

Pinned Tweet



Michael Shellenberger

@ShellenbergerMD · 12h

1. TWITTER FILES: PART 7 The FBI & the Hunter Biden Laptop How the FBI & intelligence community discredited factual information about Hunter Biden's foreign business dealings both after and *before* The New York Post revealed the contents of his laptop on October 14, 2020

In Twitter Files #6, we saw the FBI relentlessly seek to exercise influence over Twitter, including over its content, its users, and its data.

<https://twitter.com/mtaibbi/status/1603857534737072128>

In Twitter Files #7, we present evidence pointing to an organized effort by representatives of the intelligence community (IC), aimed at senior executives at news and social media companies, to discredit leaked information about Hunter Biden before and after it was published.

The story begins in December 2019 when a Delaware computer store owner named John Paul (J.P.) Mac Isaac contacts the FBI about a laptop that Hunter Biden had left with him

On Dec 9, 2019, the FBI issues a subpoena for, and takes, Hunter Biden's laptop.

<https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

Quote #7469

Bill To:
 -Lester Street
 200 550 4386
 info@lps.com

Quote covers for MacBook Pro. Allotted data capacity from 3 harddisk drive. Includes data for spare power and control customer when complete.

Qty	Item No.	Description	Unit Price	Extension	Total
1 (00)	Laptop	MacBook Pro 15"	\$85.00	\$85.00	\$85.00
		Total		\$85.00	\$85.00
		Grand Total			\$85.00

Signature: *[Handwritten Signature]*

Apple, the Apple logo, MacBook Pro, the MacBook Pro logo, and other marks are trademarks of Apple Inc., registered in the U.S. and other countries. All other marks are trademarks of their respective owners. © 2019 Apple Inc. All rights reserved. Learn more about Apple at apple.com.

UNITED STATES DISTRICT COURT
 for the
 District of Columbia

SUBPOENA TO TESTIFY BEFORE A GRAND JURY

To: [REDACTED] Case File Subpoena Number: [REDACTED]

YOU ARE COMMANDED to appear in the United States District Court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place: J. Cash Rogers Federal Building
 Room 3001, 401 King Street
 Washington, DC 20001

Date and Time:
 Response Due By: Tuesday, December 11, 2019

You must also bring with you the following documents, electronically stored information, or objects listed (if applicable):

In lieu of personal appearance, please see ATTACHMENT A.

Date: December 5, 2019

CLERK OF COURT
[Signature]
 Register of Clerk of District Court

The name, address, e-mail, and telephone number of the United States attorney, or assistant United States attorney, who requests this subpoena, are:
 Lindsey F. Wolf
 Assistant United States Attorney
 United States Attorney's Office
 1717 South Market Street, Suite 400
 Washington, DC 20009-2046
 Phone: (202) 725-4272

ATTACHMENT A

- Apple MacBook Pro Laptop Computer, Serial Number FV93C2MBIV29
- Western Digital (external hard drive); Serial Number: WX21A18A1993

By Aug 2020, Mac Isaac still had not heard back from the FBI, even though he had discovered evidence of criminal activity. And so he emails Rudy Giuliani, who was under FBI surveillance at the time. In early Oct, Giuliani gives it to [@nypost](#)

<https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

Shortly before 7 pm ET on October 13, Hunter Biden's lawyer, George Mesires, emails JP Mac Isaac.

Hunter and Mesires had just learned from the New York Post that its story about the laptop would be published the next day.

From: "Mesires, George R."
[REDACTED]

Date: October 13, 2020 at 6:58:59 PM EDT
[REDACTED]

Subject: George Mesires contact information

John Paul:

Thank you for speaking with me tonight. As I indicated, I am a lawyer for Hunter Biden and I appreciate you reviewing your records on this matter. Thank you.

George

George R. Mesires
Partner

[REDACTED]

[Faegre Drinker Biddle & Reath LLP](#)
[311 S. Wacker Drive, Suite 4300](#)
[Chicago, Illinois 60606, USA](#)

Welcome to **Faegre Drinker Biddle & Reath LLP (Faegre Drinker)** - a new firm comprising the former Faegre Baker Daniels and Drinker Biddle & Reath. Our email addresses have changed with mine noted in the signature block. All phone and fax numbers remain the same. As a top 50 firm that draws on shared values and cultures, our new firm is *designed for clients*.



7. At 9:22 pm ET (6:22 PT), FBI Special Agent Elvis Chan sends 10 documents to Twitter's then-Head of Site Integrity, Yoel Roth, through Teleporter, a one-way communications channel from the FBI to Twitter



Chan, Elvis M. (SF) (FBI)
Information Sharing

October 13, 2020 at 6:22 PM

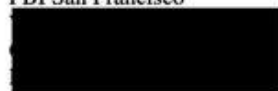
To: Yoel Roth, [REDACTED]

Twitter folks,

Heads up I will be sending a Teleporter link for you to download 10 documents. It is not spam! Please confirm receipt when you get it. Thanks.

Regards,

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco



Found in Roth Large Mailbox



Yoel Roth
Re: Information Sharing

October 13, 2020 at 6:24 PM

To: Chan, Elvis M. (SF) (FBI), Cc: Yoel Roth, [REDACTED] & 1 more

[Details](#)

Received and downloaded - thanks!

[See More](#) from Chan, Elvis M. (SF) (FBI)

8. The next day, October 14, 2020, The New York Post runs its explosive story revealing the business dealings of President Joe Biden's son, Hunter. Every single fact in it was accurate.



9. And yet, within hours, Twitter and other social media companies censor the NY Post article, preventing it from spreading and, more importantly, undermining its credibility in the minds of many Americans.

Why is that? What, exactly, happened?

10. On Dec 2, [@mtaibbi](#) described the debate inside Twitter over its decision to censor a wholly accurate article.

Since then, we have discovered new info that points to an organized effort by the intel community to influence Twitter & other platforms

<https://twitter.com/mtaibbi/status/1598822959866683394>

11. First, it's important to understand that Hunter Biden earned *tens of millions* of dollars in contracts with foreign businesses, including ones linked to China's government, for which Hunter offered no real work.

Here's an overview by investigative journalist [@peterschweizer](https://twitter.com/peterschweizer)
<https://twitter.com/i/status/1604878404486017026>

12. And yet, during all of 2020, the FBI and other law enforcement agencies repeatedly primed Yoel Roth to dismiss reports of Hunter Biden's laptop as a Russian "hack and leak" operation.

This is from a sworn declaration by Roth given in December 2020.

https://www.fec.gov/files/legal/murs/7827/7827_08.pdf

13. They did the same to Facebook, according to CEO Mark Zuckerberg. "The FBI basically came to us [and] was like, 'Hey... you should be on high alert. We thought that there was a lot of Russian propaganda in 2016 election. There's about to be some kind of dump similar to that.'"

<https://twitter.com/i/status/1604880181906116608>

14. Were the FBI warnings of a Russian hack-and-leak operation relating to Hunter Biden based on *any* new intel?

No, they weren't

"Through our investigations, we did not see any similar competing intrusions to what had happened in 2016," admitted FBI agent Elvis Chan in Nov.

1 **toward the 2020 election; is that right?**

2 A. For these USG-industry meetings, yes.

3 **Q. Were **hack-and-dump** operations discussed at**
4 **these meetings, or **hack-and-leak** operations?**

5 A. Yes, they were.

6 **Q. Tell me what was discussed about them at**
7 **these meetings?**

8 A. The context of **hack and** dump is what was
9 the FBI **and** CISA doing to prevent **hack-and-dump**
10 operations. So from the FBI side, I think we
11 already -- I already relayed to you that we had the
12 protective voices initiative. I can't remember the
13 specifics, but CISA also discussed its
14 cybersecurity awareness efforts as well as grants
15 efforts with the state-, county- **and** local-level
16 election officials.

17 **Q. Did anyone at these meetings tell the**
18 **industry participants to expect a Russian**
19 ****hack-and-dump** operation or **hack-and-leak** operation**
20 **shortly before the 2020 election cycle?**

21 MR. SUR: Objection; lacks foundation.

22 THE WITNESS: From my recollection, I
23 remember that the FBI warned -- that I or someone
24 from the FBI warned the social media companies
25 about the potential for a 2016-style DNC

1 MR. SUR: Objection in so far as the
2 answer calls for the law enforcement privileged
3 information.

4 You can answer, if you can, without
5 divulging the law enforcement privilege as to any
6 particular investigation.

7 THE WITNESS: Through our investigations,
8 we did not see any similar competing intrusions to
9 what had happened in 2016.

10 So although from our standpoint we had not
11 seen anything, we specifically, in an abundance of
12 caution, warned the companies in case they saw
13 something that we did not.

14 Q. BY MR. SAUER: So did you ask the
15 companies if they had seen any attempts at
16 intrusions or unauthorized access?

17 A. This is something that we -- that I
18 regularly ask the companies in the course of our
19 meetings.

20 Q. Did you ask them in these meetings?

21 A. Not at every meeting, but I believe I
22 asked them at some meetings.

23 Q. And did you repeatedly warn them at these
24 meetings that you anticipated there might be
25 hack-and-dump operations, Russian-initiated

1 **hack-and-dump operations?**

2 MR. SUR: Objection; vague, assumes facts
3 not on the record.

4 THE WITNESS: So repeatedly I would say --
5 can you -- can you ask your question like -- what
6 do you mean by "repeatedly"? Like 100 times, five
7 times?

8 **Q. BY MR. SAUER: Well, did you do it more**
9 **than once?**

10 A. I did it more -- yes. I warned the
11 companies about a potential for hack-and-dump
12 operations from the Russians and the Iranians on
13 more than one occasion, although I cannot recollect
14 how many times.

15 **Q. Did anybody else at the FBI talk about**
16 **hack-and-dump Russian operations?**

17 A. From my recollection, other senior
18 officials, to include Section Chief Dehmlow, likely
19 mentioned the possibility of hack-and-dump
20 operations.

