

# MATT TAIBBI CONFESSES HE HASN'T READ HIS OWN TWITTER FILES

Matt Taibbi, whom I have taken to calling "#MattyDickPics" for his wails about tweets that were part of a coordinated revenge porn campaign targeting Hunter Biden being taken down, confessed yesterday he knows virtually nothing about his own "Twitter Files" campaign, including what he himself has posted. In response to a Twitter account with just four followers that observed that his campaign had exposed nothing, MattyDickPics tweeted the following:



**Matt Taibbi** 

@mtaibbi

This has nothing to with investigations. These DHS/FBI programs are not for building cases. It's a one-way communication stream with Twitter at the end processing spreadsheets full of government-generated moderation requests. Not even close to the criminal case-building mission.

**Robert Caldwell** @RobertCald98

Replies to @MrNChance @mtaibbi

That's the thing. Nothing's been exposed. Law-enforcement agencies that use websites to conduct investigations. It's called completely fucking normal behavior. There's nothing here and you're desperate for something to be here

Before I use MattyDickPics to debunk MattyDickPics, let's first unpack his claims: He says that, "These DHS/FBI programs are not for building cases" which he judges is "Not even close to the criminal case-building mission."

Let's talk about his premise, first of all – the claim that the "mission" is about "criminal case-building."

The Cybersecurity & Infrastructure Security Agency, the part of DHS that runs what Taibbi calls a "program," describes its public-facing mission this way:

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.

In his January 6 Committee testimony, former CISA Director Chris Krebs described the kinds of things CISA would do to help protect the vote.

In terms of the bidding internal to the U.S. Government on who had lead in those three areas [targeting of campaigns, targeting of election infrastructure, disinformation], it was clear, you know, once Jeh Johnson, the prior Secretary in 2017, January of 2017, designated election infrastructure critical infrastructure, it was, you know, CISA had the lead for working with State and local election officials on protecting critical infrastructure – or election infrastructure. That's the systems. That's the hardware. That's the

equipment and the processes associated with conducting an election.

Q And so can stop you there for a second?

A Yes.

Q Is that primarily protecting against what we would think of as hacking?

A No, not necessarily. It's, again, critical infrastructure, we had an all-hazards approach. So we worked with election officials to conduct active shooter drills and 13 assessments. We would go look at election warehouses where equipment is stored in the off season, do physical risk assessments. In the wake of hurricanes, we would work with election officials. In fact, Kyle Ardoin, who's the Secretary of State in Louisiana, in 2000 – the summer of 2020, I guess, where they got hit pretty hard by an election, we helped him work with FEMA and some of the response efforts there to get resources he needed to be able to conduct the election in 2020. So it was not just cyber. That tended to be the public – at least what the public cared about or the media cared about, just because it's 2016, but it was – again, it was an all hazards. And we did – I don't want to put numbers on it, because I don't recall, again, off the top of my head, but a significant number of physical assessments of election facilities.

[snip]

Q You talked earlier about the infrastructure and protecting that. How did you work with State officials to make sure that their – to help them ensure that their equipment was safe and secure?

A We had a number of different offerings

that we had. There's an entire catalog. There's an election security catalog. It's not in here because it's thick. But we would go out and conduct things like security and vulnerability assessments. We could do red team. We could do fairly in-depth assessments of voter registration database configurations 1) We had a, what's known as cyber hygiene scan that they would sign up for and we'd do a regular scan to see if anything touching the internet was mis- – well, not misconfigured, but running an old vulnerable version. We developed in the summer before the election a product called – or tool called Crossfeed, which was a little bit more in-depth of assessing vulnerabilities of systems and websites that are touching the internet. ~ And then we would provide them reports and technical assistance on how they might secure things.

The stuff that MattyDickPics is concerned about was an effort to facilitate state election officials' ability to rebut false claims about elections.

Q We've seen some documents that were produced by DHS relating to efforts to connect with social media platforms, Twitter, for example, to working with State and local officials to try to address claims that were being made on Twitter that were false.

A Uhhh,

Q Are you familiar generally with that initiative?

A I think generally, yes. And I gave an example of the 2018 election, at least, how we were able to connect I think it was Ohio with one of the platforms.

