A MODEST PROPOSAL TO FIX FBI'S FISA 702 WOES

There's an easy way to fix the FBI's FISA 702 woes: Simply provide a way for FBI to obtain probable cause warrants — from the FISA court, if need be — for any 702 data it wants to be able to query. Armed with those probable cause warrants, virtually all the queries that have been deemed violations in recent years will be compliant with the Fourth Amendment.

The FBI can go back to doing queries on all this information without having to worry about oversight on the back end.

Problem solved, Scoob.

Section 702 of FISA is up for reauthorization this year. Partly because Republicans are upset that Donald Trump is the serial subject of criminal investigations, and partly because a series of changes to FBI's querying of 702 data has made FBI's querying process (of all data) visible for the first time, resulting in persistent violations of the new querying standard, whether and how it will be reauthorized is going to be very contentious. The two sides are talking past each other and proposing yet more tweaks that won't address two underlying causes to the problem. But my solution is an easy fix and will make all the current problems go away!

Don't get me wrong: I think all sides would hate this solution. It would result in more surveillance and more criminal investigations of US persons. But it would solve the problem everyone thinks they have.

For the FBI, it would mean this material will become discoverable to potential future defendants. For civil libertarians, it would mean the FBI would revert to the status quo of about 2015, doing millions of usually fruitless

queries on every assessment they did. But it would solve the legal problem before Congress. Which is a pretty good hint that the legal problem before Congress is not going to address the underlying reasons for the problem — and some potential solutions will make the underlying issues worse without serving US security.

I make my Modest Proposal for three reasons:

- Virtually everyone engaged in the current debate is engaged in bad faith, because everyone has an incentive to ignore the fact that the violative queries are *the way the program was designed from the start* and the way the FBI runs everything else.
- This Modest Proposal will demonstrate the degree to which current debates are ignoring two underlying problems, the way The Wall between intelligence and criminal evidence was eliminated in the wake of 9/11 and the degree to which the FBI runs on massive troves of data.
- My Modest Proposal represents FBI's likely response to current proposals for individualized warrants on *query* targets, rather than *collection* targets (indeed, some of

> this has already happened), so it's a way for people to contemplate the obvious outcomes of the current impasse, including more spying on Americans with less oversight.

The system underlying Section 702 arose because the FBI missed the 9/11 terrorists and in the panic that ensued, the Bush Administration decided it needed to identify everyone in the US with ties to known or suspected terrorists overseas. The program operated illegally as part of Stellar Wind for several years. In 2004, Jack Goldsmith imposed some limitations (some of which remain secret and misunderstood). In 2005, James Risen and Eric Lichtblau started revealing what Stellar Wind had been. Between 2004 and 2008, the content collection part of Stellar Wind was legalized, first as the Protect America Act and then as Section 702. In both the public debates over that legislation and in a Yahoo challenge to its first PAA order, the Administration and a few members of Congress obscured — even lied — about the underlying intent to use the program to identify associates of targets in the United States. Then Snowden made what was already public public (along with the names of the then-recipients of standing orders). And in the years since, each FISA 702 certification has made more of this reality visible to the FISA Judges, who almost every year get all outraged and then nevertheless reapprove the program (in part, because both 702 and FISA applications don't require the things that would really give FISC judges the means to implement real fixes).

I have laid out in recent years how this process has not worked and why we'd have the shitty opinion (again, this opinion is a year old) that we got, in part because it was obvious that Bill Barr was not making substantive changes:

- How Twelve Years of Warning and Six Years of Plodding Reform Finally Forced FBI to Do Minimal FISA Oversight (October 2019)
- The Latest Stinky 702 Opinion Bodes Poorly for the Next One (September 2020)
- The Rickety 702 System: Why It Continues to Fail (April 2021)

The underlying problem is this: The *point* from the start was to allow the FBI to see who inside the United States had ties to first, suspected terrorists and then, people of intelligence interest (which includes but is not limited to suspected spooks, hackers, and weapons proliferators) overseas. It's a great idea! But it also resulted in the FBI routinely searching on content obtained without a warrant with the intent of identifying the communications of Americans, a clear violation of the intent of the Fourth Amendment, but also what Congress and Presidents have demanded the FBI do to prevent another 9/11 or similar surprise.