21 **Q. Do you remember Section Chief Dehmlow**
22 **mentioning it?**

23 A. I said that I believe she mentioned it on
24 at least one occasion.

25 **Q. What did she say?**

1 hack-and-dump operation.

2 **Q. BY MR. SAUER: What exactly did you say to**
3 **the social media companies about that?**

4 A. Essentially what I just told you.

5 **Q. You said that there might be a Russian**
6 **hack-and-dump operation?**

7 A. So what I said was although we have not
8 seen any computer intrusions into national-level
9 political committees or election officials or
10 presidential candidates at this time, we ask you to
11 remain vigilant about the potential for
12 hack-and-dump operations, or something to that
13 effect.

14 **Q. Did you specifically refer to the 2016**
15 **hack-and-dump operation that targeted the DCCC and**
16 **the DNC?**

17 A. I believe I did.

18 **Q. Did you provide any basis to the social**
19 **media platforms for thinking that such an operation**
20 **might be coming?**

21 A. The basis was -- my basis was it had
22 happened once, and it could happen again.

23 **Q. Did you have any other specific**
24 **information other than it had happened four years**
25 **earlier?**

15. Indeed, Twitter executives *repeatedly* reported very little Russian activity.

E.g., on Sept 24, 2020, Twitter told FBI it had removed 345 “largely inactive” accounts “linked to previous coordinated Russian hacking attempts.” They “had little reach & low follower accounts.”

 Update on Russia Accounts
To: Chan, Elvis M. (SF) (FBI), Cc:  September 24, 2020 at 11:37 AM [Details](#)

Hi Elvis, we hope you are well.

We want to let you know about actions that we plan to publicly announce in the next hour. As you are aware, we are working with you and Facebook to permanently suspend accounts we can reliably attribute to Russia. Thank you for your ongoing cooperation and information sharing.

We are removing two distinct networks of accounts which we can reliably attribute to state-linked entities in Russia. Our investigations are ongoing.


The first network of accounts, totalling approximately 345, were largely inactive, and were linked to previous coordinated Russian hacking attempts. Most of the content shared by these accounts expressed views designed to advance Russia's geopolitical interests.

The second network of accounts, totalling approximately 10, purported to be associated with a website called United World International, which publishes a range of content about current global and US political issues. Links to United World International will be blocked on Twitter under our unsafe links policy detailed here.

The accounts included in this enforcement action [had little reach and low follower counts](#). We plan to send you // FITF relevant account information at the conclusion of our investigation.


Please let us know if you have any questions.

Thanks,


 Chan, Elvis M. (SF) (FBI) September 24, 2020 at 1:33 PM [Details](#)
RE: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Update on Russia Accounts
To: 

Excellent! Thanks for the heads up.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco


This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

16. In fact, Twitter debunked false claims by journalists of foreign influence on its platform

"We haven't seen any evidence to support that claim" by [@oneunderscore__](#) @NBC News of foreign-controlled bots.

"Our review thus far shows a small-scale domestic troll effort..."



Chan, Elvis M. (SF) (FBI)
Re: [SOCIAL NETWORK] Twitter referral
To: Yoel Roth, Cc: [REDACTED]

June 2, 2020 at 3:29 PM

[Details](#)

All,

Out of an abundance of caution, I wanted to reach out to you about this news story:

<https://www.nbcnews.com/tech/security/twitter-takes-down-washington-protest-disinformation-bot-behavior-n1221456>

The second part of the article focuses on the #dcblackout campaign and its potential to being driven by foreign-controlled bots. Anything we should be aware of concerning this topic? Thanks.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1
San Francisco Division
Federal Bureau of Investigation
[REDACTED]

[See More from Yoel Roth](#)



Yoel Roth
Re: [SOCIAL NETWORK] Twitter referral
To: Chan, Elvis M. (SF) (FBI), Cc: [REDACTED]

June 2, 2020 at 3:30 PM

[Details](#)

Hi Elvis,

We haven't seen any evidence to support that claim. Our review thus far shows a small-scale domestic troll effort that was amplified in some creative ways by real people - but not a significant bot or foreign angle.

Yoel

AFTER GEORGE FLOYD

White nationalist group posing as antifa called for violence on Twitter

Other misinformation and misleading claims spread across Twitter on Sunday night and into Monday related to the protests.



— Demonstrators stand around a fire during a protest near the White House on May 31, 2020.

Alex Wong / Getty Images

f t e | SAVE

Create your free profile or log in to save this article

June 1, 2020, 4:03 PM PDT / Updated June 1, 2020, 5:57 PM PDT

By Ben Collins, Brandy Zadrozny and Emmanuelle Saliba

A Twitter account claiming to belong to a national “antifa” organization and pushing violent rhetoric related to ongoing protests has been linked to the white nationalist group Identity Evropa, according to a Twitter spokesperson.

Sponsored Stories by Taboola



STUFF ANSWERED
Red Flag Symptoms of Psoriasis Most People Are Unaware Of

17. After FBI asks about a WaPo story on alleged foreign influence in a pro-Trump tweet, Twitter's Roth says, "The article makes a lot of insinuations... but we saw no evidence that that was the case here (and in fact, a lot of strong evidence pointing in the other direction)."

From: [REDACTED] <[REDACTED]@fbi.gov>

Sent: Monday, August 31, 2020 12:08 PM

To: Chan, Elvis M. (SF) ([REDACTED])

Subject: Twitter Account Inquiry: @WentDemtoRep

Hi Elvis-

I came across the following article in the Washington Post that referenced Twitter's removal of the account @WentDemtoRep due to policy violations: <https://www.washingtonpost.com/technology/2020/08/26/race-divisions-highlighted-disinformation-2016/>

According to the article, on the eve of the Republican National Convention, prominent African Americans challenged allegations of racism against President Trump, and retweeted the following message 22,000. Furthermore, the message amassed 39,000 likes within 19 hours after it was posted.

"I've been a Democrat my whole life... I joined the BLM protests months ago when they began. They opened my eyes wide! I didn't realize I became a Marxist. It happened w/o me even knowing it. I'm done with this trash. I'll be registering Republican."

At the time of suspension, was Twitter able to attribute this account and any of its activity to any particular country? In addition, did the aforementioned account, or any other suspended accounts, post similar messages related to the convention/upcoming 2020 US elections? Thank you in advance!

Respectfully,

[REDACTED]

Found in Roth Large Mailbox



Yoel Roth

Re: Twitter Account Inquiry: @WentDemtoRep

To: Chan, Elvis M. (SF) (FBI), **Cc:** [REDACTED]

August 31, 2020 at 2:15 PM

[Details](#)

Hi Elvis,

Thanks for checking in. I can confirm that the account in question is domestic in origin. The article makes a lot of insinuations about foreign interference - but we saw no evidence that that was the case here (and in fact, a lot of strong evidence pointing in the opposite direction).

Yoel

TECHNOLOGY

Black voters are being targeted in disinformation campaigns, echoing the 2016 Russian playbook

By Craig Timberg and Isaac Stanley-Becker

August 26, 2020 at 5:21 p.m. EDT



A Facebook post for a group called "Woke Blacks" was part of a Russian campaign in 2016 to discourage minority groups from voting. Race remains a key factor in disinformation campaigns as the 2020 presidential election approaches. (Jon Elswick/AP)

Comment 79 Save Gift Article Share

Four years after Russian operatives used social media in a bid to exacerbate [racial divisions in the United States](#) and suppress Black voter turnout, such tactics have spread across a wide range of deceptive online campaigns operated from numerous nations — including from within the United States itself.

18. It's not the

first time that Twitter's Roth has pushed back against the FBI. In January 2020, Roth resisted FBI efforts to get Twitter to share data outside of the normal search warrant process.

On Fri, Dec 20, 2019 at 1:02 PM Chan, Elvis M. (SF) (FBI) [REDACTED] wrote:

Hi [REDACTED]

My colleagues at the Fort had a query for you. I've provided it to you below:

A few years ago, Twitter said they would no longer provide their data feed to members of the IC. My colleagues wanted to know if that policy has changed or if you would be willing to change it. My colleagues are currently contracting with a vendor for an analytic tool for open source intelligence (only publicly available data). The commercial version of this tool includes the Twitter data feed. However, the feed was disabled because the vendor said they did not want to violate their terms of service with Twitter. My colleagues are wondering if Twitter would be open to revising its terms of service to allow this vendor to continue having access to the Twitter feed? My colleagues are happy to meet in person to discuss this issue with you if you'd like.

I hope you have a great holiday season!

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security Cyber
FBI San Francisco

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.



Yoel Roth

Re: OGA Query

To: [REDACTED]

January 7, 2020 at 5:20 PM



-Elvis

Hey [REDACTED]

As discussed, here's my suggested response - of course feel free to tweak/edit, but I tried to hit on the major points:

At this point, we don't think a call directly with your colleague at the Fort is the best path forward. As a rule we're not able to directly discuss data licensing relationships with third parties (such as the customers of our data customers), both due to confidentiality reasons and limited information on our end about the business decisions that may have led one of our customers to decline to provide services to the government. We also have a long-standing [policy](#) prohibiting the use of our data products and APIs for surveillance and intelligence-gathering purposes, which we would not deviate from. Ultimately, we want to be good partners to government and help combat our shared threats – but the best path for NSA, or any part of government, to request information about Twitter users or their content is in accordance with valid legal process.

Thanks,

Yoel

19. Pressure had been growing:

“We have seen a sustained (If uncoordinated) effort by the IC [intelligence community] to push us to share more info & change our API policies. They are probing & pushing everywhere they can (including by whispering to congressional staff).”



Carlos Monje

Re: OGA Query

To: Yoel Roth, Cc: [REDACTED]

January 2, 2020 at 11:34 AM

[Details](#)

I def agree with the caution here.