Q And it seemed as if that was a fairly

robust – I was going to say operation. That's probably too strong a word. But there was a fairly – it looked to be, from the documents I've seen, a fairly well-coordinated effort to put State officials in touch with the social media platforms and try to provide the information necessary to address what were false claims in their respective jurisdictions.

A I think certainly the efforts to make those connections was a priority. We had frequent – I think it was monthly – at least monthly I think monthly, let me put it that way meetings between interagency partners, so FBI, DNI, and CISA, with representatives from the social media platforms. And we sometimes did those out in California. You know, I would attend every now and then some of those meetings. Now, State and local partners were not there. This was just making sure the Federal Government and the social media platforms were connected and were sharing kind of our understanding of how things were playing out, what our concerns were.

None of that, CISA's role in information-sharing, is law enforcement. The one example Krebs mentioned that involved an attempted hack, CISA passed off to the FBI and intelligence agencies.

And there was a State, Delaware observed an unknown actor trying to exploit an Oracle database vulnerability that they had had patched. So what we were able to do is Delaware let us know. We said, that's interesting. ~ But because we were integrated with the FBI and the intelligence community and others, we could actually say, hey, 12 guys so it wasn't just for our benefit, like I said, decision support. We were able to share it with our operational partners

for them to go do whatever they need to do. So it was a functional operational watch cell, also coordinating situational awareness, coordinating action. And that was and that was the day.

CISA didn't ask for anything back from Twitter because CISA is not a law enforcement agency (note: one other thing MattyDickPics is referencing is that a Signal thread the FBI used for sharing information was treated as one way, but according to Chan, the social media companies would respond by other channels). It has no law enforcement mandate. It has no case-building mandate.

With regard to CISA – and MattyDickPics is not alone in this gross misunderstanding of CISA's mandate or legal status – MattyDickPics' entire premise is false.

But that also means his complaint is wrong. Is MattyDickPics complaining that people make an effort to correct errors about the election? Would he prefer that local election authorities try to chase down rumors and false claims themselves, even as they're putting in 16-hour days trying to run an election? Does he think that deliberate misinformation about elections, like non-consensually posted dick pics, must be protected on social media sites? Is he angry – as Elon Musk seems to be – that social media sites choose not to be the vehicle for messaging that makes it harder to conduct successful elections?

If you're complaining that an information-sharing agency is sharing information, then ultimately your complaint is that you don't think that information should be shared, that you don't think election officials should make an effort to ensure information about elections is clear and accurate – or at least, you don't think the federal government should do anything to protect elections. If that's your view, own it.

Even with FBI, MattyDickPics' premise that the mission is "case-building" is partly wrong. In addition to its law enforcement mission, FBI has a counterintelligence mission, which would cover a good deal of interaction with social media sites. Indeed, a great deal of entire threads of MattyDickPics' rants pertain to the FBI passing on assessments about such operations, as when accounts associated with the Internet Research Agency were shared. The FBI *has* built several cases against the IRA, but that's not the primary goal. The primary goal is to track how Russia and China and Iran attempt to interfere in our country.

Some of what MattyDickPics seems to misunderstand about this is that foreign spooks will pretend to be Americans as part of their efforts to fuck in democratic elections. For example, MattyDickPics has said nothing about the most significant hack-and-disinformation campaign from 2020, an Iranian attempt to pose as Proud Boys to send messages to Democrats to discourage them from voting. It's not impossible that some of what he has portrayed as FBI interest in "Americans" was actually an effort to adopt the identity of Proud Boys – effectively maligning right wing Trump supporters – as cover for their operation. This kind of FBI investigation might never result in charges – because you're never going to arrest the Iranian spooks behind it – but posing as American Proud Boys to interfere in the election could be charged under FARA laws.

One can complain about FBI's dual mission – lord knows I have! But one cannot claim that FBI has exclusively a case-building mission and be entirely accurate.

Still, maybe all that can be excused because MattyDickPics decided to respond to a 4-follower Twitter account that also misunderstood the premise of some of what this information sharing is about.

It's the claim that the FBI "program," at least, is not about building cases, that I find

outrageous.