On Friday, the DOJ released an opinion approving the delayed authorization of certificates first filed in October 2021 (months after my prediction that this process would continue to fail) that showed the FBI continued to commit egregious violations of the then-existing querying guidelines. (One problem with the 702 process is both the violations and the opinions have a significant lag time, and the lag time here has predictably led Republicans to blame Merrick Garland for violations that happened because Bill Barr — who is the grandfather of this entire system — didn't make radical enough fixes in 2019.) Of specific note, it showed that the FBI had done queries in conjunction with the summer 2020 unrest, the January 6 attack, and a losing political campaign known to be targeted

by a foreign intelligence service. That's bad! In several cases, though, there was some foreign component to the investigation (indeed, three of the January 6 targets did find material, which is only supposed to happen if there's some spooky tie, but it's a violation because the FBI personnel in question didn't know of those spooky ties in advance).

Numerous of the violative queries are actually pretty good uses of 702. In predicated criminal investigations against narcotics traffickers, for example, it'd be useful to learn of any *unsuspected* ties to an international trafficking network. In predicated domestic terrorism investigations, it'd be useful to know whether suspects are getting help or have associates hiding out overseas (as multiple people in the January 6 investigation are known to have); indeed the notion that we *shouldn't* know this with white terrorists when we spent decades assuming we *had* to know it with brown terrorists is racist. In vetting people for clearance or use as informants, it'd be useful to know if they've got past ties to foreign spooks. But the way the current standard works, you'll only be able to look if you already suspect such ties. As a result, the standard for associative querying is now far higher for international criminals than it is for domestic ones. In a globalized world, that seems like a stupid state to be in. But it's also the result of ingesting a lot of content into FBI servers without a warrant.

Which brings me to one of the underlying problems this debate is not addressing: The FBI runs on databases. Back during the hellacious USA Freedom Act debates, I argued that all sides should work on a collect-and-query standard to the Fourth Amendment, one that reflected both the real privacy impact of what was dismissed as "just metadata" collected and stored in large volume, and to account for the vast amount of content collected and stored for years via search warrants. What we're seeing described as violative queries are really just descriptions

of how FBI analysts work — how they've been ordered to work since 9/11. Got some new identifiers in a narcotics investigation? Stick them into the database and see what you find! Investigating a new suspect in a domestic terrorism case? Stick his identifiers in the database and see what you find!

A dirty little secret is that, with three exceptions I can think of, the privacy impact on a US person by searches done on vast stores of material obtained with a warrant is not that different from searches done on vast stores of material on foreigners obtained via Section 702. It's going to matter if the subject has incriminating or interesting ties to a past subject of surveillance, but because of the negligible cost of doing a search, millions of searches get done with no results. Most of the violative queries, in fact, result in nothing (which is one reason they went on for so long without attracting more attention).

One exception is that US law has entirely different standards for terrorism involving foreign organizations, including that people can be prosecuted for what in the domestic terrorism context would be protected by the First Amendment. Searches on content have repeatedly led to foreign terrorist investigations — though several appeals courts have reviewed such searches and found no big deal to them. Friday's opinion cited all three in judging that the 702 program complies with the Fourth Amendment. Given the FBI's success combatting domestic terrorism without such crutches, given the greater impact of domestic terrorism of late, we should reconsider the asymmetry of foreign terrorism investigations.

A second exception is that so much of our commerce is with China, but so much of China's spying is economic, that US persons with legitimate economic ties to China undergo a great deal of scrutiny. There's good reason to believe a number of US persons have been targeted for criminal investigation as a result,

some in cases that have blown up in spectacular fashion.

A third exception is that the FBI uses (or probably, used) such searches to identify potential informants. And way back in 2002, John Yoo justified identifying derogatory information (like domestic abuse or rape) that had nothing to do with terrorism but could nevertheless be used to coerce someone to become an FBI informant. So there are definitely cases where someone will be coerced by the FBI not because of any crime they've committed (or at least, not because of any international crime), but because the FBI finds their network to be interesting and wants to get that person's "cooperation" to learn more about it.

Side note: one premise of the Durham Report is that the use of informants, which the FBI considers a really low-impact investigative step, is actually really intrusive. I still believe nothing good will come out of the Durham Report, but a public debate about how intrusive the public and Congress believes the use of informants to be, which is dramatically different than what the FBI thinks, could lead to an adjustment of how it is treated in FBI's Domestic Investigations Guide, would be one such good outcome.

Because only the target of a warrant has a Fourth Amendment interest, tons of communications of innocent people get swept up with every warrant, just as tons of communications of innocent people get swept up with every 702 directive. But as FISC imposes new requirements on FBI queries, the latter has started to be treated with far greater protection than the former. That makes sense from a legal perspective (because the former was collected with a probable cause warrant but the latter was not), but not from a privacy perspective. The privacy community has spent years getting worked up about the 702 queries while largely ignoring the privacy impact of all the other data on which these very same queries

are run.