We have seen a sustained (If uncoordinated) effort by the IC to push us to share more information and change our API policies. They are probing and pushing everywhere they can (including by whispering to congressional staff). We should stay connected and keep a solid front against these efforts. My sense from the exchange below is that Elvis is sending a message he was asked to, but that he doesn't feel ownership of it and a polite discussion will suffice to answer the mail here.

Do we know which commercial provider is being referenced here by the clues offered? Do we feel like there is any additional guidance we can give to those companies that could help clarify our rules and minimize their efforts to point back at our API rules when they feel pressure from governments? It seems that DataMinr has gotten that message clearly, but we keep getting additional queries from elsewhere..

[See More from Yoel Roth](#)

--

Carlos Monje Jr.
Director of Policy & Philanthropy, United States & Canada
Twitter, Inc.
@CarlosMonjeJr
cmonje@twitter.com

20. Time and again, FBI asks Twitter for evidence of foreign influence & Twitter responds that they aren't finding anything worth reporting.

"[W]e haven't yet identified activity that we'd typically refer to you (or even flag as interesting in the foreign influence context)."

 Yoel Roth May 31, 2020 at 12:39 PM
Re: [SOCIAL NETWORK] Re: Current Status [Details](#)
To: [REDACTED]

Hi [REDACTED] and team,

We're continuing to closely monitor the situation, and haven't yet seen anything that's in line with Senator Rubio's tweet. We've heard that the tweet may have been based on a miscommunication between the Senate Intelligence Committee staff and Graphika (who they employ for narrative analysis and investigations) – but we haven't gotten any specifics beyond that.

At this stage, my team's findings have largely been that US-based trolling groups are behind some of the on-platform violative activity and misleading information we've seen. While much of this violates our terms of service, we haven't yet identified activity that we'd typically refer to you (or even flag as interesting in the foreign influence context). We're still investigating some of the new developments this morning involving Anonymous (such as #OpDeathEaters, which has been focused on a resurfacing of old Jeffrey Epstein related court documents).

As always, if there's anything you become aware of that might be interesting, please feel free to flag to us. Any source of signal on these issues is much appreciated.

Yoel

 Yoel Roth June 26, 2020 at 8:18 AM
Re: FW: Possible Terms of Service Violation - Twitter Follow Up [Details](#)
To: [REDACTED]

Thanks, [REDACTED]

Hi Elvis and team - wanted to briefly follow up on this one following our review. First, I want to apologize for any confusion here; a tooling bug on our end resulted in one of the accounts not being correctly enrolled in our authenticity checks, which is why you saw it stay online even after the others came down. We've fixed the issue.

Beyond that, to the extent the FITF is able to share any information about the sourcing of these accounts – even at a very high level, i.e. sourced from USG information, sourced from researchers outside USG who do not have access to classified information, etc – it would be much appreciated. While the accounts showed some signs of inauthenticity, they weren't so clear-cut on our end that they'd trigger a proactive referral of associated accounts or content to the Bureau. We don't at this time have clear indication that they are foreign in origin. I recognize that the Bureau's ability to share sourcing information in these cases can be constrained; but anything you're able to share that might help further our investigation here could potentially enable additional review and sharing on our side.

Thanks,

Yoel

21. Despite Twitter's pushback, the FBI repeatedly requests information from Twitter that Twitter has already made clear it will not share outside of normal legal channels.

From: Yoel Roth <yoel@twitter.com>

Sent: Monday, July 13, 2020 11:43 AM

To: [REDACTED] (CID) (FBI) <[REDACTED]>

Subject: [SOCIAL NETWORK] Re: [SOCIAL NETWORK] Re: FW: Possible Terms of Service Violation - Twitter Follow Up

Hey [REDACTED]

Sorry about the delay.

In terms of VOIP usage: Twitter requires people registering an account to confirm either an email address or a phone number. And, in the course of using Twitter, we may require accountholders to confirm a phone number if we detect any indications of suspicious activity originating from their accounts. Several of the phone numbers we observed associated with these accounts appeared to be linked to VOIP phone providers - a relatively common tactic for obtaining phone numbers for the purpose of account confirmation.

As for the VPN information: After consulting with [REDACTED], we would need legal process to provide further information about the IPs, subnets, providers, etc, associated with the authentication IPs from these accounts.

Thanks,

Yoel

On Thu, Jul 9, 2020 at 4:50 PM [REDACTED] (CID) (FBI) <[REDACTED]> wrote:

Hi Yoel-

Thank you again for taking the time to look into this matter; we really appreciate it. When available, I had a few follow up questions I'm hoping you can answer. Based on my understanding, Twitter observed some of the accounts using VPNs and VOIP as a way to obfuscate their online activities. Based on what you're seeing, would you be able to advise how the account holders were using VOIP on Twitter's platform? Also, while I understand obtaining the actual VPN IP addresses associated with the respective accounts would likely require legal process, would Twitter be open to sharing which service provider(s) those VPN IP addresses resolved to?

Please let me know if you have any questions. Thank you in advance for your time!

Respectfully,

[REDACTED]
Counterintelligence Division
Foreign Influence Task Force - Global Unit
[REDACTED]

22. Then, in July 2020, the FBI's Elvis Chan arranges for temporary Top Secret security clearances for Twitter executives so that the FBI can share information about threats to the upcoming elections.



Chan, Elvis M. (SF) (FBI)
Security Clearances

July 15, 2020 at 12:09 PM

To: Yoel Roth, [REDACTED]

All,

Since I brought up the security clearances during our call, I don't think we have anyone at Twitter who has a permanent security clearance. Correct me if I'm wrong. What I would propose is that 30 days out from the election, we get you temporary clearances. You get to pick who they would be. Let me know what you think. Thanks.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco



This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.


23. On August 11, 2020, the FBI's Chan shares information with Twitter's Roth relating to the Russian hacking organization, APT28, through the FBI's secure, one-way communications channel, Teleporter.

 Chan, Elvis M. (SF) (FBI) September 15, 2020 at 5:04 PM
RE: More Information Sharing
To: Yoel Roth, 

All,

I've got more information to share with you via Teleporter. You'll see an email from it shortly so you can download the document. Thanks!

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco



This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: Chan, Elvis M. (SF) (FBI)
Sent: Tuesday, August 11, 2020 6:28 PM
To: Yoel Roth <yoel@twitter.com>; 
Subject: Information Sharing

Alcon,

In advance of this week's meeting, I'm going to be sending you three documents through an FBI application called Teleporter. You will get a link from noreply@teleporter01.org which will expire in 24 hours. Please download the documents when you get a chance. The documents will not denote the actors so I'm providing them here: A – FITF topic, B – APT28, C – Sandworm. We will be discussing A & B, but don't have anything additional for C at this point. Thanks.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco


24. Recently, Yoel Roth told [@karaswisher](#) that he had been primed to think about the Russian hacking group APT28 before news of the Hunter Biden laptop came out.

When it did, Roth said, "It set off every single one of my finely tuned APT28 hack-and-leap campaign alarm bells."

<https://twitter.com/i/status/1604892289800605697>

25. In Aug, 2020, FBI's Chan asks Twitter: does anyone there have top secret clearance? When someone mentions Jim Baker, Chan responds, "I don't know how I forgot him" – an odd claim, given Chan's job is to monitor Twitter, not to mention that they worked together at the FBI

From: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Sent: Wednesday, August 26, 2020 2:43 PM
To: [REDACTED]
Cc: Dehmlow, Laura E. (CD) (FBI) <[REDACTED]@fbi.gov>
Subject: RE: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Re: TS Briefing

[REDACTED]

I don't know how I forgot Baker is there now. Yes, he would be perfect. Can you put us in touch with him? We're trying to nail down a date/time to provide the briefing. I'm hoping there will be an unclassified tear line that can be shared as well. Thanks!



Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: 415-553-7605
Cell: 510-719-6196
Email: [REDACTED]

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED]
Sent: Wednesday, August 26, 2020 11:40 AM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]
Cc: Dehmlow, Laura E. (CD) (FBI) [REDACTED]
Subject: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Re: TS Briefing

Hi, Elvis! Yes, we have two people. Would Jim Baker work? Let me know.

On Wed, Aug 26, 2020 at 11:35 AM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

Hi A [REDACTED]

FITF asked us to work with you to identify if there is anyone at Twitter who currently holds a TS clearance so they can get a briefing on something. I was told there might be a recent Twitter hire who still carries a TS clearance. Can you let us know what you think? Thanks!

Regards,



Elvis

1 exactly, but maybe two months ago.

2 **Q. BY MR. SAUER: How often do you talk to**
3 **her?**

4 A. Maybe on a quarterly basis.

5 **Q. Have you ever discussed with Mr. Strzok or**
6 **Ms. Page the prospect of a Russian hack-and-leak**
7 **operation?**

8 A. No. The only investigation that I ever
9 discussed with either of them was the Yahoo! hack
10 investigation.

11 **Q. Do you know anyone else associated with**
12 **the Crossfire Hurricane investigation?**

13 A. No. But I do want to add during those
14 meetings that I had with Mr. Strzok, Mr. Jim Baker,
15 who was our general counsel at the time, would
16 attend some of those meetings as well.

17 **Q. Mr. Baker would attend those meetings that**
18 **you had with Mr. Strzok about the Yahoo! hack?**

19 A. Yes. At least some of them.

20 **Q. Who else would attend those meetings?**

21 A. Just the three of them. It would be the
22 three of them getting a status update from -- they
23 would be getting a case update from me.

24 **Q. A case update about the Yahoo!**
25 **investigation?**

26. Who is Jim Baker? He's former general counsel of the FBI (2014-18) & one of the most powerful men in the U.S. intel community.

