WORKING THREAD, SECTION 215 WHITE PAPER

I've already had some things to say about the White Paper the Administration released on its metadata dragnet program and will have several more formal posts. But I wanted to capture all my notes in one place.

Page 1:

> telecommunications service providers

Note they don't say telecoms. That's because, for this program to do what they say, they also have to be getting the metadata from VOIPs. There are redactions in the Congressional documents that probably address this as well.

> The Court first authorized the program in 2006, and it has since been renewed thirty-four times under orders issued by fourteen different FISC judges.

Note that it doesn't say the program started in 2006. That's because it started in 2001, as part of Bush's illegal program. That's key because it means it was in place when Congress passed the 2006 reauthorization of PATRIOT which included "relevant to" language, but the Exec didn't brief on how that was going to be used.

> 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.

This is just the first of many many many statements in this White Paper that are

unbelievably sloppy about referring to what should only be "international" terrorists (that is, terrorists with some tie to an international terrorist group). I'll have far more to say about it, but this sloppiness led me to contemplate what would happen if this dragnet could be used for domestic terrorists — meaning authorities could see how (say) Sovereign citizens had ties to white supremacists or how anti-choice activists had ties to clinic bombers.

Page 2:

> This does not mean that Section 215 authorizes the collection and storage of all types of information in bulk: the relevance of any particular data to investigations of international terrorism depends on all the facts and circumstances. For example, communications metadata is different from many other kinds of records because it is inter-connected and the connections between individual data points, which can be reliably identified only through analysis of a large volume of data, are particularly important to a broad range of investigations of international terrorism.

This is the first of a whole thread of language in this that tries to suggest there are limits on bulk collection. They're odd, first of all, because the government has already said NSA only uses phone data (we know FBI does far more). But as I'll show, they're not very convincing in any case.

> Moreover, information concerning the use of Section 215 to collect telephony metadata in bulk was made available to all Members of Congress, and Congress reauthorized Section 215 without change after this information was provided. It is significant to the legal analysis of the statute that Congress was on notice

> of this activity and of the source of its legal authority when the statute was reauthorized.

Was it also significant to the FISC Court that congress "was on notice" of this stuff?

Page 3:

> 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.

As I'll write elsewhere, this passage and others lay out the legal case (intentional or not) that the government could use similar techniques to go after domestic (right wing, for example) terrorists.

> The Government also does not collect cell phone locational information pursuant to these orders.

As many have noted, every time the government uses "pursuant to these orders" (as they do elsewhere discussing collection of content), it lends evidence they are collecting that information via other means.

> Technical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier.

You'd think they would have had the author of this White Paper see what people had commented on on the existing leaks, as when I pointed out that technical personnel, as distinct from analysts, do get to access the metadata under other circumstances. Including spin like this

really undermines their credibility.

Page 4:

> Results of authorized queries are stored and are available only to those analysts trained in the restrictions on the handling and dissemination of the metadata. Query results can be further analyzed only for valid foreign intelligence purposes. Based on this analysis of the data, the NSA then provides leads to the FBI or others in the Intelligence Community. For U.S. persons, these leads are limited to counterterrorism investigations.

As I'll note elsewhere, this seems to explain why the banksters never get busted for money laundering.

> If the FBI investigates a telephone number or other identifier tipped to it through this program, the FBI must rely on publicly available information, other available intelligence, or other legal processes in order to identify the subscribers of any of the numbers that are retrieved. For example, the FBI could submit a grand jury subpoena to a telephone company to obtain subscriber information for a telephone number.

This is gratuitous spin. The FBI would, as they did with Basaaly Moalin, use an NSL to get this info, if they didn't have it already available (as they do a lot of numbers). To suggest they'd get a warrant just suggests there's more protection in follow-up investigation than there really is.

Page 5:

> Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues

> that were discovered as a result of DOJ and ODNI reviews and internal NSA oversight. In accordance with the Court's rules, upon discovery, these violations were reported to the FISC, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence and Judiciary Committees in great detail. These problems generally involved human error or highly sophisticated technology issues related to NSA's compliance with particular aspects of the Court's orders. The FISC has on occasion been critical of the Executive Branch's compliance problems as well as the Government's court filings. However, the NSA and DOJ have corrected the problems identified to the Court, and the Court has continued to authorize the program with appropriate remedial measures.

