TECHNICAL GLITCHES AND MINIMIZATION

A number of you sent me this Eric Lichtblau story describing how, because of a "technical glitch," the FBI accidentally got all the emails going to one domain, rather than just the emails to and from their particular target.

> A technical glitch gave the F.B.I. access to the e-mail messages from an entire computer network — perhaps hundreds of accounts or more — instead of simply the lone e-mail address that was approved by a secret intelligence court as part of a national security investigation, according to an internal report of the 2006 episode.
>
> F.B.I. officials blamed an “apparent miscommunication” with the unnamed Internet provider, which mistakenly turned over all the e-mail from a small e-mail domain for which it served as host. The records were ultimately destroyed, officials said.
>
> Bureau officials noticed a “surge” in the e-mail activity they were monitoring and realized that the provider had mistakenly set its filtering equipment to trap far more data than a judge had actually authorized.
>
> The episode is an unusual example of what has become a regular if little-noticed occurrence, as American officials have expanded their technological tools: government officials, or the private companies they rely on for surveillance operations, sometimes foul up their instructions about what they can and cannot collect.
>
> The problem has received no discussion as part of the fierce debate in Congress about whether to expand the government’s

> wiretapping authorities and give legal immunity to private telecommunications companies that have helped in those operations.
>
> But an intelligence official, who spoke on condition of anonymity because surveillance operations are classified, said: “It’s inevitable that these things will happen. It’s not weekly, but it’s common.”

My response to this is sort of similar to Kagro X’s (and given all my posts about minimization, I would certainly take issue with Lichtblau’s assertion that "the problem has received no discussion"). This story illustrates why minimization is every bit as important in the FISA discussion as immunity.

> Hmm. Minimization. That rings a bell. What was it?
>
> Oh yeah! The FISA fight in the Senate! Minimization was a concern because the Senate bill pretty much gave the government a free hand to suck up every phone call, e-mail, text message, etc. there is, and — amazingly enough — had to be amended on the floor in order to even approach a proper handling of minimization concerns. Curiously, it happened that there was no provision in the new law that said what actually happens if the government, oh, let’s say… *doesn’t* destroy "accidentally" captured communications. Senator Whitehouse had to try to shoehorn that in as an amendment, and along the way had to agree to soften his language from explicitly authorizing compliance reviews by the FISA court, down to some mumblings about how nothing in the bill should be construed to reduce or contravene the FISA court’s inherent authority to enforce its orders regarding minimization (if any).

> Subtle difference, I suppose. The affirmative power to conduct reviews, versus a grudging acknowledgment that a court should be able to enforce its own orders. But not that subtle.

The story actually does sound a genuine mistake. It illustrates the need for minimiz ation. But it doesn't explain why it is that McConnell apparently abandoned the Democratic bills in August 2007 because they actually required minimization. It doesn't explain why the Administration is so afraid of oversight on their ability to minimize US person data.

See, I'm not so much worried about mistakes like this. I'm worried about the apparent fact that having real oversight to find the non-mistakes was a deal-breaker in August.