Baker has moved in and out of government for 30 years, serving stints at CNN, Bridgewater (a \$140 billion asset management firm) and Brookings

Jim Baker

SUMMARY AND OBJECTIVES

Effective, adaptive, and values-driven senior executive with extensive leadership, management, legal, policy, media, and teaching experience in several world-class organizations in the public, private, and educational sectors. Seeking opportunities with a dynamic and impactful organization facing a range of complex and demanding challenges. Experience includes:

- Substantial private sector legal experience in the tech/social media, telecom, and financial sectors.
- Former chief legal officer of the Federal Bureau of Investigation (FBI), a global national security and law enforcement agency with 36,000 employees and a \$8.7 billion budget.
- Reputation as "one of the most trusted, longest-serving national security officials in the [U.S.] government." *The Washington Post*, December 21, 2017.
- Inspirational leader of several large organizations facing numerous hard challenges.
- Reliable partner for senior management teams in high-impact and high-stress operational environments.
- Strategic thinker and innovative problem-solver in a broad range of substantive areas.
- Proven ability to develop and maintain productive relationships with key stakeholders.
- Dedicated mentor and coach focused on recruiting and retaining high-performers.
- A leading legal and policy expert on technology, privacy, cybersecurity, and surveillance.
- Substantial legislative experience, including numerous appearances before the U.S. Congress.
- Effective internal and external communicator with significant public speaking experience.
- A leader who values and promotes diversity and inclusion.
- Senior Executive Service (SES) member in the U.S. federal government for 14 years.

PROFESSIONAL WORK EXPERIENCE

Deputy General Counsel and Vice President, Legal
Twitter, Inc., San Francisco, California

June 2020-Present

Provide legal advice regarding litigation, law enforcement, national security, content moderation and enforcement, public policy, and human rights matters globally for a prominent social media company. Lead a worldwide team of 300 trust and safety professionals who address voluminous and time sensitive law enforcement requests and copyright/trademark matters. Regularly advise the board of directors, CEO, chief legal officer, and general counsel on a wide range of highly complex and critical matters.

Member, Board of Directors
enable, Inc., Boston, Massachusetts

February 2020-Present

Serve as a member of the board of directors of an artificial intelligence/machine learning start-up in the productivity enhancement space.

Principal **May 2018-Present**
JKV Advisors, LLC, Takoma Park, Maryland

Provide strategic advisory services to technology sector companies confronting difficult security, cybersecurity, and privacy risk issues.

Policy Director **January 2019-June 2020**
The R Street Institute, Washington, D.C.

Served as Director of National Security and Cybersecurity at a non-partisan, non-profit center-right think tank. Supervised a team of senior fellows and fellows who researched, published and engaged with policymakers and others on a wide range of national security and cybersecurity policy issues.

Legal Analyst **June 2019-May 2020**
CNN, Washington, D.C.

Provided on-air legal analysis regarding a range of topics and the news of the day.

Senior Strategic Advisor **January 2018-May 2018**
Federal Bureau of Investigation (FBI), Washington, D.C.

Served as a senior FBI leader providing executive levels of the organization with strategic management advice regarding a variety of technology and innovation projects, including cybersecurity, artificial intelligence and machine learning initiatives, digital transformation, improving the FBI's technology procurement process, and encryption.

General Counsel **January 2014-January 2018**
Federal Bureau of Investigation (FBI), Washington, D.C.

Led the FBI's legal team regarding a wide range of highly challenging national security, law enforcement, and litigation issues, including the Hillary Clinton email investigation, the investigation of Russian efforts to influence the 2016 U.S. presidential election, and high-profile encryption litigation involving Apple, Inc. Consistently provided senior FBI leaders with sound advice on risk management, crisis management, and organizational strategy. Accomplishments include:

- Successfully supervised all legal affairs of the nation's premier national security and law enforcement agency, including counterterrorism, counterintelligence, cyber, criminal, science and technology, privacy and civil liberties, government contracting, and employment law, as well as all aspects of civil litigation (including eDiscovery)
- Led FBI's Office of General Counsel, with 300 employees (including 200 attorneys)
- Program Manager for FBI's Chief Division Counsel Program through which an additional 125 attorneys provide legal advice and services to the FBI's 56 field offices
- Improved significantly the FBI's relationship with the technology sector post-Snowden disclosures
- Led the FBI's cross-functional team (legal, policy, legislative, and public affairs) responsible for supporting the Executive Branch's successful efforts to renew Section 702 of the Foreign Intelligence Surveillance Act
- Developed and implemented the first-ever comprehensive reorganization of the Office of General Counsel based on sound management principles and analysis

Associate General Counsel
Bridgewater Associates, LP, Westport, Connecticut

February 2012-January 2014

Provided legal advice on intellectual property matters to the world's largest and most successful hedge fund in a highly demanding environment. Specific accomplishments are confidential.

Associate Deputy Attorney General
United States Department of Justice
Office of the Deputy Attorney General, Washington, D.C.

July 2009-October 2011

Supervised the Department's national security portfolio on behalf of the Deputy Attorney General regarding intelligence, cyber, surveillance, rule of law, export control, and other sensitive and high-risk matters. Accomplishments include:

- Led Department's cross-functional team responsible for national security and law enforcement cyber law and policy
- Represented the Deputy Attorney General at numerous meetings of the Deputies Committee of the National Security Council (NSC) and other interagency meetings
- Supervised the Department's legal activities in Iraq and Afghanistan
- Testified before Congress on numerous occasions regarding cybersecurity, electronic surveillance and privacy, emergency preparedness, and treaty matters

Assistant General Counsel for National Security
Verizon Business, Ashburn, Virginia

April 2008-July 2009

Provided legal and policy advice on a variety of national security, law enforcement, privacy, and cybersecurity issues, as well as matters regarding the Foreign Corrupt Practices Act (FCPA). Accomplishments include:

- Developed highly effective working relationships with internal business clients that operated various sophisticated technologies, including the internet backbone, and provided cybersecurity products and services to internal and external customers
- Assisted internal clients with identifying, understanding, and mitigating legal and reputational risk consistent with business objectives

Counsel for Intelligence Policy
United States Department of Justice
National Security Division, Office of Intelligence Policy and Review, Washington, D.C.

May 2001-October 2007

Led a Department of Justice component with 125 employees (100 attorneys) and an annual budget of \$31 million. Responsible for development, coordination, and implementation of Department policy with regard to intelligence, counterintelligence, and other national security matters. Advised the Attorney General and other Department leaders on such matters. Led the organization through numerous challenges, including 9/11 and its aftermath. Accomplishments include:

- Conducted robust and effective oversight of U.S. Intelligence Community activities

- Evaluated Departmental activities and existing and proposed foreign intelligence and counterintelligence activities of the FBI, NSA, and other Intelligence Community members to determine their consistency with intelligence law and policies
- Responsible for representing the United States on all matters before the Foreign Intelligence Surveillance Act (FISA) Court, including supervising all attorneys appearing before the court and the preparation of all FISA applications
- Supervised the Office's legislative activities, including appearing before congressional committees numerous times, and its response to oversight bodies (such as Congress, the Inspector General, and the 9/11 Commission)

Deputy Counsel for Intelligence Operations **April 1998-May 2001**
 United States Department of Justice
 Office of Intelligence Policy and Review, Washington, D.C.

Led Department's legal team responsible for preparation of all FISA applications; advised Department leadership on national security and related oversight matters; conducted oversight of Intelligence Community; extensive dealings with Congress.

Attorney Advisor **October 1996-April 1998**
 United States Department of Justice
 Office of Intelligence Policy and Review, Washington, D.C.

Line attorney position representing the United States before the FISA Court on numerous counterintelligence and international terrorism matters. Conducted oversight of the FBI and other U.S. Intelligence Community members.

Trial Attorney **November 1990-October 1996**
 United States Department of Justice
 Criminal Division, Fraud Section, Washington, D.C.

Line federal prosecutor handling numerous complex international fraud cases, including Foreign Corrupt Practices Act (FCPA) violations, at grand jury, trial, and appeal stages.

Federal Judicial Law Clerk **June 1988-October 1990**
 Honorable Bernard A. Friedman
 U.S. District Court for the Eastern District of Michigan, Detroit, Michigan

AWARDS AND HONORS

- National Intelligence Meritorious Unit Citation for the Reauthorization of Section 702 of FISA (2018)
 - Justice Department's Edmund J. Randolph Award for Outstanding Service (2007) (Justice Department's highest award)
 - National Security Agency (NSA) Director's Distinguished Service Medal (2007)
 - NSA's Intelligence Under Law Award (2007)
 - U.S. Intelligence Community Award for Excellence in Counterterrorism (2006)
 - Presidential Rank Meritorious Executive Award (2003)
 - Attorney General's Honors Program (1990)
-

TEACHING AND FELLOWSHIPS

Lecturer on Law **2007-2009 and 2011-Present**
 Harvard Law School, Cambridge, Massachusetts

Visiting Fellow, Governance Program **May 2018-January 2019**
 Brookings Institution, Washington, D.C.

Distinguished Visiting Fellow **May 2018-January 2019**
 Lawfare Institute, Washington, D.C.

Fellow **January-May 2007**
 Institute of Politics, John F. Kennedy School of Government
 Harvard University, Cambridge, Massachusetts

27. As general counsel of the FBI, Baker played a central role in making the case internally for an investigation of Donald Trump

<https://www.wsj.com/articles/fbi-took-michael-sussmanns-allegation-of-trump-russia-ties-seriously-former-official-testifies-11652985514>

28. Baker wasn't the only senior FBI exec. involved in the Trump investigation to go to Twitter.

Dawn Burton, the former dep. chief of staff to FBI head James Comey, who initiated the investigation of Trump, joined Twitter in 2019 as director of strategy.

29. As of 2020, there were so many former FBI employees – "Bu alumni" – working at Twitter that they had created their own private Slack channel and a crib sheet to onboard new FBI arrivals

 **Matthew Williams** June 15, 2020 at 5:29 PM
Welcome!!
To: jbaker@twitter.com, Dawn Burton

Hey Jim!!

