DENNIS BLAIR'S SPOKESPERSON: THE DOMESTIC SURVEILLANCE PROGRAM VIOLATES THE FOURTH AMENDMENT

I've already posted on the general contents of Lichtblau and Risen's seemingly quarterly report that illegal wiretapping is still going on—including the eye-popping news that Bill Clinton's emails were illegally accessed. But I wanted to focus on one really critical passage of the story.

> The N.S.A. declined to comment for this article. Wendy Morigi, a spokeswoman for Dennis C. Blair, the national intelligence director, said that because of the complex nature of surveillance and **the need to adhere to the rules of the Foreign Intelligence Surveillance Court, the secret panel that oversees surveillance operation, and "other relevant laws and procedures, technical or inadvertent errors can occur."**
>
> "When such errors are identified," Ms. Morigi said, "they are reported to the appropriate officials, and corrective measures are taken." [my emphasis]

The DNI is basically blaming its "technical or inadvertent errors" [no word about Clinton's emails, which can't be inadvertent] on "the need to adhere to the rules of FISC and other relevant laws **and procedures**."

Not only does this not make sense, but it completely undercuts any claim that this program is legal under the Fourth Amendment.

In one of the most important posts of mine that

few people ever read, I explained why. I showed that the FISA Court of Review understood the Protect America Act (and I believe the same holds true for the FISA Amendment Act program) does not, by itself, comply with the Fourth Amendment. Rather, the FISCR explicitly said that the wiretap program only complied with the Fourth Amendment's probable cause requirement through the application of a provision in Executive Order 12333 that requires only that the Attorney General "determine" that surveillance is directed against an agent of a foreign power. And the PAA program (and, I assume, the FAA program) only complies with the Fourth Amendment's requirement for particularity through a set of procedures not mandated by PAA or FAA, and not shared with the telecoms handing over their customer data.

The FISCR explained:

> The petitioner's arguments about particularity and prior judicial review are defeated by the way in which the statute has been applied. When combined with the PAA's other protections, the [redacted] procedures and the procedures incorporated through the Executive Order are constitutionally sufficient compensation for any encroachments.
>
> The [redacted] procedures [redacted] are delineated in an ex parte appendix filed by the government. They also are described, albeit with greater generality, in the government's brief. [redacted] Although **the PAA itself does not mandate a showing of particularity**, see 50 USC 1805b(b), **this pre-surveillance procedure strikes us as analogous to and in conformity** with the particularity showing contemplated by *Sealed Case*. [my emphasis]

These are precisely the procedures, I suspect, that the DNI's office is now **blaming** for the "inadvertent" review of US person emails.

And you can see why, from the rest of the article. Knowing that these procedures are the only thing fulfilling the Fourth Amendment's requirement for particularity, read this passage, which appears to describe precisely the procedures in question.

> He said he and other analysts were trained to use a secret database, code-named Pinwale, in 2005 that archived foreign and domestic e-mail messages. He said Pinwale allowed N.S.A. analysts to read large volumes of e-mail messages to and from Americans as long as they fell within certain limits — no more than 30 percent of any database search, he recalled being told — and Americans were not explicitly singled out in the searches.
>
> The former analyst added that his instructors had warned against committing any abuses, telling his class that another analyst had been investigated because he had improperly accessed the personal e-mail of former President Bill Clinton.

Well, no wonder the procedures don't prevent the "inadvertent" access of emails!!! The procedures start by allowing analysts to review 30% of every database search!! So already, a US person has a 30% chance that her emails will get swept up and reviewed by someone at NSA!! And the NSA is relying on just those procedures to prevent someone from giving into natural curiosity to access, say, the ex-President's emails, if they happen to be among the 30% of emails he accesses.

And then there's the possibility that the NSA will just happen to suck up and review an extra thousand emails in its search.

> "Say you get an order to monitor a block of 1,000 e-mail addresses at a big corporation, and instead of just

> monitoring those, the N.S.A. also monitors another block of 1,000 e-mail addresses at that corporation," one senior intelligence official said. "That is the kind of problem they had."

A thousand extra email addresses here and a thousand extra email addresses there, and pretty soon you've thrown all claim to particularity out the window. (Incidentally, the people serving as sources for this story aren't fucking around—the surest way to get people concerned about domestic surveillance is to tell them their business emails are being monitored.)

So here's what we know about our nation's domestic surveillance program:

1. The FISA Court of Review has revealed that the only thing that fulfills the Fourth Amendment's particularity requirement is a set of secret procedures
2. The DNI has suggested that those procedures don't work

Call me crazy, but between the DNI and the FISCR, I think they've made the case that their own program is illegal.