This differs in some interesting ways from other versions of the same paragraph, as I'll show in follow-up.

> This conclusion does not mean that any and all types of business records—such as medical records or library or bookstore records—could be collected in bulk under this authority. In the context of communications metadata, in which connections between individual data points are important, and analysis of bulk metadata is the only practical means to find those otherwise invisible connections in an effort to identify terrorist operatives and networks, the collection of bulk data is relevant to FBI investigations of international terrorism.

Note this passage only addresses whether the govt would use 215 to collect these things in bulk, not whether it would (as it could) collect

them in smaller amounts. Also note that it chooses to use the most extreme case (which Congress perennially tries to limit anyway), rather than the more interesting cases, like gun purchases or credit card information.

Page 6:

> Section 215 authorizes the FISC to issue an order for 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," except that it prohibits an "investigation of a United States person" that is "conducted solely on the basis of activities protected by the first amendment to the Constitution."

Note this passage leaves out 215's application to clandestine intelligence, which is also permissible. Normally, this wouldn't bug me, since they purportedly can't use the dragnet for anything but terror. But as you'll see the language starts to get funky here.

> The FBI conducts the investigations consistent with the Attorney General's Guidelines for Domestic FBI Operations, U.S. Dep't of Justice (2008), which direct the FBI "to protect the United States and its people from . . . threats to the national security" and to "further the foreign intelligence objectives of the United States," a mandate that extends beyond traditional criminal law enforcement. See id. at 12. The guidelines authorize a full investigation into an international terrorist organization if there is an "articulable factual basis for the investigation that reasonably indicates that the group or organization may have

> engaged . . . in . . . international terrorism **or other threat to the national security**," or may be planning or supporting such conduct.

Two points. First, I'm trying to figure out why they always go back to the 2008 Guidelines rather than the 2011 DIOG, but I don't have an answer to that yet. Also, note how they can investigate a terrorist organization for things that threaten national security but aren't terrorism? Interesting.

Page 7:

> There is little question that in enacting Section 215 in 2001 and then amending it in 2006, Congress understood that among the things that the FBI would need to acquire to conduct terrorism investigations were documents and records stored in electronic form. Congress may have used the term "tangible things" to make clear that this authority covers the production of items as opposed to oral testimony, which is another type of subpoena beyond the scope of Section 215.
>
> [snip]
>
> The word "tangible" can be used in some contexts to connote not only tactile objects like pieces of paper, but also any other things that are "capable of being perceived" by the senses. See Merriam Webster Online Dictionary (2013) (defining "tangible" as "capable of being perceived especially by the sense of touch") (emphasis added).

Love how the Admin plays dumb about why they switched to "tangible," then notes that it could be something perceptible rather than, say, a business record.

Note, too, what the Admin should be explaining

in here is why they're using the Business Records/ Tangible Things provision to get something—phone records—for which there is a statute clearly intended, the Pen Register/Trap and Trace.

Page 8:

> Specifically, in the circumstance where the Government has reason to believe that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information—and that it is necessary to collect a large volume of data in order to employ the analytic tools needed to identify that information—the standard of relevance under Section 215 is satisfied.

Consider how this standard would apply to NCTC, which has been empowered to get any federal database it says has info relevant to terrorism.

> The legislative history of Section 215 also supports this reading of the provision to include electronic data. In its discussion of Section 215, the House Report accompanying the USA PATRIOT Reauthorization Act of 2006 notes that there were electronic records in a Florida public library that might have been used to help prevent the September 11, 2001, attacks had the FBI obtained them. See H.R. Rep. No. 109-174(I), at 17-18 (2005). Specifically, the report describes "records indicat[ing] that a person using [the hijacker] Alhazmi's account used the library's computer to review September 11th reservations that had been previously booked." Id. at 18. Congress used this example to illustrate the types of "tangible things" that Section 215 authorizes the FBI to obtain through a FISC order. Moreover, the House Report cites testimony in 2005 by the Attorney General before the House

> Committee on the Judiciary, where the Attorney General explained that Section 215 had been used "to obtain driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen-register devices." Id. (emphasis added). Telecommunications service providers store such subscriber information electronically. Accordingly, the House Report suggests that Congress understood that Section 215 had been used to capture electronically stored records held by telecommunications service providers and reauthorized Section 215 based on that understanding.