So excited you are here. I am no longer the newest Bu alum :)

Here is the "Bu to Twitter" translation chart I mentioned. Adding Dawn so she can add/correct.

Again, welcome! Super pumped to work with you again!

Matt

Thing	Bureau	Twitter
Climate Survey	AES	Pulse
Intranet Homepage	Red side Homepage	Birdhouse
Team/Topic Sites	FBI SharePoint Sites	Confluence
Internal Academy	Virtual Academy	go/learning
Expense Tool	TRIP	Concur
Personnel Tool	EPAS/HR Source	Workday
401k	TSP	Vanguard
Payroll	NFC	ADP
Critical Announcements	DENS	Everbridge
Short Summary	BLUF (bottom-line up front)	TL:DR (too long, didn't read)

30. Efforts continued to influence Twitter's Yoel Roth.

In Sept 2020, Roth participated in an Aspen Institute "tabletop exercise" on a potential "Hack-and-Dump" operation relating to Hunter Biden

The goal was to shape how the media covered it – and how social media carried it

CONFIDENTIAL

Aspen Digital Hack-and-Dump Working Group — September 2020

EXERCISE :: The Burisma Leak

Day One: Monday, October 5th

- Anonymous website, BIDENCRIMES.info, and a Twitter account, @HUNTERLOLZ, begin posting documents that purport to be from Burisma, tied to Hunter Biden. Splashed across the top of the site, in English, is “Joe Biden betrayed america before for \$\$\$\$. He’ll do it again.” Initially, the documents, mostly in Ukrainian, appear to be minutes of various Burisma board meetings, internal emails, and financial records. There is initially no sign of a smoking gun.
 - NOTE: The website appears to have been first registered in 2016. No ownership information is public. The Twitter account was created in 2014, oddly just before Hunter joined the Burisma board. It has tweeted once and follows one person.

Day Two: Tuesday, October 6th

- The Drudge Report links to the anonymous website, BIDENCRIMES.info, and the site is quickly picked up by other fringe media and begins to spread on social media sites.

Day Three: Wednesday, October 7th

- *Fox & Friends* discusses BIDENCRIMES.info in its 7 a.m. block. @RealDonaldTrump tweets six minutes later, “Is Joe Biden biggest criminal of all time? Check out @HUNTERLOLZ.”
- Three reporters (Dina Temple-Rason, Donje O’Sullivan, and Ellen Nakashima) are contacted by an anonymous ProtonMail account, BIDENCRIMES@protonmail.com, and each sent a different document. None of the documents have appeared on the public website. They are each told they are the only reporter receiving a specific document.
 - Dina’s document purports to be a ledger of payments showing that Hunter Biden was paid \$3 million over two months in 2015 by Burisma, far more than had been reported publicly before.
 - Donje’s document is a 2016 email, purportedly from Hunter to his father, dated the evening before the firing of prosecutor Viktor Shokin, simply titled “Burisma,” and the body of which reads: “I really need you to do this for me.”
 - Ellen’s document purports to be the board contract between Burisma and Hunter.
- In Ukraine, Burisma announces that it has no evidence of any hack of its servers, disavows all files as forgeries.

Day Four: Thursday, October 8th

- The Biden campaign, adopting the policy of Hillary Clinton's campaign in 2016 and the Macron campaign, says they will not confirm the veracity of any documents.
- CrowdStrike announces, without further detail, it has reason to believe that BIDENCRIMES.info is the work of Fancy Bear (APT 28).
- CNN's Jim Scuitto reports an anonymous Cloudflare executive who says that he doubts the CrowdStrike appraisal; Cloudflare believes that no foreign actor is involved and has evidence that BIDENLEAKS.info is being hosted and run by Americans.
- At 4 p.m., the *Washington Post* publishes a story by Ellen Nakashima confirming that the Burisma board contract given to her is legitimate; there is no wrongdoing evident or alleged in the document, but Burisma sources confirm the document is real.
- Cesar Conde, the chairman of NBC News, announces that because of the suspicion that the BIDENCRIMES.info leaks are coming from a foreign power with a goal of undermining America's free and fair elections, no aspect of NBC News or MSNBC will report on the allegations or use the materials as the basis for reporting. In his statement, carried live on the evening news with Lester Holt, he asks all other news organizations to follow NBC's leadership. The Guardian quickly announces it will follow the same principle, as does The Huffington Post.
- At Ohio Trump rally that night, crowd starts chanting "LOCK HIM UP." President Trump, at podium, pumps his fists as the crowd chants.

Day Five: Friday, October 9th

- In a statement released at 9 a.m. and signed only by him, Director of National Intelligence John Ratcliffe says he has no reason to believe the documents posted by BIDENCRIMES.info are forgeries, nor does the IC have reason to believe the website is a Russian operation.
- At 11 a.m., on the House floor, House Intelligence Chair Adam Schiff says that according to his briefings, the IC is not being forthright with the American people about the source and veracity of the leaks.
- Also at 11 a.m., Mandiant releases a short statement saying it has traced the source of BIDENLEAKS.info to infrastructure consistent with China's Ministry of State Security.

- At 2 p.m., @HUNTERLOLZ tweets a link out to a .zip file that appears to contain a new tranche of 20,000 documents, mostly in Ukrainian, stolen from Burisma and posted on BIDENCRIMES.info.
- All but simultaneously, at 2:01 p.m., @DonaldJTrumpJr, @TeamTrump, and @parscale all retweet the @HUNTERLOLZ post.
- By 3 p.m., Twitter determines that the hosting service for the .zip tweeted by @HUNTERLOLZ traces back to a server in Hong Kong.
- That afternoon, Facebook's sources inside the IC tell Facebook to be wary about the DNI's statement.
- At 5 p.m., Dina Temple-Raston airs an NPR story saying that she has confirmed the \$3 million payment document she received is fake.

Day Six: Saturday, October 10th

- Overnight, progressive blogger Josh Marshall notices and tweets out one document in the new tranche of .zip files that appears to be a confirmation of a wire transfer for \$1 million from Deutsche Bank to an off-shore account in the name of Hunter Biden, dated two days after the firing of the chief prosecutor, Shokin. Overnight, independent security researchers and news organizations find the majority of the .zip files are authentic, but some are manipulated. First Draft News tweets an hour after Josh's tweet that his document appears to be an authentic Burisma document but has been edited—what was edited is unclear.
- At 10 a.m., the *New York Times* posts a story saying that two anonymous "senior Justice Department officials" in Washington say that the acting U.S. attorney in D.C. has empaneled a grand jury to investigate Joe Biden.

Day Seven: Sunday, October 11th

- On the Sunday shows, Biden campaign staff dismiss the entire hack-and-leak as dirty tricks by Vladimir Putin.
- After the morning shows air, *The Daily Beast* quotes two "former senior intelligence officials" that the directors of the CIA and NSA refused to sign onto Ratcliffe's Friday statement, although sources differ why they did not sign it. David Sanger matches that reporting an hour later.
- Alex Berenson announces on Twitter that he's conducted an interview, via DM, with the person behind @HUNTERLOLZ and that he believes the person is an American.

Day Eight: Monday, October 12th

- At 7:15 a.m., President Trump calls into *Fox & Friends* and says he hopes the FBI will investigate Joe Biden.
- At 9 a.m., Attorney General Bill Barr holds a press conference to say the American people deserve the truth and that he has instructed the FBI to verify the allegations of Joe Biden and Hunter Biden's corruption. He announces that the Justice Department is investigating wrongdoing by Hunter Biden and Joe Biden for money laundering, tax fraud, theft of honest services, and acting as an unregistered foreign agent. In response to a reporter's question, he volunteers that he believes Joe Biden should submit to an FBI interview within days.
- At 11 a.m., Senator Richard Blumenthal says the American people are being lied to and demands in a CNN interview, "Paul Nakasone, Gina Haspel, and Chris Wray owe Americans the truth. I can't say more than that."
- At 2 p.m., Jim Comey tweets "FBI agents tell me they are being silenced about the truth. Donald Trump is illegally coordinating with Putin. He must resign."
- At 7:30 p.m., Rudy Giuliani says on Fox News that he was right all along re: 2019 Ukraine pressure campaign.

Day Nine: Tuesday, October 13th

- @realDonaldTrump tweets at 6:15 a.m.: "See, Ukraine phone call was perfect — I knew Sleepy Joe was actually Crooked Joe! Tell FBI: LOCK HIM UP!"

Day Ten: Wednesday, October 14th

- Rep. Devin Nunes, Sen. Tom Cotton, and Secretary of State Mike Pompeo announce they will travel immediately to Kiev to get Burisma's cooperation with the unfolding investigation. They depart that night on an official US government jet.

Day Eleven: Thursday, October 15th

- The second presidential debate

Bidencrimes.info 17 letters,

31. The organizer was Vivian Schiller, the fmr CEO of NPR, fmr head of news at Twitter; fmr Gen. mgr of NY Times; fmr Chief Digital Officer of NBC News

Attendees included Meta/FB's head of security policy and the top nat. sec. reporters for [@nytimes](#) [@wapo](#) and others



Garrett Graff

October 17, 2020 at 4:44 AM

Stephen was right!

To: Janine Zacharia, Vivian Schiller, Nathaniel Gleicher, Yoel Roth, Olga Belogolova, claire@firstdraftnews.com, david.e.sanger@gmail.com, Nakashima, Ellen, Davis, Rick, Andrew James Grotto, David McCraw, Noah Shachtman

[Hide](#)

32. By mid-Sept, 2020, Chan & Roth had set up an encrypted messaging network so employees from FBI & Twitter could communicate.

They also agree to create a “virtual war room” for “all the [Internet] industry plus FBI and ODNI” [Office of the Director of National Intelligence].