Among the single screen caps that Twitter Files followers have latched onto most – along with one about Adam Schiff inappropriately and unsuccessfully trying to use Twitter's QAnon rules to protect staffers (I won't link that because MattyDickPics doxxed the person in question), a CIA official asking to be included in a public event, and the NSA asking whether Twitter still prohibited Dataminr from sharing the "firehose" of Twitter content with intelligence agencies (they did, though under Elmo, the Saudis and Qataris will reportedly be given access to it) – is this one, which they claim is proof that the FBI asked for location data without legal process:



**18.** In an internal email from November 5, 2022, the FBI's National Election Command Post, which compiles and sends on complaints, sent the SF field office a long list of accounts that "may warrant additional action":

A screenshot of an internal email from the FBI's National Election Command Post (NECP) to the San Francisco (SF) field office. The email is from ASAC Chan and is dated Sunday, November 6, 2022, 12:30 PM. The subject is "request for Coordination with Twitter". The email body discusses the request for coordination with Twitter regarding accounts that may warrant additional action. It includes a list of 25 Twitter accounts and a note that the FBI will provide follow-up information. The email ends with a "Please let us know if you need additional information to process this request by replying all to this email." and "Thanks, -Michael".

9:00 PM · Dec 16, 2022 · 8.3M Views

As a threshold matter, note what this is not: an email from Elvis Chan, the guy in charge of San Francisco's Election Command Post, to Twitter. It is an email from the National Election Command Post to *Chan*. MattyDickPics doesn't

explain how Twitter got this. He has “censored” how Chan sent this to Twitter.

Before I get into the content, let me repeat some background that two of Elmo’s pets, at least, claim to be familiar with, which I laid out here. Here’s how Chan explained the actions of both the National and San Francisco Election Command Post, which is behind a great deal of the FBI to Twitter requests MattyDickPics wails about.

A. During FBI San Francisco’s 2020 election command post, which I believe was held from the Friday before the election through election night, that Tuesday at midnight, information would be provided by other field offices and FBI headquarters about disinformation, specifically about the time, place or manner of elections in various states. These were passed to FBI San Francisco’s command post, which I mentioned to you before I was the daytime shift commander, and we would relay this information to the social media platforms where these accounts were detected. So I do not believe we were able to determine whether the accounts that were posting time, place or manner of election disinformation, whether they were American or foreign.

Q. But you received reports, I take it, from all over the country about disinformation about time, place and manner of voting, right?

A. That is – we received them from multiple field offices, and I can’t remember. But I remember many field offices, probably around ten to 12 field offices, relayed this type of information to us. And because DOJ had informed us that this type of information was criminal in nature, that it did not matter where the – who was the source of the information, but that

it was criminal in nature and that it should be flagged to the social media companies. And then the respective field offices were expected to follow up with a legal process to get additional information on the origin and nature of these communications.

Q. So the Department of Justice advised you that it's criminal and there's no First Amendment right to post false information about time, place and manner of voting?

[snip]

A. That was my understanding.

Q. And did you, in fact, relay – let me ask you this. You say manner of voting. Were some of these reports related to voting by mail, which was a hot topic back then?

A. From my recollection, some of them did include voting by mail. Specifically what I can remember is erroneous information about when mail-in ballots could be postmarked because it is different in different jurisdictions. So I would be relying on the local field office to know what were the election laws in their territory and to only flag information for us. Actually, let me provide additional context. **DOJ public integrity attorneys were at the FBI's election command post and headquarters.** So I believe that all of those were reviewed before they got sent to FBI San Francisco.

Q. So those reports would come to FBI San Francisco when you were the day commander at this command post, and then FBI San Francisco would relay them to the various social media platforms where the problematic posts had been made, right?

A. That is correct.

Q. And then the point there was to alert the social media platforms and see if they could be taken down, right?

A. It was to alert the social media companies to see if they violated their terms of service.

[snip]

Q. And this command post was chosen to be – I mean, it addresses nationwide election-related information, right?

A. So every field office, every FBI field office was mandated by headquarters to stand at a command post at least on election day. And FBI San Francisco was responsible for relaying any time, place or manner disinformation or malign-foreign-influence information to the social media companies as well as accepting any referrals from the social media companies.

