JOHN BATES' TWO WIRETAPPING WARNINGS: WHY THE GOVERNMENT TOOK ITS INTERNET DRAGNET COLLECTION OVERSEAS

A couple of us were joking on Twitter the other day that the June-July 2010 John Bates opinion released the other day — in which he yelled mightily about illegal collection that had persisted for 5 years but then rubber stamped the government's plan to vastly expand metadata collection — ought to lead to the term "Bates stamp" to take on new meaning, a rubber stamp by a FISC judge.

(I'm working on a separate post that shows the timing of all this, but for the moment, you'll have to trust me that Bates' opinion was written some time around July 2010.)

Bates did, however, sort of kind of rein in the government's actions, spending the last 17 pages of his opinion explaining how 50 USC 1809(a) prohibited him from allowing the government to use metadata it had collected for years in violation of the court's rules.

Basically, Bates argued that the government would be guilty of illegal wiretaps under FISA if it used the illegally collected information. I believe the illegal collection involved taking metadata that counted as content and/or didn't count as addressing information.

The government, in a submission and a reply to him, argued that was not the case. It made several arguments: first, it claimed their collection wasn't "intentional" and therefore distributing it would not count as an illegal wiretap.

> Insofar as the government contends that Section 1809(a)(2) reaches only "intentional violations of the Court's orders," or "willful" as opposed to intentional conduct, see Memorandum of Law at 74 n. 37, the Court disagrees. The plain language of the statute requires proof that the person in question "intentionally" disclosed or used information "knowing or with reason to know" the information was obtained in the manner described.

It also argued that the Pen Register statute allowed the Court to override the wiretap prohibitions.

> The government argues that the opening phrase of 50 U.S.C. § 1842(a) vests the Court with authority to enter an order rendering Section 1809(a)(2) inapplicable. See Memorandum of Law at 74 n. 37.

It argued that because the Court could limit what the government could do with the data, it could also expand it.

> The government next contends that because the Court has, in its prior orders, regulated access to and use of previously accumulated metadata, it follows that the Court may not authorize NSA to access and use all previously collected information, including information that was acquired outside the scope of prior authorizations, so long as the information "is within the scope of the [PR/TT] statute and the Constitution." Memorandum of Law at 73.

It then argued that the Court's own rules allowed it to authorize access to the data.

> The government further contends that Rule 10(c) of the Rules of this Court

> gives the Court discretion to authorize access to and use of the overcollected information. Memorandum of Law at 73.

Finally, Article II argued that Article III had inherent authority to ignore the law. (!)

> Finally, insofar as the government suggests that the Court has an inherent authority to permit the use and disclosure of all unauthorized collection without regard to Section 1809, see Memorandum of Law at 73-74 & n.37, the Court again must disagree.

To each of these claims, Bates basically answered that whatever authority the Court had, it didn't extend to ignoring a law passed by Congress (nevermind the FISC has stretched several laws passed by Congress to breaking point).

> The Court simply lacks the power, inherent or otherwise, to authorize the government to engage in conduct that Congress has unambiguously prohibited

The one thing the government asked Bates to do which he might have authority to do — to retroactively rewrite the orders issued since July 14, 2004 to allow for the collection in question — he refused to do as improper.

> In its [redacted] Response at page 4 n.1, the government added an alternative request for the Court to amend all prior bulk PR/TT orders nunc pro tunc to permit acquisition of the overcollected information. The Court denies that request. Nunc pro tunc relief is appropriate to conform the record to a court's original intent, but it is not a means to alter what was originally intended or what actually transpired.

Having said "no" the government in 6 different

ways, Bates then said yes.

His ruling applied only to data the government knew had been overcollected. He considered, but ultimately did not apply, his ruling to data that the government did not know had been overcollected.

> When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2). Of course, government officials may not avoid the strictures of Section 1809(a)(2) by cultivating a state of deliberate ignorance when reasonable inquiry would likely establish that information was indeed obtained through unauthorized electronic surveillance.
>
> [snip]
>
> In light of the government's assertions of need, and in heavy reliance on the assurances of the responsible officials, the Court is prepared – albeit reluctantly – to grant the government's request with respect to information that is not subject to Section 18099a)(2)'s prohibition. Hence, the government may access, use, and disseminate such information subject to the restrictions and procedures described above that will apply to future collection.

In short, Bates said the government could use the illegally collected data so long as it remained ignorant that it was illegally collected, but darnit, don't pretend to be ignorant just to be sure you can use data you collected illegally.

I'm sure that sent precisely the right message.

As I said, that was around July 2010. About 10 months later, the government came back and told Bates they were collecting content illegally. Which led to Bates writing another really angry opinion that, nevertheless, allowed the government to vastly expand access (in that case, via back door searches on PRISM material).