From: Yoel Roth <yoel@twitter.com>
Sent: Monday, September 21, 2020 04:32 PM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]
Cc: Yoel Roth <yoel@twitter.com> [REDACTED]
Subject: [SOCIAL NETWORK] Re: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Re: Election Communication Platform

Hey Elvis,

Apologies for the delayed responses. Notes on your 3 questions are below - happy to find time this week, or we can check in briefly on Friday's call.

1. What USG agencies will be allowed on the channel? I think the easy ones will be FBI, DHS/CISA, and ODNI. For your awareness, State/GEC, NSA, and CIA have expressed interest in being allowed on in listen mode only. Welcome your thoughts on this.

The agreed-upon parameters for the channel (by industry) are that it's one-way communication **from** government **to** industry. We explicitly do not plan to have conversation/discussion/responses back in this forum. So the USG attendees there I think would largely be driven by who FBI wants to share information with in this setting. I will note, given at least some of the orgs on this list (e.g. State/GEC) have been somewhat more press-happy than others, I worry a bit about whether information shared in confidence with industry could result in announcements being made which disrupt our operational work. Put another way, there might be value in keeping the circle of trust here quite small. I also worry about the precedent of expanding it to include organizations which aren't typically present in our meetings. I'm also not entirely sure that every member of that group wants their phone number *quite so broadly available*. And, finally, I'd need to run this by the industry group again - they only agreed to FBI. Happy to do so if you think there's value, but I'm thinking it might be simpler to keep it to industry/FBI.

2. How many USG participants will be allowed onto the channel? Will it only be people that industry already knows? I ask because at the FBI SF command center, there will be three other supervisors working shifts when I'm not there. I also know different FITF personnel will be rotating through the command post at FBIHQ.

We didn't get into the specifics of this, but I can't imagine any of that would be problematic.

3. When will the channel be activated and for how long?

We discussed the election period, broadly defined. Probably not indefinitely, but keeping it going at minimum through January seems reasonable.

 Chan, Elvis M. (SF) (FBI)  Roth Large September 21, 2020 at 8:48 PM
Re: [SOCIAL NETWORK] Re: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Re: Election Communication Platform [Details](#)
To: Yoel Roth, Cc: [REDACTED]

Hi Yoel,

Thanks for the response. I have some additional questions regarding them. I am aware the industry is meeting about this on Friday so you may not have any clarification until then. We can discuss during and after our scheduled meeting depending on what your schedule looks like.

1. If it will only be one-way communication from the USG to the industry, it seems like it should at least be FBI and CISA. We can give you everything we're seeing from the FBI andUSIC agencies. CISA will know what is going on in each state via the Homeland Security Information Network (HSIN).

However, how will the industry partners communicate back with the FBI and CISA? For the FBI, will you use the pre-established channels already in use? For example, you or Angela will email me directly.

If that is the case, that will work for the FBI, but I don't know what communication channels you have with CISA. Or will the industry partners rely on the FBI to be the belly button for the USG? We can do that as well. We just need to know the industry group's preference.



2. Sounds good. We will likely only establish one Signal channel for FBI San Francisco and one for FBIHQ. The FITF unit chiefs may want to be on the channel as well. I will provide the companies with our command post shift roster so you know who is on shift for any given day.

3. Facebook had mentioned activating the Signal channel before the first presidential debate, which works for us, but we won't have the enhanced staffing levels until October 28th at FBIHQ and October 30th at FBI San Francisco. I don't think we will stay in enhanced posture through January so I think we would revert back to the standard channels sometime in November, perhaps after the elections are certified.


Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1
San Francisco Division
Federal Bureau of Investigation
[REDACTED]

33. Then, on Sept 15, 2020 the FBI's Laura Dehmlow, who heads up the Foreign Influence Task Force, and Elvis Chan, request to give a classified briefing for Jim Baker, without any other Twitter staff, such as Yoel Roth, present.

 Jim Baker FBI Emails September 15, 2020 at 6:13 PM
Re: [SOCIAL NETWORK] Re: [SOCIAL NETWORK] Re: [EXTERNAL EMAIL] - [SOCIAL N...
To: Dehmlow, Laura E. (CD) (FBI), Jim Baker,  [Details](#)

Hi Jim and 

I hope all is well. , can you help Laura Dehmlow and Elvis Chan of the FBI schedule a classified briefing for Jim? They would like to meet early next week if possible.

Thank you!

34. On Oct 14, shortly after @NYPost publishes its Hunter Biden laptop story, Roth says, "it isn't clearly violative of our Hacked Materials Policy, nor is it clearly in violation of anything else," but adds, "this feels a lot like a somewhat subtle leak operation."

 Yoel Roth October 14, 2020 at 8:51 AM
Re: [for your awareness] New York Post Article / Action from FB [Details](#)
To:  & 6 more

Hey 

Thanks - we're aware of this and are tracking closely. At this time, given the alleged provenance of the materials (a laptop mysteriously dropped off at repair shop in Delaware), it isn't clearly violative of our Hacked Materials Policy, nor is it clearly in violation of anything else. That said, the questionable origins here are obviously causing a lot of people to make references to 2016 - and my personal view on this, unsubstantiated by hard evidence as yet, is that this feels a lot like a somewhat subtle leak operation. We'll be developing a recommendation for what, if anything, we want to do over the course of the day today.

Yoel

Jim Baker, [REDACTED], and 1 other added comments to the following document

2020-10-14 NYPost Hunter Biden Laptop Article - PRIVILEGED AND...

New
2 comments

Comments

our teams continue to investigate the origins of the material included in the reporting.



[REDACTED]

I'm struggling to understand the policy basis for marking this as unsafe, and I think the best explainability argument for this externally would be that we're waiting to understand if this story is the result of hacked materials. We'll face hard questions on this if we don't have some kind of solid reasoning for marking the link unsafe.



Trenton Kennedy

cc: @yoel@twitter.com @sommerse@twitter.com
@j...@twitter.com @...@twitter.com



[REDACTED]

Will we also mark similar stories as unsafe?

<https://www.foxnews.com/politics/hunter-biden-emails-senate-homeland-security-committee-investigating-hard-drive-laptop>



Yoel Roth

The policy basis is hacked materials - though, as discussed, this is an emerging situation where the facts remain unclear. Given the SEVERE risks here and lessons of 2016, we're erring on the side of including a warning and preventing this content from being amplified.



Vijaya Gadde

What is the warning that will come up?



Yoel Roth

When you click the link, you'll see the generic unsafe URL message (references spam, malware, and violations of the Twitter Rules) - not ideal, but it's the only thing we have



[REDACTED]

Whatever we do in the comms (this will become a bias claim for Jack pre-hearing immediately), let's make it clear we're proactively but cautiously interpreting this through the lens of our hacked materials policy and allowing the link with a warning and significant reduction of spread.



[REDACTED]

To Ian's point, can we truthfully claim that this is part of the policy? i.e. As part of our approach to addressing potentially hacked materials, we are limiting visibility of related stories on Twitter while our investigation is ongoing.



Jim Baker New

[PRIVILEGED AND CONFIDENTIAL]

I support the conclusion that we need more facts to assess whether the materials were hacked. At this stage, however, it is reasonable for us to assume that they may have been and that caution is warranted. There are some facts that indicate that the materials may have been hacked, while there are others indicating that the computer was either abandoned and/or the owner consented to allow the repair shop to access it for at least some purposes. We simply need more information.

Reply

Open

37. As for the FBI, it likely would have taken a few *hours* for it to confirm that the laptop had belonged to Hunter Biden. Indeed, it only took a few days for journalist [@peterschweizer](https://twitter.com/peterschweizer) to prove it.
<https://twitter.com/i/status/1604903049339604994>

38. By 10 am, Twitter execs had bought into a wild hack-and-dump story

“The suggestion from experts - which rings true - is there was a hack that happened separately, and they loaded the hacked materials on the laptop that magically appeared at a repair shop in Delaware”



Yoel Roth

October 14, 2020 at 10:12 AM

Re: [for your awareness] New York Post Article / Action from FB

To: [REDACTED], SCALE Legal Cc: & 15 more

[Details](#)

[REDACTED] [+SCALE Legal](#) as well

Hi folks,

Lots of good discussion of this case in the doc. Sharing a bit of additional context about why we're recommending this action:

The key factor informing our approach is consensus from experts monitoring election security and disinformation that this looks a lot like a hack-and-leak that learned from the 2016 Wikileaks approach and our policy changes. The suggestion from experts - which rings true - is there was a hack that happened separately, and they loaded the hacked materials on the laptop that magically appeared at a repair shop in Delaware (and was *coincidentally* reviewed in a very invasive way by someone who *coincidentally* then handed the materials to Rudy Giuliani). Given the severe risks we saw in this space in 2016, we're recommending a warning + deamplification pending further information.

If additional information emerges that establishes the origins of the materials more conclusively, we could either reverse this action and remove the warning, or escalate our enforcement (should it cross the line fully into hacked materials).

We recognize that the product experience of the warning label is less than ideal, and will surface that feedback with the Experience team again as evidence for why we need more robust URL management options.

Based on a discussion with Vijaya, we'll move forward with this action once we get signoff from comms.

Yoel

38. By 10 am, Twitter execs had bought into a wild hack-and-dump story

“The suggestion from experts - which rings true - is there was a hack that happened separately, and they loaded the hacked materials on the laptop that magically appeared at a repair shop in Delaware”



Perry, Matthew J. (OGC) (FBI)

📁 Jim...BI Emails

October 14, 2020 at 3:38 PM

Jim/Matt

To: Jim Baker



Mail
Attachment.ics

1 KB

40. The influence operation persuaded Twitter execs that the Hunter Biden laptop did *not* come from a whistleblower.

One linked to a Hill article, based on a WaPo article, from Oct 15, which falsely suggested that Giuliani's leak of the laptop had something to do with Russia.