Watch the way the White Paper cherry picks Congressional Record.

Page 9:

> Congress legislated against that legal background in enacting Section 215 and thus "presumably kn[e]w and adopt[ed] the cluster of ideas that were attached to [the] word in the body of learning from which it was taken." See FAA v. Cooper, 132 S. Ct. 1441, 1449 (2012) (internal citation and quotation marks omitted). Indeed, as discussed above, in identifying the sort of items that may be the subject of a Section 215 order, Congress expressly referred to items obtainable with "a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation" or "any other order issued by a court of the United States directing the production of records or tangible things," 50 U.S.C. § 1861(c)(2)(D), indicating that it was well aware of this legal context when it added the relevance requirement. That

> understanding is also reflected in the statute's legislative history. See 152 Cong. Rec. 2426 (2006) (statement of Sen. Kyl) ("Relevance is a simple and well established standard of law. Indeed, it is the standard for obtaining every other kind of subpoena, including administrative subpoenas, grand jury subpoenas, and civil discovery orders.").

This is a particularly bad cherry pick. As this brief makes clear, the Congressional record included a number of people saying they used relevant as a limitation on what had gone before.

Page 11:

> It is reasonable to conclude that Congress had that broad concept of relevance in mind when it incorporated this standard into Section 215. The statutory relevance standard in Section 215, therefore, should be interpreted to be at least as broad as the standard of relevance that has long governed ordinary civil discovery and criminal and administrative investigations, which allows the broad collection of records when necessary to identify the directly pertinent documents. To be sure, the cases that have been decided in these contexts do not involve collection of data on the scale at issue in the telephony metadata collection program, and the purpose for which information was sought in these cases was not as expansive in scope as a nationwide intelligence collection effort designed to identify terrorist threats. While these cases do not demonstrate that bulk collection of the type at issue here would routinely be permitted in civil discovery or a criminal or administrative investigation, they do show that the "relevance" standard

> affords considerable latitude, where necessary, and depending on the context, to collect a large volume of data in order to find the key bits of information contained within.

This passage is funny for two reasons. Note they just assume that's what Congress had in mind, rather than consulting the record. But also note that they admit previous claims (including one made earlier in this passage) — that the dragnet is akin to a grand jury subpoena — doesn't work.

> First, Section 215's standard on its face is particularly broad, because the Government need only show that there are "reasonable grounds to believe" that the records sought are relevant to an authorized investigation. 50 U.S.C. § 1861(b)(2)(A). That phrase reflects Congress's understanding that Section 215 permits a particularly broad scope for production of records in connection with an authorized national security investigation.11
>
> 11 Some Members of Congress opposed Section 215 because in their view it afforded too broad a standard for collection of information. See, e.g., 152 Cong. Rec. 2422 (2006) (statement of Sen. Feingold) ("[T]he deal would allow subpoenas in instances when there are reasonable grounds for simply believing that information is relevant to a terrorism investigation. That is an extremely low bar."); 156 Cong. Rec. S2108-01 (2010) (statement of Sen. Wyden) ("'Relevant' is an incredibly broad standard. In fact, it could potentially permit the Government to collect the personal information of large numbers of law-abiding Americans who have no connection to terrorism whatsoever.")

Page 12:

> In the particular circumstance in which the collection of communications metadata in bulk is necessary to enable discovery of otherwise hidden connections between individuals suspected of engaging in terrorist activity,

EFF calls the dragnet an "Associational Database," and this passage makes it clear the government agrees. This is not about phone calls. It is about relationships.

> Rather, for Section 215 to be effective in advancing its core objective, the FBI must have the authority to collect records that, when subjected to reasonable and proven investigatory techniques, can produce information that will help the Government to identify **previously unknown** operatives and thus to prevent terrorist attacks before they succeed. [my emphasis]

The two public cases in which Section 215 has been used involved people who were already known to the government, Moalin through a previous investigation into him, and Zazi's accomplice through Zazi.

