DOMESTIC TERRORISTS AND THE DRAGNET DATABASE

This is the first reference to actual alleged terrorists in the Administration's White Paper on the Section 215 metadata dragnet (there's one earlier reference to counterterrorism).

> This telephony metadata is important to the Government because, by analyzing it, the Government can determine whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States.

It's a remarkable reference, in that it (and the prior mention of counterterrorism) doesn't limit the terrorism in question to international terrorism (that which transcends national boundaries). And that's not the only place in the White Paper where the government neglects such a modifier: by my rough count, about half the references to terrorism include no indication in the sentence that the discussion is limited exclusively to international terrorism.

But there should be such a limitation. The Section 215 statute (which is broader in scope than the 215 metadata dragnet) makes quite clear that its use, when concerning a US person, is limited to **international** terrorism or clandestine activities.

> Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers,

> documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person **or to protect against international terrorism or clandestine intelligence activities**, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. [my emphasis]

And the Primary Order for the program notes it can only be used "to protect against international terrorism."

So legally, at least, the dragnet can only be used for foreign terrorism. Which is why I find it so disturbing the legal argument laid out here doesn't make that distinction very carefully (and indeed, distinguish what makes the tracking of foreign terrorists legal whereas similar tracking of domestic ones would not be).

Let me be clear: **I'm not alleging the government has extended the use of either Section 215 or the metadata dragnet to investigating domestic terrorists**. In other statements — and indeed, usually in statements that address intelligence programs addressed to Al Qaeda and other terrorists — the Administration the distinction quite clear.

By comparison, look at the way Jack Goldsmith defined the targets of Bush's illegal wiretap program in his May 6, 2004 OLC memo. Remember, while this passage pertains just to content collection, Bush's illegal program did include precisely the same dragnet function (Goldsmith's discussion of both Internet and phone metadata dragnets in the memo remains redacted, but we know he discussed at least the Internet metadata dragnet).

> the authority to intercept the content of international communications "for which, based on the factual and

> practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe … [that] a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group," as long as that group is al Qaeda, an affiliate of al Qaeda or another international terrorist group that the President has determined both (a) is in armed conflict with the United States and (b) poses a threat of hostile actions within the United States;

By comparison, here's how one of the passages from the White Paper describes the limits on the database to foreign terrorism.

> The Government cannot conduct substantive queries of the bulk records for any purpose other than counterterrorism. Under the FISC orders authorizing the collection, authorized queries may only begin with an "identifier," such as a telephone number, that is associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court.

Thus, even where the White Paper is specific, it doesn't lay out what makes foreign terror metadata somehow legally distinct from domestic terror metadata, aside from the approval of the court.

By being downright sloppy about the distinction in the White Paper, the government actually lays out the case that they **could** use a metadata dragnet to pursue domestic terrorists, as in this section which emphasizes suspects in the US are the target because they might be planning to attack the "homeland."

> The most analytically significant

> terrorist-related communications are those with one end in the United States or those that are purely domestic, because those communications are particularly likely to identify suspects in the United States—whose activities may include planning attacks against the homeland.

Or in this section, which argues that discovering and tracking terrorists fulfills the requirements of a Special Needs collection.

> On the other side of the scale, the interest of the Government—and the broader public—in discovering and tracking terrorist operatives and thwarting terrorist attacks is a national security concern of overwhelming importance.
>
> [snip]
>
> Thus, even if the appropriate standard for the telephony metadata collection program were not relevance, but rather a Fourth Amendment reasonableness analysis, the Government's interest is compelling and immediate, the intrusion on privacy interests is limited, and the collection is a reasonably effective means of detecting and monitoring terrorist operatives and thereby obtaining information important to FBI investigations.

So while the White Paper's description of the actual query process makes it clear that the dragnet can be used only to hunt people with ties to foreign terrorists, in a number of places the government makes a legal argument that it would be permitted to hunt domestic terrorists using such a dragnet as well.

Using the government's logic, mind you, there **should** be no distinction. The government argues that if the government interest is compelling

and immediate — as it would be with Timothy McVeigh every bit as much as it was with Anwar al-Awlaki — then it has the authority to conduct such surveillance.

But when you imagine this dragnet being used in the name of pursuing domestic terrorists, it quickly becomes clear why it would be — and is, even when limited to foreign terrorists — so problematic.

If you searched two or three hops from Timothy McVeigh, you'd be inventing probable cause to investigate a whole slew of potentially loathsome but perfectly legal right wing activists. If you searched two or three hops from Scott Roeder (George Tiller's assassin), you'd be inventing probable cause to investigate much of the anti-choice movement. If you searched two or three hops from the Occupy Cleveland activists convicted of plotting to blow up a bridge, you'd be inventing probable cause to investigate much Occupy generally.

In all of these cases, accessing that metadata (and putting it into the corporate store, which is accessible for counterterrorism investigations, again not modified to limit it to international context) would provide key insights into Constitutionally protected political groups. But that's almost certainly the case for certain extremist mosques around the country as it is.

And while you're not supposed to investigate these groups solely on the basis of First Amendment protected activities, the association with a presumed terrorist seems to provide the additional rationale the FBI would need to open at least a preliminary investigation. Plus, as the White Paper argued, by claiming a good faith investigation into terrorism, the government can dismiss any and all First Amendment concerns (note, in context this reference to terrorism makes clear that it pertains to foreign terrorism).

> Rather, the collection is in furtherance

> of the compelling national interest in identifying and tracking terrorist operatives and ultimately in thwarting terrorist attacks, particularly against the United States. It therefore satisfies any "good faith" requirement for purposes of the First Amendment. See Reporters Comm., 593 F.2d at 1052 ("[T]he Government's good faith inspection of defendant telephone companies' toll call records does not infringe on plaintiffs' First Amendment rights, because that Amendment guarantees no freedom from such investigation.")

The First Amendment protected association demonstrated by the database would, in effect, provide the rationale to claim this wasn't an investigation solely on the basis of First Amendment protected political speech.

Going back to the Goldsmith opinion — and the 2006 White Paper limited to the intercept part of the illegal program, both include this language about the wiretap Keith precedent.

> Keith made clear that one of the significant concerns driving the Court's conclusion in the domestic security context was the inevitable connection between perceived threats to domestic security and political dissent. As the Court explained: "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'" Keith, 407 U.S. at 314; see also id. at 320 ("Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and

> continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent."). Surveillance of domestic groups raises a First Amendment concern that generally is not present when the subjects of the surveillance are foreign powers or their agents.

I realize the government doesn't consider creating a database of every phone-based relationship in the US surveillance. I realize Keith pertained to wiretapping, not metadata.

But you would expect some kind of language like this in the metadata White Paper anyway, because mapping relationships in the way the government does so clearly infringes on political dissent, whether that dissent happens in mosques or anti-choice churches.

It's not there. Nor is any other language that would distinguish the targeting of international terrorists from targeting domestic ones.

They're not using the dragnet to map the relationships of domestic terrorists and their legally protected associates. But legally, they've already laid out the case to do so.