Here's a timeline of that later back-and-forth. But as a reminder, the government came and said, "golly, we've been collection US person content for 3 years off our upstream collection conducted under Section 702." Bates spent 3 months trying to get them to nail down how much US person content it entailed, but the government only agreed to count a small fraction of it (having been told just a year before, we now know, that if it doesn't know it's domestic, it can keep and use the data). On October 3, 2011, Bates imposed new minimization procedures on the stuff the government had agreed to count. In that opinion, he referenced this 2010 opinion, noting that dissemination of data intentionally collected illegally violated 50 USC 1809(a)(2).

> The government's revelations regarding the scope of NSA's upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime (1) to "engage[] in electronic surveillance under color of law except as authorized" by statute or (2) to "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. See [redacted] (concluding that Section 1809(a)(2) precluded the Court from approving the government's proposed use of, among other things, certain data acquired by NSA without statutory authority through its "upstream collection"). The Court will address Section 1809(a) and related issues in a separate order. [my

> emphasis]

Notably, Bates considers both — the collection of Internet metadata collection from telecom switches, and the collection of Internet content from telecom switches — "upstream collection."

Here's what happened next, as described in this post:

> In the days after Bates' ruling, the government considered appealing it. On October 13 (10 days after his initial rule) Bates gave the government a schedule for responding to his 1809(a) concerns. In its first response, the government said 1809(a) didn't apply. But then, on November 22, they finally responded to his concerns in earnest.
>
> > The Court therefore directed the government to make a written submission addressing the applicability of Section 1809(a), which the government did on November 22, 2011. See [redacted], Oct. 13, 2011 Briefing Order, and Government's Response to the Court's Briefing Order of Oct. 13, 2011 (arguing that Section 1809(a)(2) does not apply).
>
> It's unclear what the government argued in that November 22 submission, or what the redacted title is (the November 30, 2011 opinion references a November 29 submission). But shortly thereafter, the government started taking action.
>
> > Beginning late in 2011, the government began taking steps that had the effect of mitigating any Section 1809(a)(2) problem, including the risk that information

> > subject to the statutory criminal prohibition might be used or disclosed in an application filed before this Court.

At first, the government claimed it couldn't segregate the illegal data, but would make sure it was subjected to some of the limitations imposed with the new minimization procedures.

> > Although it was not technically feasible for NSA to segregate the past upstream collection in the same way it is now segregating the incoming upstream acquisitions, the government explained that it would apply the remaining components of the amended procedures approved by the Court to the previously collected data, including (1) the prohibition on using discrete, non-target communications determined to be to or from a U.S. person or a person in the United States, and (2) the two-year age-off requirement. See id. at 21.

By April 2012, however, they decided (they claimed, in oral form — any bets we learn this oral assurance was false?) to come up with a better solution — purging what they could identify entirely.

> > Thereafter, in April2012, the government orally informed the Court that NSA had made a "corporate decision" to purge all data in its repositories that can be identified as having been acquired through upstream

> > collection before the October 31, 2011 effective date of the amended NSA minimization procedures approved by the Court in the November 30 Opinion.
>
> Then they went through and figured out what reports derived from the tainted collections, and assessed whether they could be individually defended or not.
>
> In the end, Bates never ruled on whether the government was — as they claimed — exempt from rules limiting the collection and dissemination of illegally collected data.
>
> > Under the circumstances, the Court finds it unnecessary to further address the arguments advanced by the government in its November 22, 2011 response to the Court's October 13, 2011 briefing order regarding Section 1809(a), particularly those regarding the scope of prior Section 702 authorizations.

One thing the government did to respond to Bates' finding that they were at risk, once again, of violating 1809(a)(2), was to purge the data (remembering, of course, they had avoided admitting they knew the great bulk of the US person data was US person data and therefore illegal).

But another thing that happened in precisely that period, as it turns out, is that the government decided to "stop" it's Internet metadata program under the PR/TT orders (the government itself has said it halted the program in 2011, and we know it occurred near the end of the year because Ron Wyden and Mark Udall say they spent most of the year talking about how ineffective it was).

Only, the government didn't stop collecting Internet metadata.

They just moved it overseas.

That's the critical importance of the Snowden revelations about — among other things — our theft of Google and Yahoo data from their servers overseas. It shows that even while the government claims to have "stopped" its Internet metadata program, it actually accelerated its metadata (and content) collection overseas.

You see, 1809(a)(2) only applies to "electronic surveillance," which by definition is acquisition in the United States.

Now, as I laid out here, to the extent the government is collecting content, it still has a legal problem with its overseas collection, because FISA Amendments Act prohibits electronic surveillance on Americans overseas without a warrant.

But it will no doubt offer the same arguments it did for years, apparently, to justify collecting content in the name of metadata to rationalize evading John Bates' efforts at making it follow the law by moving overseas.

This collection was declared illegal way back in 2004. And the government has spent the interim 9 years trying to find a way to continue it nevertheless.