Another dirty little secret is that FISA allows the privacy community visibility on FBI behavior that the privacy community has to do a lot more work to get in the criminal context. So every three years the privacy community has an opportunity to make a big stink and raise money from donors, all while very similar criminal data is being queried zillions of times a year with little notice.

Which leads me to the second underlying problem here, The Wall. Whether true or not, one reason spooks used to excuse their failure to prevent 9/11 is that they weren't permitted to use data collected using intelligence authorities in criminal investigations (which, in turn, made it harder to use intelligence information to coerce informants). So FISC was forced to permit the use of information collected using individualized FISA orders in criminal prosecutions (which only happens around ten times a year). But that approval was grand-fathered onto 702 collection. Because the FBI has a dual intelligence/law enforcement role, it was permitted to ask for a small percentage of the content collected under 702. But for years, that content got sucked into FBI databases and treated just like all the other content they had ingested, with the result that 702 content was queried zillions of times in usually fruitless searches a year. It is absolutely the FBI's job to hunt down foreign hackers, terrorists, or spies using 702 data. But when those foreign hackers, terrorists, or spies network with Americans, because of the way The Wall came down after 9/11, that 702 data can be used to predicate investigations against Americans.

The legal contortions around justifying the way the barrier formerly known as The Wall have gotten really remarkable, always premised on the notion that what's outside the US has national security implications but what's inside does not. Again, in a globalized world — especially one in which domestic terrorism is a bigger

threat than international terrorism — that's a ridiculous stance. The stance arises from the definition of Presidential (and Executive) power, not from threats to the country.

The privacy community has decided they're going to fight for an individualized warrant for every query, including "queries" that are part of combatting cyberattacks (including cyberattacks against corporate entities), which is what the IC credibly claims they're increasingly using 702 for. They're asking for this standard even though the FBI doesn't have to get individualized warrants for queries of material obtained with a warrant.

My Modest Proposal would instead require the FBI to get a probable cause criminal warrant on the collection targets themselves for everything they otherwise would get under 702, targeted at the intelligence target, rather than the query target before they can query it. But once they've done so, they could put it in the same bucket on which the FBI does their zillion searches every year. Because, after all, at that point it would become the same kind of data. The FBI could keep other 702 data on entirely separate servers for use only with regards to the FBI's foreign targets. There already is one such server at the FBI, because the FBI hasn't been able to do drop down menus to record the purpose of queries to comply with the evolving query requirements.

I suspect that my Modest Proposal might be what results if this debate blows up — though it might happen with little notice. I say that because that's precisely what has sometimes happened in the past when authorities surrounding surveillance techniques used in counterterrorism were made more onerous. Back in 2014, FISC required a higher standard to obtain prospective cell site location data than a number of states would, so in some cases, the FBI would choose to use criminal process rather than FISA process. Similarly, the reason the FBI never needed to rely on the Section 215 phone

dragnet to find suspected terrorists in the US is that phone records are really easy to get in the US, and the FBI could accumulate enough of those phone records to get the coverage they needed. The number of individualized FISA orders has similarly dramatically shrank after the Carter Page fiasco — but that surveillance didn't go away, it just went somewhere else, and much of that spying can be via other authorities.

Much of the content that the FBI obtains under 702 is cloud data from US providers, and the FBI has been able to do entire foreign focused national security investigations using criminal process, such as when the FBI indicted GRU hackers using much the same criminal process used to successfully prosecute Vladimir Klyushin. At least with regards to cloud providers, what you can't get from a probable cause warrant, but that you get from 702, is prospective coverage, with new communications coming in on a timely basis in real time. But DOJ gets a shit-ton of stuff when they obtain warrants for cloud providers.

Such a Modest Proposal might require a kind of programmatic warrant — say, targeting all of GRU's known identifiers. This kind of programmatic targeting was likely used for Section 215 when Obama imposed pre-approval for those queries. There would just be lots more of them, You'd have to create a FISC Magistrate to deal with the volume.

One more thing has changed in recent years that would make this feasible — which change would accelerate if the FBI had to use probable cause warrants to get the same data they're currently getting under 702: The FBI has focused on a variety of crimes — foreign agent laws, sanctions violations, and cryptocurrency enabled crimes — that'd be the kinds of crimes they'd use if forced to get probable cause warrants on targets. If they were forced to go this route, there'd be more open investigations into people, including US persons.

It would ensure that data searched in any of the FBI’s zillion yearly searches was obtained using a warrant. But it wouldn’t at all limit the number of Americans exposed to such searches. And it would wildly limit the oversight on such searches.