Twitter Thread by Julian Sanchez

Julian Sanchez
@normative

I suppose I need to do a proper thread about this Durham filing folks are losing their minds over. OK, here goes.

First, virtually none of what appeared in the recent filing from Durham's office is new information. Here's a New York Times story from *over four months ago* with basically all of it. https://t.co/USr70d8NfD

Second, nothing in the filing supports breathless claims technically illiterate cable hosts are making. It does not allege anyone "hacked" Trump computers, or was paid to "infiltrate" networks, or that anyone "intercepted e-mails and text messages."

Here's a simplified version of what it does say, again, virtually all of which was reported in an obscure little alternative news outlet called The New York Times back in September.

A Virginia-based tech company called Neustar, which provides a variety of Internet registry & security services, had lawful access to databases of government DNS data as part of a contract to monitor for malware & cyberattacks, which was provided to Georgia Tech researchers.

For the non-technical: "DNS" = "Domain Name System." It's basically the Internet's equivalent of a phone directory, translating human-intelligible addresses like "https://t.co/ts8QkYZBcj" into the numerical IP addresses computers use to send each other information.

DNS lookup data, which is what Neustar & the Georgia Tech researchers had, does not include the contents of Internet traffic. It tells you when a computer was looking for the address of another computer. ("Hey, address book, I need the current IP address of website-dot-com.")

The GA Tech researchers—whose job was to look for suspicious patterns in the DNS record they'd been provided—found various things they regarded as suspicious.

In particular, they found evidence of unusual volumes of traffic between servers associated with the Trump Organization and a Russian bank, as well as evidence of (rare in the US) Russian-made smartphones near the White House.

The researchers wrote up their suspicions, which then-Neustar executive Rodney Joffe passed on to attorney Michael Sussman, who also did work for the Clinton campaign. Sussman shared their findings with the FBI and later CIA.

Some aspects of this are potentially shady. There's likely an innoccuous explanation for the data the researchers found suspicious, and both they and Joffe seem to have disliked Trump.

Obviously, I don't have the data they looked at, and wouldn't be qualified to evaluate it if I did. Durham seems to think their views of Trump colored their evaluation of how suspicious the data was. I don't know, but it's possible.

That said: Neither Joffe nor the GA Tech researchers were being paid by the Clinton campaign. Nobody "hacked" or "intercepted" anything. They were analyzing data they had lawful access to, in order to look for suspicious patterns that might suggest foreign cyberattacks.

Neither Joffe nor the researchers are accused of any crime. Sussman is accused of lying about whether he was working on Clinton's behalf when he passed their findings on to FBI, which he denies.

So is there anything to this? Well, maybe! But probably not a ton. It's possible that Joffe & the researchers read the data as more suspicious than it really was, and that their negative view of Trump influenced their interpretation of what they were seeing.

That's clearly Durham's view. I don't know; again, I'm not competent to check their work, but it's possible.

That said, I haven't seen anyone who IS competent suggest that this was some crazy fabrication. In other words, it's not that it wasn't suspicious, it's that it WAS suspicious but maybe there turns out be an innocent explanation.

In any event, it's a little difficult to see what any of these parties are supposed to have done wrong. They found suspicious traffic in data they were lawfully provided to analyze for that purpose, and reported their findings to law enforcement.

Maybe it turns out there was nothing there—it's frankly still not completely clear what the traffic was—but there's no evidence suggesting any of this was elaborately masterminded by Hillary Clinton.

The rather tenuous Clinton link is that Joffe passed the researchers' findings on to FBI & CIA via Sussman, a prominent cybersecurity lawyer who'd also done work for the Clinton campaign.

Durham says Sussman was working on Clinton's behalf as well as Joffe's when he met with FBI officials to convey the data, and lied about it. Sussman denies this, and the evidence seems pretty thin, but we'll see how that plays out in court.

Two pertinent points: The White House data concerning Russian phones dated from the Obama administration, and was shared with CIA well after the campaign (and Sussman's work for the campaign) ended. So that doesn't square well with Durham's theory.

So is this all a big nothingburger? Well, no, not entirely. But (as with previous FISA stories), the right media's desire to find a huge dramatic Watergate-level conspiracy is obscuring the kernel of a legitimate policy issue.

What I see as the legitimate policy issue is that you've got private cybersecurity researchers & companies making somewhat ad-hoc decisions about when to disclose nonpublic telecommunications data to the government.

The Electronic Communications Privacy Act spells out a legal process by which FBI (or other law enforcement) can obtain telecommunications metadata from providers. Providers may not disclose it directly to government outside that process, with specific exceptions.

With the Alfa Bank data, you've apparently got researchers conveying information gleaned from Neustar's DNS lookups to law enforcement via an intermediary. That was probably legal, but also reflects a loophole in federal privacy law.

