

HAVE CLAPPER, FEINSTEIN, AND ROGERS CONFUSED THE DISTINCT ISSUES OF SECTION 215 AND PRISM? OR ARE THEY INDISTINCT?

[youtube]hmw4G5q10kE[/youtube]

Last year, when Pat Leahy tried to switch the FISA Amendments Act reauthorization to a 3 year extension instead of 5, which would have meant PATRIOT and FAA would be reconsidered together in 2015, the White House crafted a talking point claiming that would risk confusing the two provisions.

Aligning FAA with expiration of provisions of the Patriot Act risks confusing distinct issues.

In the last week, the Guardian had one scoop pertaining to FAA (the PRISM program) and another to PATRIOT (the use of Section 215 to conduct dragnet collection of Americans' phone records).

Since then, almost everyone discussing the issues seems to have confused the two.

Including, at a minimum, Mike Rogers, as demonstrated by the video above. When Dianne Feinstein started explaining the Section 215 Verizon order, Mike Rogers interrupted to say that the program could not be targeted at Americans. But of course the Section 215 order was explicitly limited to calls within the US, so he had to have been thinking of PRISM.

Then there what, on first glance, appears to be confusion on the part of journalists. I noted

how Reuters' Rogers-related sources were clearly confused (or in possession of a time machine) when they made such claims, and NYT appeared to conflate the issues as well. Similarly, Andrea Mitchell took this exchange – which is clearly about Section 215 – and elsewhere reported that the law allowing NSA to wiretap Americans (which could be FISA or FAA) stopped the attack.

ANDREA MITCHELL:

At the same time, when Americans woke up and learned because of these leaks that every single telephone call in this United States, as well as elsewhere, but every call made by these telephone companies that they collect is archived, the numbers, just the numbers, and the duration of these calls. People were astounded by that. They had no idea. They felt invaded.

JAMES CLAPPER:

I understand that.

[snip]

A metaphor I think might be helpful for people to understand this is to think of a huge library with literally millions of volumes of books in it, an electronic library. Seventy percent of those books are on bookcases in the United States, meaning that the bulk of the of the world's infrastructure, communications infrastructure is in the United States.

[snip]

So the task for us in the interest of preserving security and preserving civil liberties and privacy is to be as precise as we possibly can be when we go in that library and look for the books that we need to open up and actually read.

[snip]

So when we pull out a book, based on its essentially is— electronic Dewey Decimal System, which is zeroes and ones, we have to be very precise about which book we're picking out. And if it's one that belongs to the— was put in there by an American citizen or a U.S. person.

We ha— we are under strict court supervision and have to get stricter— and have to get permission to actually— actually look at that. So the notion that we're trolling through everyone's emails and voyeuristically reading them, or listening to everyone's phone calls is on its face absurd. We couldn't do it even if we wanted to. And I assure you, we don't want to.

ANDREA MITCHELL:

Why do you need every telephone number? Why is it such a broad vacuum cleaner approach?

JAMES CLAPPER:

Well, you have to start someplace. If— and over the years that this program has operated, we have refined it and tried to— to make it ever more precise and more disciplined as to which— which things we take out of the library. But you have to be in the— in the— in the chamber in order to be able to pick and choose those things that we need in the interest of protecting the country and gleaning information on terrorists who are plotting to kill Americans, to destroy our economy, and destroy our way of life.

ANDREA MITCHELL:

Can you give me any example where it actually prevented a terror plot?

JAMES CLAPPER:

Well, two cases that— come to mind,

which are a little dated, but I think in the interest of this discourse, should be shared with the American people. They both occurred in 2009. One was the aborted plot to bomb the subway in New York City in the fall of 2009.

And this all started with a communication from Pakistan to a U.S. person in Colorado. And that led to the identification of a cell in New York City who was bent on— make— a major explosion, bombing of the New York City subway. And a cell was rolled up, and in their apartment, we found backpacks with bombs.

A second example, also occurring in 2009, involved— the— one of the— those involved, perpetrators of the Mumbai bombing in India, David Headley. And we aborted a plot against a Danish news publisher based on— the same kind of information. So those are two specific cases of uncovering plots through this mechanism that— prevented terrorist attacks.

What would seem to support the conclusion that everyone was just very confused is that, in his talking points on the two programs, Clapper claims three examples as successes for the use of PRISM, none of which is Zazi or Headley.

Now, the AP reports Clapper's office (which is fast losing credibility) has circulated talking points making the claim that PRISM helped nab Zazi.

The Obama administration declassified a handful of details Tuesday that credited its PRISM Internet spying program with intercepting a key email that unraveled a 2009 terrorist plot in New York.

The details, declassified by the director of national intelligence, were circulated on Capitol Hill as part of

government efforts to tamp down criticism of two recently revealed National Security Agency surveillance programs.

But, as I suggested last year, the White House clearly wasn't concerned about us confusing our pretty little heads by conflating FAA and Section 215. Rather, it seemed then to want to hide the relationship between the dragnet collection of Americans calls and the direct access to Internet providers' data.

But Clapper and DiFi seem to hint at the relationship between them.

In her first comments about Section 215 (even before PRISM had broken) DiFi said this.

The information goes into a database, the metadata, but cannot be accessed without what's called, and I quote, "reasonable, articulable suspicion" that the records are relevant and related to terrorist activity.

And in his talking points on 215, Clapper said this.

By order of the FISC, the Government is prohibited from indiscriminately sifting through the telephony metadata acquired under the program. All information that is acquired under this program is subject to strict, court-imposed restrictions on review and handling. The court only allows the data to be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization.

This standard – reasonable suspicion that the records are relevant to or associated with a terrorist investigation (I'll come back to the

terrorism issue in another post) – is not the 215 standard, because it requires reasonable suspicion. But it's not as high as a FISA warrant would be, which requires it to be more closely related than "relevant" to a terrorist investigation.

So what standard is this, and where did it come from?

Via email, Cato's Julian Sanchez hypothesizes that the FISA Court may have required the government apply the standard for Terry stops and ECPA to their ability to access US person data from the database.

It looks like they essentially imported the Terry stop-and-frisk standard, maybe by way of the ECPA "specific and articulable facts" standard in 18 USC 2703, as a post-collection constraint on QUERIES of the database, rather than its collection. That would comport with the DOD understanding that "acquisition" of a communication only occurs when it's actually processed into human-readable form and received by an analyst: They've concluded that the "relevance" test can be embedded in back end restrictions at the "query" phase where "acquisition" happens rather than the initial copying of the data. And they've used the ECPA/Terry standard as the test of relevance.

In other words, DiFi and Clapper's comments, in particular, and the underlying confusion that suggests there's a tie between PRISM and the Section 215 database generally, seem to suggest that the PRISM collection provides the evidence the government uses to get access to the predominantly US person metadata to start seeing which Americans have 6 degrees of separation from the terrorists.

They're saying over and over again that they just can't go into the database willy nilly.

Except they can access the PRISM data willynilly (including seeing the US person data) and use that to access a data of predominantly American records.