MINIMIZATION IN THE AGE OF CYBERWAR

I'd like to compare how the NSA talking point document released yesterday compares with a document Glenn Greenwald has or has seen, with respect to minimization under Section 702 (PRISM/FAA) collection. Remember PRISM allows the government to access Internet communications with little review of individual targeting decisions, and any American communications accessed with that foreign target communication is also viewed.

The NSA document says US person communications can only be disseminated (this includes getting shared with FBI) if it is necessary to understand the communication, and evidence of crime, or indicates a threat of death.

> The dissemination of any information about U.S. persons is expressly prohibited unless it is necessary to understand foreign intelligence or assess its importance; is evidence of a crime; or indicates a threat of death or serious bodily harm.

The Guardian document (which they did not publish) says US person communications — and note, these are entirely domestic communications — can be disseminated in two slightly different cases and a third unrelated one. The unrelated one permits US person communications to be disseminated if it contains "information necessary to understand or assess a communications security vulnerability."

> One typical example is a document submitted by the NSA in July 2009. In its first paragraph, it purports to set forth "minimization procedures" that "apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that

> is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended."
>
> That document provides that "communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data." It also states that "such communications or information" – those from US citizens – "may be retained and disseminated" if it meets the guidelines set forth in the NSA's procedures.
>
> Those guidelines specifically address what the NSA does with what it calls "domestic communications", defined as "communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition". The NSA expressly claims the right to store and even disseminate such domestic communication if: (1) "it is reasonably believed to contain significant foreign intelligence information"; (2) "the communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed"; or (3) "the communication is reasonably believed to contain technical data base information, as defined in Section 2(i), or information necessary to understand or assess a communications security vulnerability." [my emphasis]

Now, this is not an apple to apple comparison. Indeed, this could very well be an apples to

small rubber child's ball comparison.

The NSA document purports to describe minimization as it occurs today. The Guardian one dates to July 2009, so may be out of date, for starters.

And by design, the NSA timeline focuses on terrorism examples because TERROR TERROR TERROR is very convincing to people who don't want to think. Based on the mention of a "communications security vulnerability," the Guardian one seems to be a 702 order describing minimization for a cybersecurity order.

If that's true, though, it suggests two things. First, that hacking has been equated to terrorism as a crime adequate to disseminate US person communications with no warrant.

And this is where the difference in the standard on foreign intelligence gets interesting: the NSA document claims that only communications necessary to understand foreign intelligence merits dissemination. The Guardian document only need be "reasonably believed to contain significant foreign intelligence information" (though admittedly, that may be the language used in the first instance).

But again, this minimization order is 4 years old. The other day the WaPo suggested that the NSA has changed how they collect Internet metadata (which may be what that other clause "technical data base information, as defined in Section 2(i)" in the minimization order refers to. It may be they're conducting their cybersecurity dragnet via other means, perhaps even as a way to maintain this lower standard of minimization.

The government is clearly planning to engage in far more intrusive collection in the name of cyberwar than described in discussions about Section 702 (and at the end of the hearing yesterday, Mike Rogers alluded to keeping the programs in place, with their permissive standards, for other reasons, which I took to mean cybersecurity). And that is bound to treat

far more Americans as targets of foreign-type collection.