And I think there's an important policy conversation to have about that: Are we comfortable with a status quo where outside researchers get this sort of access to your DNS lookups, and then hand that data to the FBI if they deem it suspicious?

Especially where, as here, the stated purpose is to look for signs of foreign cyberattacks, but what gets reported is not really evidence of an apparent attack on the U.S. firm.

So there IS, I think, a potential story and a serious policy issue here. It's just about a million miles away from "ZOMG Killary hacked Trump's computers at the White House."

The serious story is about who has access to our DNS data—which is not traffic content, but nevertheless potentially quite revealing—and under what circumstances it can be shared with the government.

And there are concerning features of this case, I think, even if we put aside the "Grand Hillary Plot" version of the story. The Alfa link ended up leaking to the press just before the election, although with an exculpatory framing. https://t.co/UOtbSqtN5t

Even without the Grand Plot narrative, this should be troubling. Researchers with (legal) access to nonpublic Internet metadata spot something they deem suspicious linked to a presidential candidate.

They share this with the FBI, thanks to a loophole in the law that bypasses the judicial process. Congress gets briefed, and soon it's on the front page of the newspaper shortly before an election.

Do I think the Clinton campaign orchestrated all this? No. Is it great for democracy that ambiguous analysis of Internet traffic linked to candidates is disclosed at the discretion of security researchers? Also no.

Again, as with FISA, this seems to interest the frothier corners of the media only to the extent it feeds into a narrative about some kind of insidious conspiracy. And the evidence for that just ain't there.

But there is, I think, evidence that fuzzy rules around access to (and sharing of) metadata end up making the disclosure of sensitive data most of us would expect to be private highly discretionary.

And I think you can reasonably question whether that's how we want this stuff to work, without it being a crime, or a plot, or BIGGER THAN WATERGATE.

I will, incidentally, note something of a pattern here. There were serious problems with the FISA process used to target Carter Page. But it was only interesting if it was part of a Deep State Plot to Get Trump.

There are valid questions to raise about the unmasking of Tucker Carlson's identity in disseminated intelligence reports gleaned from monitoring of Russian officials, but it turned into fantasies about NSA SPYING ON ME TO TAKE MY SHOW OFF THE AIR.

Here we have a story that I think ought to be at least somewhat concerning about the potential political impact of gaps in federal rules governing access to and sharing of telecommunications metadata.

The coverage from right-wing media is a technically illiterate conspiracy corkboard covered in yarn, and the mainstream coverage thus far has mostly been about pointing out why that's silly and wrong.

In all of these cases, the compulsive need to generate conspiratorial froth pitched at outraging people half-watching cable from a barstool obscures the kernel of a real story. Not the SCANDAL OF THE CENTURY, but a story meriting thought and attention.

And then coverage by more serious reporters end up itself being conditioned by the froth (and the need to whack through the many, many false claims bubbling out of it).

And the latter is sort of understandable! You have Fox hosts literally saying, verbatim, "Hillary Clinton hired people who hacked into Donald Trump's home and office computers and planted evidence…". Every part of that is a preposterous lie.

So you almost have to clear the air before you can get to the real story. And maybe the commercial imperatives driving journalism make the "Sexy Scandal or Nothingburger?" Frame inevitable. But it's too bad.

A final note: Again, none of this is new information. The New York Times reported all this four months ago. The current freakout follows Durham's inclusion of it in an oddly lengthy "background" section to a completely unrelated motion.

So this does look a bit like an effort from Durham's camp to fan the flames, though the really outrageous lies the cable talkers came up with don't resemble anything in Durham's filing.

I note that we are coming up on 3 years of the Durham probe, during which time he has successfully prosecuted one case of genuine misconduct by a DOJ lawyer, handed to him on a silver platter by the IG, and filed one very weak-looking case for lying to the FBI against a lawyer.

As @emptywheel & others have noted, this comes right after the statute of limitations lapsed for any charges to conceivably be brought concerning the 2017 CIA meeting.

So there’s an odor to all this of an effort to create the appearance of having uncovered some grand conspiracy that Durham has no intention of attempting to actually prove or charge.

Yeah, this is a relevant point I should have mentioned: At present, to the chagrin of infosec folks, most DNS resolution requests are still unencrypted. https://t.co/mRpXjUx9Ik

> DNS queries are non-encrypted data that flows over the internet. If I know someone's IP I can use @WiresharkNews (or similar) to find out all sorts of things about what they're doing.
>
> — Dr. Brandon E.M. Savage (@SavageDrums) February 16, 2022

That’s gradually changing, but in 2016-2017, this almost certainly would have been data visible to anyone running basic network admin tools anywhere between the client & the resolver.