IS THIS WHY BANKSTERS DON'T GO TO JAIL FOR LAUNDERING TERRORIST FINANCES?

I'm in the middle of a deep dive in the Section 215 White Paper — expect plenty of analysis on it in coming attractions!

But I want to make a discrete point about this passage, which describes what happen to query results.

> 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.

The Primary Order released several weeks back calls these stored query results "the corporate store." As ACLU laid out, the government can do pretty much whatever it wants with this corporate store — and their analysis of it is not audited.

> All of this information, the primary order says, is dumped into something called the "corporate store." Incredibly, the FISC imposes *no* restrictions on what analysts may subsequently do with the information. The FISC's primary order contains a crucially revealing footnote stating that "the Court understands that

> NSA may apply the full range of SIGINT analytic tradecraft to the result of intelligence analysis queries of the collected [telephone] metadata." In short, once a calling record is added to the corporate store, anything goes.
>
> More troubling, if the government is combining the results of *all* its queries in this "corporate store," as seems likely, then it has a massive pool of telephone data that it can analyze in any way it chooses, unmoored from the specific investigations that gave rise to the initial queries. To put it in individual terms: If, for some reason, your phone number happens to be within three hops of an NSA target, *all* of your calling records may be in the corporate store, and thus available for any NSA analyst to search at will.
>
> But it's even worse than that. The primary order prominently states that whenever the government accesses the wholesale telephone-metadata database, "an auditable record of the activity shall be generated." It might feel fairly comforting to know that, if the government abuses its access to all Americans' call data, it might eventually be called to account—until you read footnote 6 of the primary order, which *exempts entirely* the government's use of the "corporate store" from the audit-trail requirement.

The passage from the White Paper seems to suggest there are limits (though it doesn't explain where they come from, because they clearly don't come from FISC).

This analysis must have a valid foreign intelligence purpose – which can include political information, economic information, espionage information, military information, drug information, and the like. Anything other

countries do, basically.

But if the data in the corporate store pertains to US persons, the FBI can only get a lead "for counterterrorism purposes."

At one level, this is (small) comfort, because it provides a level of protection on the dragnet use.

But it also may explain why HSBC's US subsidiary didn't get caught laundering al Qaeda's money, or why JP Morgan always gets to self-disclose its support for Iranian "terrorism." So long as the government chooses not to treat banks laundering money for terrorists as material support for terror, then they can consider these links (which surely they've come across in their "corporate store!) evidence of a financial crime, not a terrorist one, and just bury it.

I would be curious, though, whether the government has ever used the "corporate store" to police Iran sanctions. Does that count as a counterterrorism purpose? And if so, is that why Treasury "finds" evidence of international bank violations so much more often than it does American bank violations?