



**ELECTION INTERFERENCE: HOW THE FBI “PREBUNKED” A TRUE STORY
ABOUT THE BIDEN FAMILY’S CORRUPTION IN ADVANCE OF THE 2020
PRESIDENTIAL ELECTION**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives



October 30, 2024

EXECUTIVE SUMMARY

“But, when we get hauled up to [Capitol] hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG [U.S. Government] to plan for it.”

—July 15, 2020, 3:17 p.m. ET, internal Facebook message during Facebook’s meeting with the FBI and other agencies.¹

At 5:00 a.m. ET, on Wednesday, October 14, 2020, less than three weeks before the 2020 presidential election, the *New York Post* published a potentially election-altering news story about a years-long influence peddling scheme carried out by the family of the Democratic nominee for president, former Vice President Joe Biden.² The *Post* article detailed how Hunter Biden leveraged his famous last name to provide foreign officials with access to his father in exchange for the Biden family’s significant financial gain.³ This information was recovered from the hard drive of a laptop attributed to Hunter Biden, and the article included pictures of a signed federal subpoena, demonstrating that the Federal Bureau of Investigation (FBI) had seized that hard drive.⁴ Neither Hunter Biden nor the Biden presidential campaign denied the allegations or the provenance of the laptop; indeed, the Biden Department of Justice (DOJ) has since authenticated the laptop as evidence in federal court.⁵

Soon after the *Post* article was published, however, something strange happened. Almost immediately, major social media platforms, including Twitter and Facebook—the modern-day digital town square—censored the true story about Biden family influence peddling. As a consequence, millions of Americans cast their presidential vote unaware of serious, credible allegations of misconduct levied against one of the two candidates. This censorship served to benefit one candidate over the other and wrongfully affected the 2020 election.⁶ Today, these companies and their executives belatedly admit that their censorship was wrong.⁷

Why were the social media companies so ready to censor a true story about Hunter Biden featured in a prominent American newspaper? Because the FBI had primed them for it. For nearly a year, the FBI had been conditioning social media companies to expect a “hack-and-leak” operation from Russia involving Hunter Biden. In more than thirty meetings across eight

¹ Internal messages among Facebook personnel (July 15, 2020, 3:17 p.m.), *see Ex. 10*.

² *See Emma-Jo Morris & Gabrielle Fonrouge, Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. POST (Oct. 14, 2020).

³ *Id.*

⁴ *Id.*

⁵ James Lynch, *Prosecution Introduces Hunter Biden’s Infamous Laptop at Trial, Uses Data as Evidence of Crack Addiction*, NAT. REVIEW (June 4, 2024).

⁶ *See, e.g., Rich Noyes, SPECIAL REPORT: The Stealing of the Presidency, 2020*, MEDIA RSCH. CTR. (Nov. 24, 2020) (“Even more Biden voters (45.1%) said they were unaware of the financial scandal enveloping Biden and his son, Hunter . . . According to our poll, full awareness of the Hunter Biden scandal would have led 9.4% of Biden voters to abandon the Democratic candidate[.]”).

⁷ Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[W]e shouldn’t have demoted the [*New York Post*] story.”); Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.); Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.).

months, the FBI led Big Tech to believe that the allegations in the *Post* story were Russian disinformation, even though the FBI had authenticated Hunter Biden’s laptop nearly a year prior.⁸

Beginning in early 2020, the FBI embarked on a concerted campaign to preemptively debunk—or “prebunk”—allegations about the Biden family’s influence peddling. Federal agencies repeatedly warned social media platforms about a pre-election Russian influence operation relating to Hunter Biden and the Ukrainian company Burisma.⁹ In many of these meetings between federal agencies and Big Tech, the FBI raised the topic of potential “hack-and-leak” operations amid conversations about “election security” and potential foreign influence operations.¹⁰ In response, some platforms even adopted new content moderation policies specifically designed to address hacked materials.¹¹

Then, when the *Post* reported on Biden family influence peddling the morning of October 14, 2020, Big Tech did exactly what it had been primed to do. The social media companies obediently treated the article as a potential Russian hack-and-leak operation and applied their content moderation policies to censor it, prevent it from spreading, and hide it from the American people.¹²

Of course, as was obvious then and as is widely acknowledged now,¹³ the laptop was real and its contents were authentic. It was not Russian disinformation. The FBI knew this, too—it had been in possession of Hunter Biden’s laptop since late 2019 and used it in one or more ongoing investigations in 2020.¹⁴ Indeed, in June 2024, the Justice Department used content from the laptop as evidence against Hunter Biden in his trial for felony gun crimes.¹⁵ And yet, the FBI not only primed the social media companies to distrust allegations about Biden family influence peddling in advance, it misled social media companies about the authenticity of Hunter Biden’s laptop after the *Post* story broke.¹⁶

The FBI’s duplicity notwithstanding, Big Tech companies bear blame as well. Contemporaneous documents from the relevant period show that social media companies

⁸ See *infra* Section II.B; Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12.

⁹ See *infra* Section II.C.

¹⁰ *Id.*

¹¹ See *infra* Section II.D.

¹² See *infra* Section III.

