PCLOB'S NEW WORK: EXAMINING "ACTIVITIES" TAKING PLACE IN THE LOOPHOLES OF EO 12333

On Wednesday, the Privacy and Civil Liberties Oversight Board met to approve its next project. They are just about completing a general overview of the Intelligence Community's use of EO 12333 (as part of which they've been nagging agencies, notably DEA and Treasury, to comply with requirements imposed by Ronald Reagan). Next, they will move onto a deep dive of two programs conducted under EO 12333, one each for NSA and CIA. PCLOB has now posted materials from Wednesday's meeting, though this overview is also useful.

Keeping in mind that PCLOB already has a pretty good sense of what the agencies are doing, consider this description of its deep dive into activities of NSA and CIA.

> During the next stage of its inquiry, the Board will select two counterterrorism-related activities governed by E.O. 12333, and will then conduct focused, in-depth examinations of those activities. The Board plans to concentrate on activities of the CIA and NSA, and to select activities that involve one or more of the following: (1) bulk collection involving a significant chance of acquiring U.S. person information; (2) use of incidentally collected U.S. person information; (3) targeting of U.S. persons; and (4) collection that occurs within the United States or from U.S. companies. Both reviews will involve

> assessing how the need for the activity in question is balanced with the need to protect privacy and civil liberties. The reviews will result in written reports and, if appropriate, recommendations for the enhancement of civil liberties and privacy.

Some of this is unsurprising. If PCLOB were to conduct a review of SPCMA, it would be assessing NSA's analysis of incidentally collected US person data collected in great volume as a result of collecting in bulk. Indeed, conducting such a review would get to a lot of the issues raised by John Napier Tye in PCLOB testimony.

But I'm more interested in bullets 3 and 4.

Bullet 3 suggests that CIA and/or NSA are targeting US persons under EO 12333.

There are certainly ways that's permissible. For example, EO 12333 permits agencies to conduct physical surveillance of their employees.

> (1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and
>
> (2) Physical surveillance of a military person employed by a non-intelligence element of a military service;

And it permits physical surveillance overseas if significant information can't reasonably acquired by other means.

> Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

You'd think this would bump up against the FISA

Amendments Act very quickly, but remember that this EO was updated in the days after FAA was completed, so everything in it likely accounts for FAA.

On that note, this useful post from Jonathan Mayer (click through for the handy graphic) describes how NSA's classified EO 12333 permits the Attorney General to authorize the surveillance of US persons or entities for limited periods of time.

> A third area of Executive Order 12333, on American soil, is the "Classified Annex Authority" or "CAA." Its source is a classified addition to Executive Order 12333, set out in an NSA policy document.[13] The most recent revision, from 2009, reads:
>
> > Communications of or concerning a United States person[14] may be intercepted intentionally or selected deliberately . . .
> >
> > with specific prior approval by the Attorney General based on a finding by the Attorney General that there is probable cause to believe the United States person is an agent of a foreign power and that the purpose of the interception or selection is to collect significant foreign intelligence. Such approvals shall be limited to a period of time not to exceed ninety days for individuals and one year for entities.
>
> That provision appears to allow the Attorney General to unilaterally trump FISA. I'm not*entirely* confident that's what it means, but it sure looks like it.[15]
>
> I'm skeptical that the executive branch

> can just brush aside FISA, especially on American soil. In Justice Jackson's famous phrasing, when the executive branch acts in clear violation of a legislative enactment, its "power is at its lowest ebb." Nevertheless, the executive branch does appear to claim that Article II can override FISA, and it does appear to have invoked this Classified Annex Authority on occasion.[16]

Finally, remember that CIA has conducted investigations targeting Senate Intelligence Committee staffers, which suggests it interprets its ability to conduct counterintelligence investigations unbelievably broadly.

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.

But we also know NSA and its partner GCHQ have stolen unencrypted US company data overseas. And while the theft off Google's fiber has, hopefully, been stopped, there's still quite a lot of ways NSA can steal this data.

In any case, the terms of PCLOB's investigation sure seem to suggest that CIA and/or NSA are exploiting the holes in EO 12333 in significant enough ways to raise concerns for PCLOB.