistence that this doesn't change what they're already doing, suggests they're already using this data for broad purposes, though the really unlimited use of it would be limited to metadata analysis.

At the very least, this means the government is able to engage in metadata analysis of Americans for far more uses than permitted under FISA, and do so without the First Amendment review required under FISA. It means NSA can construct the dossiers based on metadata on Americans so long as they do it with EO 12333 data. The use

of E0 12333 also provides a way for the Attorney General to authorize spying on content that will only, with the new provision, receive outside oversight after 5 years.

Between Litt's broadcast comments Friday (which Edward Snowden emphasized in his appearance at the conference) as well as comments made in the House in response to Amash's challenge, there exists abundant record that the IC is not claiming new affirmative authorities.

But why should they? What they are instead now confirming is they have already been using US person data collected under E0 12333 – and not just metadata.

Bob Litt may take solace that, back when I was 10 and he was not far out of law school, Congress chose not to regulate spying overseas. But they've repeatedly tried to regulate spying on Americans, both metadata and content, since then. And the claim that the IC didn't even want to limit data retention to affirmative foreign intelligence purposes after hoarding vast troves of US person for 5 years (during which point they don't have to claim it's foreign intelligence information), they seem to have violated Congress' repeated efforts to protect Americans except in case of a foreign intelligence purpose.

Of course, Congress' only response to that was to pass Section 309, not to do anything about the larger risks of spying on Americans (with the related overcollection on foreigners).