THE 6-MONTH REVIEW

In Lichtblau and Risen's piece on the ongoing warrantless wiretap problems, they report that the problems were identified in preparation of a semiannual review of the warrantless wiretap program.

> The overcollection problems appear to have been uncovered as part of a twice-annual certification that the Justice Department and the director of national intelligence are required to give to the Foreign Intelligence Surveillance Court on the protocols that the N.S.A. is using in wiretapping. That review, officials said, began in the waning days of the Bush administration and was continued by the Obama administration. It led intelligence officials to realize that the N.S.A. was improperly capturing information involving significant amounts of American traffic.

Best as I can tell, this is the semiannual assessment in question.

> ''(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to—
>
> ''(A) the Foreign Intelligence Surveillance Court; and
>
> ''(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

> > ''(i) the congressional intelligence committees; and
> >
> > ''(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

So, basically, every six months, the DNI and AG need to look at the program and see whether the NSA is complying with the targeting and minimization requirements of the law.

The targeting language basically says NSA cannot intentionally target US persons.

> ''(b) LIMITATIONS.—An acquisition authorized under subsection (a)—
>
> ''(1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> ''(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> ''(3) may not intentionally target a United States person reasonably believed to be located outside the United States;
>
> ''(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
>
> ''(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

And the minimization requirements require that incidentally collected US person data must not be circulated improperly and must be destroyed.

> (h) "Minimization procedures", with

respect to electronic surveillance, means—

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section

> 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

In short, they were preparing to do a report on whether they were complying with requirements that:

- No US person data be collected intentionally
- The amount of US person data incidentally collected must be minimized
- Incidentally collected US person data cannot be disseminated (though there's a giant loophole for "foreign intelligence information")
- Unless they have a court order, US person data must be destroyed within 72 hours

In preparing this report, NSA determined it was out of compliance.

Two things Russ Feingold has said suggest that the loopholes in the dissemination of "foreign intelligence information" and for retaining US person data may have been exploited. First, in his statement today, Feingold said,

> In addition, the administration should declassify certain aspects of how these authorities have been used so that the American people can better understand their scope and impact.

And, during David Kris' confirmation hearing on February 25 (at which point Holder would presumably have already delayed the report), Feingold and Kris had this exchange:

> SEN. FEINGOLD: We had an opportunity – and you can respond in a minute – but we had an opportunity earlier today to discuss in a classified setting specific concerns I have about how the FISA amendment act has been implemented. Without discussing those specifics in an open hearing, do you agree that there are serious problems that need to be corrected?
>
> MR. KRIS: Senator, I do, I appreciate very much the meeting we had this morning, you raised a number of concerns that I as an outsider had not appreciated and you certainly got my attention. I have been thinking about it since we met and if it's even possible you increased my desire to, if I were to be confirmed, to get to the bottom of the FISA amendments act and I hope if I am confirmed that I can take advantage of your learning of others on the committee and the intelligence committee to see how best to make any necessary improvements.

In other words, at around the same time as Holder was scrambling to fix this problem, Feingold was surprising David Kris–who at the time had probably the best understanding of what the illegal program was and current program is of anyone not yet read into the program–with details on how it had been used.

All of which suggests that NSA was already using all the loopholes at its disposal (I'll explain later why I'm all but certain, for example, that they have been keeping US person data for more than 72 hours with the approval of FISC). But even still, they were out of compliance.

That either means they were intentionally unintentionally collecting US person data.

Or they were disseminating incidentally collected US person data.

Given that data mining is part of this program, I’m guessing it means they’re still data mining US person data, whether or not that US person data has any ties to terrorism or foreign intelligence.