> Notably, Congress specifically rejected proposals to limit the relevance standard so that it would encompass only records pertaining to individuals suspected of terrorist activity.12
>
> 12 See S. 2369, 109th Cong. § 3 (2006) (requiring Government to demonstrate relevance of records sought to agents of foreign powers, including terrorist organizations, or their activities or contacts); 152 Cong. Rec. S1598-03 (2006) (statement of Sen. Levin) ("The Senate bill required a showing that the records sought were not only relevant to

> an investigation but also either pertained to a foreign power or an agent of a foreign power, which term includes terrorist organizations, or were relevant to the activities of a suspected agent of a foreign power who is the subject of an authorized investigation or pertained to an individual in contact with or known to be a suspected agent. In other words, the order had to be linked to some suspected individual or foreign power. Those important protections are omitted in the bill before us."); 152 Cong. Rec. H581-02 (2006) (statement of Rep. Nadler) ("The conference report does not restore the section 505 previous standard of specific and articulable facts connecting the records sought to a suspected terrorist. It should."); 151 Cong. Rec. S14275-01 (2005) (statement of Sen. Dodd) ("Unfortunately, the conference report differs from the Senate version as it maintains the minimal standard of relevance without a requirement of fact connecting the records sought, or the individual, suspected of terrorist activity. Additionally, the conference report does not impose any limit on the breadth of the records that can be requested or how long these records can be kept by the Government.").

Note the dates here.

Page 13:

> If not collected and held by the NSA, telephony metadata may not continue to be available for the period of time (currently five years) deemed appropriate **for national security purposes** because telecommunications service providers are not typically required to retain it for this length of time. [my emphasis]

First, the government repeatedly misrepresents the history behind current retention rules, as this post makes clear.

But also note they describe the appropriate retention period for national security purposes, not just counterterrorism purposes.

Page 14:

> This conclusion does not mean that the scope of Section 215 is boundless and authorizes the FISC to order the production of every type of business record in bulk—including medical records or library or book sale records, for example.

As noted earlier, the government chooses to use the example of items that Congress tried to limit. This passage introduces a long passage in which the government pretends there's not a huge gap between these uses and the metadata dragnet.

> Although there could be individual contexts in which the Government has an interest in obtaining medical records or library records for counterterrorism purposes, these categories of data are not in general comparable to communications metadata as a means of identifying previously unknown terrorist operatives or networks.

Note, explosive precursor purchases is something that can (and has) been used to ID purported terrorists. Again, they're using an example that is absurd so as to distract from a more obvious example.

Page 15:

> The vast majority of the telephony metadata is never seen by any person because it is not responsive to the limited queries that are authorized. But the information that is generated in response to these limited queries could

> be especially significant in helping the Government identify and disrupt terrorist plots.

Note they say the information "could" be especially significant, not that it has at any time in the past.

> Thus, while the relevance standard provides the Government with broad authority to collect data that is necessary to conduct authorized investigations, the FISC's orders require that the data will be substantively queried only for that authorized purpose. That is the balanced scheme that Congress adopted when it joined the broad relevance standard with the requirement for judicial approval set forth in Section 215.

Note, it is referring to FISC orders, based on an agreement briefed but not shared before Congress first passed the relevance standard in 2006. Congress didn't adopt this, it was handed to them.

> 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. See Haig v. Agee, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.")

This passage is part of the special needs argument that the white paper probably adopts from earlier (Goldsmith era) OLC memos. But here, it doesn't modify terrorists (as Goldsmith did) to limit it to international terrorists. As I'll show later, this basically makes the case for using these tools against domestic

terrorists. And if we're doing it for the security of the nation, what would prevent us from using it against gun crimes, which are a bigger threat to the security of the country?

Page 16:

> Nothing in the text of the statute suggests that FISC orders may relate only to records previously created.
>
> [snip]
>
> Nor is there any legislative history indicating that Congress intended to prevent courts from issuing prospective orders under Section 215 in these circumstances.

Note how, after relying so closely on a (cherry-picked) version of the legislative record, here it becomes entirely unnecessary?

> Section 215 orders are not being used to compel a telecommunications service provider to retain information that the provider would otherwise discard, because the telephony metadata records are routinely maintained by the providers for at least eighteen months in the ordinary course of business pursuant to Federal Communications Commission regulations. See 47 C.F.R. § 42.6.

Here the govt admits what it elsewhere (even in this white paper) ignores about govt requirements on maintaining data.

> This type of prospective order also provides efficient administration for all parties involved—the Court, the Government, and the provider. There is little doubt that the Government could seek a new order on a daily basis for the records created within the last 24 hours. But the creation and processing of such requests would impose entirely

> unnecessary burdens on both the Court and the Government—and no new information would be anticipated in such a short period of time to alter the basis of the Government's request or the facts upon which the Court has based its order.

