EO 12333 THREATENS OUR DEMOCRACY

Among the many posts I've written about Executive Order 12333 — the order that authorizes all non-domestic spying — includes this post, where I noted that proposed changes to NSA's phone dragnet won't affect programs authorized by EO 12333.

> Obama was speaking only about NSA's treatment of Section 215 metadata, not the data — which includes a great amount of US person data — collected under Executive Order 12333.
>
> [snip]
>
> Section 215 metadata has different and significantly higher protections than EO 12333 phone metadata because of specific minimization procedures imposed by the FISC (arguably, **the program doesn't even meet the minimization procedure** requirements mandated by the law). We've seen the implications of that, for example, when the NSA **responded** to being caught watch-listing 3,000 US persons without extending First Amendment protection not by stopping that tracking, but simply cutting off the watch-list's ability to draw on Section 215 data.
>
> Basically, the way NSA treats data collected under FISC-overseen programs (including both Section 215 and FISA Amendments Act) is to throw the data in with data collected under EO 12333, but add query screens tied to the more strict FISC-regulations governing production under it.
>
> [snip]
>
> NSA's spokeswoman will say over and over that "everyday" or "ordinary" Americans

> don't have to worry about their favorite software being sucked up by NSA. But to the extent that collection happens under EO 12333, they have relatively little protection.

That's precisely the point made in an important op-ed by the State Department's former Internet freedom chief, John Napier Tye, who had access to data from EO 12333 collection.

> Bulk data collection that occurs inside the United States contains built-in protections for U.S. persons, defined as U.S. citizens, permanent residents and companies. Such collection must be authorized by statute and is subject to oversight from Congress and the Foreign Intelligence Surveillance Court. The statutes set a high bar for collecting the content of communications by U.S. persons. For example, Section 215 permits the bulk collection only of U.S. telephone metadata — lists of incoming and outgoing phone numbers — but not audio of the calls.
>
> Executive Order 12333 contains no such protections for U.S. persons if the collection occurs outside U.S. borders.
>
> [snip]
>
> Unlike Section 215, the executive order authorizes collection of the content of communications, not just metadata, even for U.S. persons. Such persons cannot be individually targeted under 12333 without a court order. However, if the contents of a U.S. person's communications are "incidentally" collected (an NSA term of art) in the course of a lawful overseas foreign intelligence investigation, then Section 2.3(c) of the executive order explicitly authorizes their retention. It does not require that the affected U.S. persons

> be suspected of wrongdoing and places no limits on the volume of communications by U.S. persons that may be collected and retained.

Tye reveals that a document the White House provided to Congress said it had no intention of limiting back door searches of EO 12333 collected data because it would require too many changes to existing programs.

> In that document, the White House stated that adoption of Recommendation 12 [which would requiring purging US person data] would require "significant changes" to current practice under Executive Order 12333 and indicated that it had no plans to make such changes.

And Tye implies that NSA is using EO 12333 to conduct the Internet dragnet.

> All of this calls into question some recent administration statements. Gen. Keith Alexander, a former NSA director, has said publicly that for years the NSA maintained a U.S. person e-mail metadata program similar to the Section 215 telephone metadata program. And he has maintained that the e-mail program was terminated in 2011 because "we thought we could better protect civil liberties and privacy by doing away with it."Note, however, that Alexander never said that the NSA stopped collecting such data — merely that the agency was no longer using the Patriot Act to do so. I suggest that Americans should dig deeper.

I have made repeatedly covered SPCMA, the EO 12333 authorized Internet dragnet, which the government rolled out just as it was shutting down its PATRIOT-authorized Internet dragnet.

Because you've been reading me, you already knew what most others are only discovering because of this op-ed.

The most important point Tye made — it's one I've made too, but it can't be said enough — is this:

> The [Executive] order as used today threatens our democracy.

There is almost no oversight over this — and when Mark Udall suggested DOJ should exercise more of a role, the AAG for National Security showed no interest. This is the executive choosing to spy on Americans outside of all oversight.

That's a threat to our democracy.