Q. So FBI San Francisco had the special job of referring concerns to social media companies?

[snip]

THE WITNESS: Yes, and the reason for that is because the majority of the social media companies are headquartered in FBI San Francisco's territory. [my emphasis]

That is, *much of this activity* (including this screen cap in particular) came in the context of a DOJ Public Integrity determination that lying about the time, place, or manner of voting might be a crime, and – Chan's understanding at least – referrals to Twitter had already been vetted by a Public Integrity prosecutor.

As I've noted, this is not a frivolous claim. In early 2021, one of Bill Barr's closest

associates, Seth DuCharme, then serving as EDNY US Attorney, charged a Jack Posobiec associate named Douglass Mackey with violations of the Ku Klux Klan Act for doing this kind of thing at scale, by tweeting that users could text their vote in rather than show up and cast it, in 2016. Almost 5,000 people responded to this campaign and texted in their “vote” for President. It took two years and some HuffPo reporting before Mackey was identified and several more years to charge him.

Mackey is aggressively contesting the charge, including on First Amendment grounds; his trial is scheduled to start on March 13.

There's even a tie between Mackey's campaign and Elmo's efforts to restore white supremacists to the platform. Right wingers have been lobbying Elmo to reinstate the pseudonymous [Ricky\\_Vaughn99](#) account.



**Ariweinstein** @poisoned... 9 Dec 2022  
@elonmusk @Ricky\_Vaughn99 must be reinstated he is a freedom fighter and friend of @Twitter. #freericky @WorldWarWang where's Ricky Vaughn



That's what this is about: Efforts, some conducted at scale, to suppress the vote of certain Americans by lying to them about how or when or where to vote. And the involvement of prosecutors *on the front end* indicates that this was not just an effort to alert Twitter to misinformation so it could remove it if it chose to. This activity – which, again, makes up a great deal of what MattyDickPics has wailed about – was conducted in the context of law

enforcement investigations.

But MattyDickPics has already confirmed that. The very screen cap in question – one of the screen caps that MattyDickPics’ frothers are most outraged about (caveating, again, that MattyDickPics chose to “censor” how Chan actually passed this onto Twitter) – asks for the following regarding 25 accounts that are “spread[ing] misinformation about the upcoming election:”

1. Coordination between [San Francisco’s Field Office] and Twitter to determine whether the accounts identified below have violated Twitter’s terms of service and may be subject any actions deemed appropriate by Twitter.
2. The issuance of preservation letters regarding any of the accounts identified below to preserve subscriber information and content information *pending the issuance of legal process*.
3. Any location information associated with the accounts that Twitter will voluntarily provide to aid the FBI in assigning any follow-up deemed necessary to the appropriate FBI field office.

MattyDickPics has focused primarily on Bullet 1: If this violates Twitters terms of service, then – the FBI request suggests – Twitter can choose to do what it wants. That’s the “censorship” of

efforts to dupe people into wasting their ability to participate in democracy that MattyDickPics is so outraged about.

Bullet 2, however, single-handedly refutes MattyDickPics' claim from yesterday. Chan was supposed to ask for preservation letters, a request that Twitter preserve the account long enough that the FBI could follow up with a subpoena and/or warrant to get the subscriber information and then the content. This screen cap is *explicitly* about FBI's case-building mission. MattyDickPics proved, on December 16, that MattyDickPics' claims yesterday are false.

And even Bullet 3 – the reason this was deemed such an abuse – is about building a case. The National Command Post was not asking, voluntarily, for information that would help it identify whose mother's basement this disinformation campaign was launched from, whether Brooklyn or Iran. Rather, it was asking for location information sufficiently detailed such that DOJ could assign follow-up leads to a US Attorney's office that might be able to prosecute it. In fact, Mackey is challenging his prosecution, in part, by challenging venue in Brooklyn, a subject on which Judge Nicholas Garaufis has reserved judgment. That request for location information – accompanied as it was by a request for preservation order to get location information with a warrant – was all part of building a case.

One can certainly argue that the prosecution of Mackey and people like him for trying to affect the election by duping people out of their vote is a violation of the First Amendment, just like one can argue, as MattyDickPics is, that Twitter should be forced to permit users to use the platform to dupe others – Mackey allegedly targeted Blacks and Spanish speakers – out of casting their vote.

That's a debate we can have.

But there's no debate about whether these Command Post requests came in a framework that

envisioned the possibility of case-building.  
MattyDickPics has already proven that  
MattyDickPics is lying about that.