This is supposed to be a legal argument. But it relies on convenience to make it. And of course nowhere does it explain why the appropriate vehicle for this isn't a different kind of order.

> Providers would also be forced to review daily requests of differing docket numbers,

Useful detail: each extension gets a docket number.

Page 17:

> The telephony metadata collection program satisfies the plain text and basic purposes of Section 215 (as well as the Constitution, see infra pp. 20-24) and is therefore lawful. But to the extent there is any question as to the program's compliance with the statute, it is significant that, after information concerning the telephony metadata collection program carried out under the authority of Section 215 was made available to Members of Congress, Congress twice reauthorized Section 215. When Congress reenacts a statute without change, it is presumed to have adopted the administrative or judicial interpretation of the statute if it is aware of the interpretation. See Lorillard v. Pons, 434 U.S. 575, 580 (1978). The FISC's conclusion that Section 215 authorized the collection of telephony metadata in bulk was classified and not publicly known.

> However, it is important to the legal analysis of the statute that the Congress was on notice of this program and the legal authority for it when the statute was reauthorized.

This is where the white paper demonstrates the core problem with the way we legislate, in that it admits both that this was classified but then says that putting Congress "on notice" is adequate to saying they've approved.

Page 20:

> Nothing in United States v. Jones, 132 S. Ct. 945 (2012), changed that understanding of the Fourth Amendment. The Court's decision in that case concerned only whether physically attaching a GPS tracking device to an automobile to collect information was a Fourth Amendment search or seizure.

They're trying hard to ignore the language on persistence here.

> And the volume of records does not convert that activity into a search. Further, Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched." Steagald v. United States, 451 U.S. 204, 219 (1981); accord, e.g., Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) ("Fourth Amendment rights are personal rights which . . . may not be vicariously asserted.'") (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)). Because the Fourth Amendment bestows "a personal right that must be invoked by an individual," a person "claim[ing] the protection of the Fourth Amendment . . . must demonstrate that he personally has an expectation of privacy in the place

> searched, and that his expectation is reasonable.” Minnesota v. Carter, 525 U.S. 83, 88 (1998). No Fourth Amendment-protected interest is generated by virtue of the fact that the telephony metadata records of many individuals are collected rather than those of a single individual.

Whereas above it was dodging persistence, here it is dodging the comprehensiveness of this. THis is a database of every single person’s relationships. That’s an individual incursion.

Page 21:

> On the other side of the balance, there is an exceptionally strong public interest in the prevention of terrorist attacks, and telephony metadata analysis can be an important part of achieving that objective. This interest does not merely entail “ordinary crime-solving,” King, 133 S. Ct. at 1982 (Scalia, J., dissenting), but rather the forward-looking prevention of the loss of life, including potentially on a catastrophic scale. Given that exceedingly important objective, and the minimal, if any, Fourth Amendment intrusion that the program entails, the program would be constitutional even if the Fourth Amendment’s reasonableness standard applied.

This comes at the close of the special needs section. Note, most of the mention serves to get Scalia on your side with his dissent. But note the logic: precrime is worth more than criminal investigation.

> The telephony metadata collection is also consistent with the First Amendment. It merits emphasis again in this context that the program does not collect the content of any

> communications and that the data may be queried only when the Government has a reasonable, articulable suspicion that a particular number is associated with a specific foreign terrorist organization. Section 215, moreover, expressly prohibits the collection of records for an investigation that is being conducted solely on the basis of protected First Amendment activity, if the investigation is of a U.S. person. The FBI is also prohibited under applicable Attorney General guidelines from predicating an investigation solely on the basis of activity protected by the First Amendment.

This is a really important section. Note how it dismisses any First Amendment complaint because the investigation is not predicated on solely First Amendment activity, then says the collection can't be done for an investigation predicated solely on First Amendment. That's how they get around the First Amendment problem with researching the associations of people whose very associations are protected by the First AMendment.

Page 22:

> The Government's collection of telephony metadata in support of investigative efforts against specific foreign terrorist organizations are not aimed at curtailing any First Amendment activities, whether free speech or associational activities. 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.")

This is interesting because it mentions associational rights here—because that is what is really being infringed. But then it effectively says it's okay to do so because it is all in good faith.