From: Nick Pickles <npickles@twitter.com>
Subject: Re: PRIVILEGED - Hacked Materials updates source-of-truth
Date: October 16, 2020 at 10:26 AM
To: [REDACTED]
Cc: [REDACTED]



The current policy is anchored in "attempts to compromise or infiltrate computer systems for malicious purposes" - we'd have to be feeling pretty vindictive to say whistleblowers or dissidents were malicious.

Plus isn't the issue with whistleblowers data theft rather than hacking (hence Snowden was charged under the Espionage Act vs Assange charged under Computer Fraud and Abuse Act?).

This does point to the question of whether we should have a factor in the policy relating to proximity and relevance to critical civic events informing our enforcement, which would protect something of dubious provenance but with public interest (eg [Fintel files](#)).

(I'd also note the seemingly well-timed [briefings from Govt](#) sources highlighting concerns about the source of the hard drive, which would support an assessment that it's neither whistleblower or dissident content.)

Thanks
Nick

On Fri, 16 Oct 2020 at 11:02, [REDACTED] wrote:

I think this is intended to not only protect media reporting but whistleblowers and dissidents so as not to silence those voices ...

On Fri, Oct 16, 2020 at 12:38 PM Nick Pickles <npickles@twitter.com> wrote:

Adding [REDACTED]

At a high level, I'm still struggling to understand how we've gone from a narrow issue about how to scope the policy around media reporting, to a far broader roll back of our approach to hacked materials. Labelling something that looks and smells like a hostile attempt to interfere in an election feels like we're dodging a pretty fundamental question about how we protect the public conversation, for the sake of appeasing a vocal political group who at this point seem willing to accept the fruits of foreign interference to help their own political fortunes.

Flagging this piece in [Just Security](#) this morning, "Of the available options, the platforms

Just In...

White House says it is preparing for a possible second round of coronavirus fight

Lawmaker says it is possible to hold a public hearing

The reality of oxygen shortage in 2021

Market predicted that 7.5% could be lost in 2021

'Virtually' video game

NATIONAL SECURITY

Intelligence officials warned Trump that Giuliani was target of Russian influence campaign: report

RUSSIAN CAMPAIGN TO INFLUENCE (7)



The Washington Post
Democracy Dies in Darkness

White House was warned Giuliani was target of Russian intelligence operation to feed misinformation to Trump

By Shane Harris, Ellen Nakashima, Greg Miller and Josh Dawsey
October 15, 2020 at 7:15 p.m. EDT



Former New York mayor Rudolph W. Giuliani pauses while addressing Trump supporters on Oct. 12, 2020, during a Columbus Day gathering at a Trump-campaign field office in Philadelphia. (Jacqueline Lanza/AP)

Comment 3822 Save Gift Article Share

U.S. intelligence agencies warned the White House last year that President Trump's personal lawyer Rudolph W. Giuliani was the target of an influence operation by Russian intelligence, according to four former officials familiar with the matter.



41. There is evidence that FBI agents have warned elected officials of foreign influence with the primary goal of leaking the information to the news media. This is a political dirty trick used to create the perception of impropriety.

42. In 2020, the FBI gave a briefing to Senator Grassley and Johnson, claiming evidence of "Russian interference" into their investigation of Hunter Biden.

The briefing angered the Senators, who say it was done to discredit their investigation.

https://www.grassley.senate.gov/imo/media/doc/grassley_johnson_to_fbi_-_august_2020_briefing.pdf

43. "The unnecessary FBI briefing provided the Democrats and liberal media the vehicle to spread their false narrative that our work advanced Russian disinformation."

United States Senate

WASHINGTON, DC 20510

August 25, 2022

VIA ELECTRONIC TRANSMISSION

Ms. Nikki Floris
Intelligence Analyst in Charge
Intelligence Division, Washington Field Office
Federal Bureau of Investigation

Mr. Bradley Benavides
Deputy Assistant Director
Counterintelligence Division
Federal Bureau of Investigation

Dear Ms. Floris and Mr. Benavides:

On August 6, 2020, as we were finishing our September 23, 2020, report on Hunter Biden's financial connections to foreign governments and questionable foreign nationals, you provided a briefing to us on behalf of the FBI and Intelligence Community.¹ As we have publicly and privately stated to you and Director Wray since that briefing, the briefing was unnecessary and was only done because of pressure from our Democratic colleagues, including Democratic Leadership, to falsely attack our Biden investigation as advancing Russian disinformation.²

¹ Chairman Charles Grassley, S. Comm. on Fin., and Chairman Ron Johnson, S. Comm. on Homeland Sec. and Governmental Aff. *Hunter Biden, Burisma, and Corruption: The Impact on U.S. Government Policy and Related Concerns*, (Sept. 23, 2020) <https://www.finance.senate.gov/imo/media/doc/HSGAC%20-%20Finance%20Joint%20Report%202020.09.23.pdf>.

² Letter from Chairman Charles Grassley, S. Comm. on Fin., and Chairman Ron Johnson, S. Comm. on Homeland Sec. and Governmental Aff., to Ranking Member Ron Wyden, S. Comm. on Fin., and Ranking Member Gary Peters, S. Comm. on Homeland Sec. and Governmental Aff. (July 28, 2020); Press Release, Sen. Charles E. Grassley, Sen. Ron Johnson, Denounce Democrat Disinformation Campaign In Response To Peters, Wyden, Democrat Leaders' Letters (July 28, 2020), <https://www.grassley.senate.gov/news/news-releases/johnson-grassley-denounce-democrat-disinformation-campaign-response-peters-wyden>; Press Release, Sen. Charles E. Grassley, Grassley (Again) Rejects Democrats' Baseless Claims About Burisma Probe (Sept. 16, 2020), <https://www.grassley.senate.gov/news/news-releases/grassley-again-rejects-democrats-baseless-claims-about-burisma-probe>; Floor Speech, Sen. Charles E. Grassley, Grassley On The Ukraine Investigation (Sept. 29, 2020), <https://www.grassley.senate.gov/news/news-releases/grassley-ukraine-investigation>; Floor Speech, Sen. Charles E. Grassley, Grassley On Democrats Spreading Disinformation To Protect President Biden (Mar. 18, 2021), <https://www.grassley.senate.gov/news/news-releases/grassley-on-democrats-spreading-disinformation-to-protect-president-biden>; Floor Speech, Sen. Charles E. Grassley, The Media Again Takes Liberal Disinformation Bait On Biden Family Oversight (May 11, 2021), <https://www.grassley.senate.gov/news/remarks/the-media-again-takes-liberal-disinformation-bait-on-biden-family-oversight>; Letter from Sen. Charles E. Grassley, and Sen. Ron Johnson to Inspector General Horowitz (July 20, 2021), https://www.grassley.senate.gov/imo/media/doc/grassley_johnson_to_justice_dept_inspectorgeneralaugust2020briefing.pdf.

For example, on July 13, 2020, then-Minority Leader Schumer, Senator Warner, Speaker Pelosi and Representative Schiff sent a letter, with a classified attachment, to the FBI to express a purported belief that Congress was the subject of a foreign disinformation campaign.³ The classified attachment included unclassified elements that, among other things, attempted – and failed – to tie our investigation into the Biden family’s financial deals to foreign disinformation. Those elements were then leaked to the press.⁴ As you are undoubtedly aware, we’ve successfully refuted those false allegations and, most recently, we’ve made public a series of authentic bank records relating to the Biden family’s connections to the communist Chinese government, which Democrats had previously tried – and failed – to claim advanced Russian disinformation.⁵

In addition, on July 16, 2020, then-Ranking Member Peters and then-Ranking Member Wyden wrote to us requesting a briefing from the FBI’s Foreign Influence Task Force on matters purportedly relating to our investigation.⁶ On July 28, 2020, we responded to them and reminded them that in March 2020, the FBI and relevant members of the Intelligence Community had already briefed our committees and provided assurances that there was no reason that our committees should not continue their investigation.⁷ Nonetheless, the FBI succumbed to the Democratic pressure and provided the infamous August 6, 2020, briefing.

With respect to the substance of the briefing, it consisted primarily of information that we already knew and information unconnected to our Biden investigation. We made clear to you at the briefing that it was not relevant to the substance of our work. In response, you stated that the FBI is not attempting to “quash, curtail, or interfere” in the investigation in any

³ Letter from Minority Leader Charles Schumer, Vice Chairman Mark Warner, S. Select Comm. on Intelligence, Speaker Nancy Pelosi, and Chairman Adam Schiff, H. Select Comm. on Intelligence, to Fed. Bureau of Investigation (July 13, 2020), https://intelligence.house.gov/uploadedfiles/20200713_big_4_letter_to_fbi_director_wray_-_defensive_briefing_signed.pdf.

⁴ Natasha Bertrand, Andrew Desiderio, and Kyle Cheney, *Democrats: Packets sent to Trump allies are Part of Foreign Plot to Damage Biden*, POLITICO (July 23, 2020), [foreign-plot-to-damage-biden-380217](https://www.politico.com/news/2020/07/23/democrats-packets-sent-to-trump-allies-are-part-of-foreign-plot-to-damage-biden-380217); As the Ranking Members have repeatedly said, they and their staff have not received, relied upon, or solicited information from Derkach.

⁵ Floor Speech, Sen. Charles E. Grassley, Sen Ron Johnson Discuss Investigation into Biden Family Foreign Financial Entanglements - Part I (Mar. 28, 2022) <https://www.grassley.senate.gov/news/remarks/grassley-johnson-discuss-investigation-into-biden-family-foreign-financial-entanglements-part-i>; see also Floor Speech, Sen. Charles E. Grassley, Sen Ron Johnson Release Bank Records Tying Biden Family to CCP-Linked Individuals & Companies (Mar. 29, 2022), <https://www.grassley.senate.gov/news/remarks/grassley-johnson-release-bank-records-tying-biden-family-to-ccp-linked-individuals-and-companies>; Floor Speech, Sen. Charles E. Grassley, Sen. Ron Johnson, The Biden Family Investigation – Part III: James Biden (Apr. 5, 2022) <https://www.grassley.senate.gov/news/remarks/the-biden-family-investigation-part-iii-james-biden>.

