# THE GOVERNMENT SEZ: WE DON'T HAVE A DATABASE OF ALL YOUR COMMUNICATION

I'm going to try to do a series of posts on the FISA Appeals Court ruling before football starts tomorrow. In this post, I just want to point to a passage that deserves more scrutiny:

> The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.(26)

To translate, if the government collects information from a US citizen (here or abroad), a legal permanent US resident, a predominantly US organization, or a US corporation in the course of collecting information on someone it is specifically targeting, it it claims it does not keep that in a database (I'll come back and parse this in a second). In other words, if the government has a tap on your local falafel joint because suspected terrorists live off their falafels, and you happen to call in a take out order, it does not that have in a database.

There are reasons to doubt this claim. First of all, because we know of huge new data storage facilities, and they've got to be filling those facilities with something. Of course, they might just store US person communications on servers, but not in a formal database, and thereby be able to claim they've not got your falafel order in a database proper.

But we also know that when Russ Feingold proposed several measures to protect this kind

of incidental data during last year's FISA debate, Mike McConnell and Michael Mukasey started issuing veto threats. For example, when Feingold proposed adding this amendment to the new FISA changes,

> At such time as the Government can reasonably determine that a communication acquired under this title (including a communication acquired under subsection (a)(2)) is to or from a person reasonably believed to be located in the United States, such communication shall be segregated or specifically designated and no person shall access such a communication, except in accordance with title I or this section.

Mukasey and McConnell threw out a bunch of vague alarmist objections.

> The Mukasey-McConnell attack on segregation is most telling. They complain that the amendment makes a distinction between different kinds of foreign intelligence (one exception to the segregation requirement in the amendment is for "concerns international terrorist activities directed against the United States, or activities in preparation therefor"), even while they claim it would "diminish our ability swiftly to monitor a communication from a foreign terrorist overseas to a person in the United States." In other words, the complain that one of the only exceptions is for communications relating terrorism, but then say this will prevent them from getting communications pertaining to terrorism.
>
> Then it launches into a tirade that lacks any specifics:
>
> > It would have a devastating impact on foreign intelligence surveillance operations; it is

> > unsound as a matter of policy; its provisions would be inordinately difficult to implement; and thus it is unacceptable.
>
> As Feingold already pointed out, the government has segregated the information they collected under PAA—they're already doing this. But to justify keeping US person information lumped in with foreign person information, they offer no affirmative reason to do so, but only say it's too difficult and so they refuse to do it.

They made similar objections when Feingold attempted to prohibit reverse targeting and prevent the use of improperly collected information. **All** of these objections indicate that they cannot—or refuse to—add protections for this incidental information.

Which frankly leaves me wondering whether the government isn't massively parsing that claim.

> The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons,

Did the court ask only about a database consisting entirely of incidentally collected information? Did they ask whether the government keeps incidentally collected information in its existing databases (that is, it doesn't have a database devoted solely to incidental data, but neither does it pull the incidental data out of its existing database)? Or, as bmaz reminds me below but that I originally omitted, is the government having one or more contractors maintain such a database? Or is the government, rather, using an expansive definition of targeting, suggesting that anyone who buys falafels from the same place that suspected terrorist does then, in turn, becomes targeted?

McConnell and Mukasey's objections to Feingold's amendments make sense only in a situation in which all this information gets dumped into a database that is exposed to data mining. So it's hard to resolve their objections with this claim—as described by the FISA Appeals Court. Unless, of course, they're parsing wildly with the Court to get a favorable ruling.