⁶ Letter from Ranking Member Ron Wyden, S. Comm. on Fin., and Ranking Member Gary Peters, S. Comm. on Homeland Sec. and Governmental Aff., to Chairman Grassley, S. Comm. on Fin., and Chairman Ron Johnson, S. Comm. on Homeland Sec. and Governmental Aff. (July 16, 2020),

https://www.hsgac.senate.gov/imo/media/doc/200716_Letter_PetersWyden_IntelligenceBriefingRequest.pdf.

⁷ Letter from Chairman Charles Grassley, S. Comm. on Fin., and Chairman Ron Johnson, S. Comm. on Homeland Sec. and Governmental Aff., to Ranking Member Ron Wyden, S. Comm. on Fin., and Ranking Member Gary Peters, S. Comm. on Homeland Sec. and Governmental Aff. (July 28, 2020).

way.⁸ We also made clear our concern that the briefing would be subject to a leak that would shed a false light on the focus of our investigation. Indeed, on May 1, 2021, the Washington Post did exactly that and so did the other inaccurate media articles during the course of our investigation which falsely labeled our investigation as advancing Russian disinformation.⁹ Moreover, whistleblowers have recently alleged that in August 2020, the same month you provided the briefing to us, FBI officials initiated a scheme to downplay derogatory information on Hunter Biden for the purpose of shutting down investigative activity relating to his potential criminal exposure by labeling it “disinformation.”¹⁰ Whistleblowers have also alleged that local FBI leadership instructed employees not to look at the Hunter Biden laptop immediately after the FBI had obtained it.¹¹

At the briefing as well as after, we requested relevant records relating to what happened at the briefing, including the 302 or similar summary, the intelligence basis for the briefing and the personnel involved in making the decision to brief us. On August 12, 2020; May 3, 2021; July 25, 2022; and August 11, 2022, those requests were made.¹² The FBI has consistently failed to respond in full to each request and failed to provide those critical records which casts further doubt on the true purpose for the briefing.

Simply put, the unnecessary FBI briefing provided the Democrats and liberal media the vehicle to spread their false narrative that our work advanced Russian disinformation. Although you stated that the FBI didn’t intend to “interfere” in our investigation, the practical effect of such an unnecessary briefing and the subsequent leaks relating to it created interference, which frustrated and obstructed congressional oversight efforts.

⁸ S. Rep., Hunter Biden, Burisma, and Corruption: The Impact on U.S. Government Policy and Related Concerns, S. Comm. on Homeland Sec. and Governmental Aff. and S. Comm. on Fin., 116TH CONG. (2020) at 59, https://www.hsgac.senate.gov/imo/media/doc/HSGAC_Finance_Report_FINAL.pdf.

⁹ Ellen Nakashima, Shane Harris and Tom Hamburger, *FBI was aware of prominent Americans, including Giuliani, were targeted by Russian influence operation*, The Washington Post (May 1, 2021).

https://www.washingtonpost.com/national-security/rudy-giuliani-fbi-warning-russia/2021/04/29/5db90f96-a84e-11eb-bca5-048b2759a489_story.html; See Natasha Bertrand, Kyle Cheney, and Andrew Desiderio, *Dem leaders demand FBI briefing on 'foreign interference campaign' targeting lawmakers*, POLITICO (July 20, 2020), <https://www.politico.com/news/2020/07/20/democrats-fbi-briefing-foreign-interference-campaign-373134>.

¹⁰ Press Release, Sen. Charles E. Grassley, *Whistleblowers' Reports Reveal Double Standard In Pursuit of Politically Charged Investigations By Senior FBI, DOJ Officials* (July 25, 2022), <https://www.grassley.senate.gov/news/news-releases/whistleblowers-reports-reveal-double-standard-in-pursuit-of-politically-charged-investigations-by-senior-fbi-doj-officials>.

¹¹ Letter from Sen. Ron Johnson, to Justice Department Inspector General Michael Horowitz (Aug. 23, 2022) <https://www.ronjohnson.senate.gov/services/files/7CD44E16-BF0B-495E-8B87-900467F69E50>.

¹² Letter from Chairman Charles Grassley, S. Comm. on Fin., to Attorney General Garland and Director Wray (Aug. 12, 2020) https://www.grassley.senate.gov/imo/media/doc/grassley_to_justice_deptfbibriefing.pdf; Letter from Chairman Charles Grassley, S. Comm. on Fin., and Chairman Ron Johnson, S. Comm. on Homeland Sec. and Governmental Aff., to Director Wray and Director Avril Haines (May 3, 2021) https://www.grassley.senate.gov/imo/media/doc/grassley_johnson_to_fbi_odni_-_briefing.pdf; Letter from Ranking Member Charles Grassley to Attorney General Garland and Director Wray (July 25, 2022) https://www.grassley.senate.gov/imo/media/doc/grassley_to_justice_deptfbipoliticalbiasfollowup.pdf; Ranking Member Charles Grassley, *Questions for the Record - FBI Oversight Hearing* (Aug. 11, 2022) https://www.grassley.senate.gov/imo/media/doc/fbi_oversight_hearing_questions_for_the_record_-_senator_grassley.pdf.

The FBI answers to Congress and the American people; therefore, we request that you appear before us for a transcribed interview on these and related matters no later than September 8, 2022. In addition, at the time of our initial request in August 2020, all records relating to the briefing should have been preserved.¹³ This letter reiterates that request.

Sincerely,



Charles E. Grassley
Ranking Member
Committee on the Judiciary



Ron Johnson
Ranking Member
Permanent Subcommittee
on Investigations

cc: The Honorable Richard Durbin
Chairman
Committee on the Judiciary

The Honorable Jon Ossoff
Chairman
Permanent Subcommittee on Investigations

The Honorable Michael Horowitz
Inspector General
Department of Justice

44. Notably, then-FBI General Counsel Jim Baker was investigated *twice,* in 2017 and 2019, for leaking information to the news media.

“You’re saying he’s under criminal investigation? That’s why you’re not letting him answer?” Meadows asked.

“Yes”

<https://www.politico.com/story/2019/01/15/fbi-general-counsel-criminal-investigation-1101774>

45. In the end, the FBI's influence campaign aimed at executives at news media, Twitter, & other social media companies worked: they censored & discredited the Hunter Biden laptop story.

By Dec. 2020, Baker and his colleagues even sent a note of thanks to the FBI for its work.



46. The FBI's influence campaign may have been helped by the fact that it was paying Twitter millions of dollars for its staff time.

“I am happy to report we have collected \$3,415,323 since October 2019!” reports an associate of Jim Baker in early 2021.

Run the business - we made money!

[Details](#)

To: Jim Baker, Cc: Sean Edgett

Jim, FYI, in 2019 SCALE instituted a reimbursement program for our legal process response from the FBI. Prior to the start of the program, Twitter chose not to collect under this statutory right of reimbursement for the time spent processing requests from the FBI.

I am happy to report we have collected \$3,415,323 since October 2019! This money is used by LP for things like the TTR and other LE-related projects (LE training, tooling, etc.).

--



Safety, Content, & Law Enforcement (SCALE)

47. And the pressure from the FBI on social media platforms continues

In Aug 2022, Twitter execs prepared for a meeting with the FBI, whose goal was "to convince us to produce on more FBI EDRs"

EDRs are an "emergency disclosure request," a warrantless search.

From: [REDACTED]
Subject: Advance read-out on 9/6 meeting with FBI
Date: August 25, 2022 at 1:58 PM
To: [REDACTED]

AL

Team:

I had an advanced prep call today with [REDACTED] of the FBI for your 9/6 meeting with them. Here are some key takeaways:

- Attending on the FBI side will be [REDACTED], plus people from NTOC and perhaps others from violent crimes at HQ.
- Their goal in the meeting is to convince us to produce on more FBI EDRs.
- They will try and do this by having NTOC educate us on the threats they are seeing, their procedures and processes for responding to tips, and what their standards are for when they seek EDRs.
- They plan on bringing statistics on our rate of compliance, which they labeled variable, and several "forehead knockers" (i.e. situations where in the FBI view there is no reason why we would not have complied).
- They repeatedly emphasized Twitter's lower level of compliance in comparison with other platforms. I, kindly, emphasized back that repeatedly stressing that to our team is not going to be a good strategy to move the needle in their direction.

These bullets make it seem like this will be a confrontational meeting, which I do not think it will be. Instead, I get the feeling they are genuinely baffled and frustrated that their "rate of success" (as they say) is so low at Twitter.

On our side, I think it could be helpful to have some statistics at our fingertips about how the FBI has far and away a greater rate of production than anyone else (I assume this is true). It might also be helpful to get a sense of the reasons we are denying their requests. Matt suggested that it was our high requirement of imminence (which is the narrative I expect his team will push), so it would be interesting to see if that's actually the issue, or if it's something else.

I realize no one has time to do anything extra, so these are just nice to haves, not must haves. You all are perfectly fine to just go into the meeting and listen and say thanks so much for your input and leave. But if you have interest in countering their version of the facts, it would probably be helpful to do a little digging on our side.

Thanks so much,

[REDACTED]

In response to the Twitter Files revelation of high-level FBI agents at Twitter, [@Jim_Jordan](#) said, "I have concerns about whether the government was running a misinformation operation on We the People."

<https://nypost.com/2022/12/17/twitter-leadership-full-of-former-fbi-agents-linkedin-records-show/>

Anyone who reads the Twitter Files, regardless of their political orientation, should share those concerns.

/END