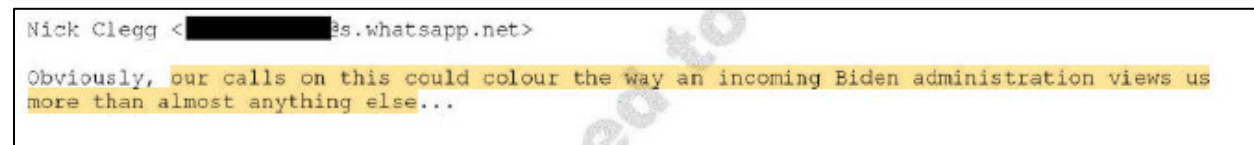
¹³ See, e.g., Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[T]he reporting was not Russian disinformation[.]”); Marshall Cohen & Holmes Lybrand, *Special counsel plans to use infamous Hunter Biden laptop as evidence at gun trial*, CNN (May 22, 2024); Ingrid Jacques, *Trump right about Hunter’s ‘laptop from hell,’ though Biden claimed Russian disinformation*, USA TODAY (June 6, 2024).

¹⁴ Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12.

¹⁵ Ryan King et al., *Hunter Biden gun trial jurors shown infamous laptop first exposed by The Post in dramatic courtroom reveal*, N.Y. POST (June 4, 2024); see also Josh Christenson, *Video of Dems, media rejecting Post’s Hunter Biden laptop story as ‘Russian disinfo’ goes viral after FBI confirms authenticity in court*, N.Y. POST (June 6, 2024).

¹⁶ See *infra* Section III.

recognized and received information that the Biden family influence peddling allegations were likely not Russian disinformation;¹⁷ nonetheless senior leadership at these companies decided to take steps to hide this true content highly relevant to the upcoming presidential election because they knew a failure to censor the story could affect how a potential incoming Biden-Harris Administration would treat them.¹⁸



Nick Clegg <[REDACTED]@s.whatsapp.net>
Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else...

“Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else...”

—Oct. 14, 2020, internal messages between Facebook’s then-Vice President of Global Affairs Nick Clegg to Vice President of Global Public Policy Joel Kaplan about Facebook’s censorship of the *New York Post* article

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have been conducting oversight of how and to what extent the Executive Branch has coerced or colluded with companies and other intermediaries to censor lawful speech.¹⁹ Through a series of reports, the Committee and Select Subcommittee have revealed how the Executive Branch worked with social media companies, “disinformation” pseudoscientists, and others to censor Americans’ online speech.²⁰

This interim report focuses on the coordination between the FBI and Big Tech to suppress allegations about Biden family influence peddling in advance of the 2020 election. Testimony from key FBI and Big Tech personnel and subpoenaed nonpublic internal documents and communications obtained by the Committee and Select Subcommittee show that in the months before the election, the FBI provided social media companies with specific warnings:

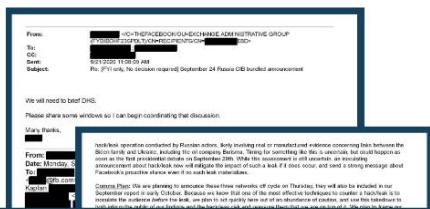
¹⁷ See, e.g., *infra* Section III.B.3.

¹⁸ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), see Ex. 101.

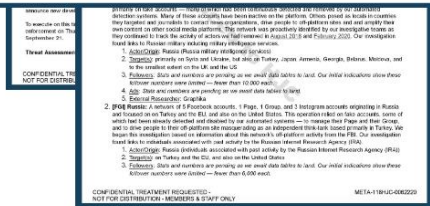
¹⁹ See Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

²⁰ See, e.g., STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE CENSORSHIP-INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITICS OF THE BIDEN ADMINISTRATION (Comm. Print May 1, 2024); STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF THE NATIONAL SCIENCE FOUNDATION: HOW NSF IS FUNDING THE DEVELOPMENT OF AUTOMATED TOOLS TO CENSOR ONLINE SPEECH “AT SCALE” AND TRYING TO COVER UP ITS ACTIONS (Comm. Print Feb. 5, 2024); STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023); STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE FBI’S COLLABORATION WITH A COMPROMISED UKRAINIAN INTELLIGENCE AGENCY TO CENSOR AMERICAN SPEECH (Comm. Print July 10, 2023); STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

- **WHO: *Russia*.** The FBI repeatedly warned Big Tech of a potential influence operation by Russian actors targeting the 2020 election.²¹
- **WHAT: *A hack-and-leak operation*.** The FBI repeatedly warned Big Tech that the Russian influence operation would likely take the form of a hack and leak, similar to the leak of Democratic National Committee emails in 2016.²²
- **WHEN: *Late September or October 2020*.** The FBI repeatedly warned Big Tech that this hack-and-leak operation would come right before the election, either as “an October surprise”²³ or “as soon as the first Presidential debate on September 29th.”²⁴
- **WHY: *To reveal “evidence” regarding “links between the Biden family and Ukraine,” including “Burisma.”*** The FBI warned Big Tech that the Russian hack-and-leak operation would likely involve “real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma.”²⁵ Internal Microsoft notes state that a “week” before the *New York Post* story broke on October 14, the “FBI tipped [Big Tech] off” that “this Burisma story was likely to emerge.”²⁶



Threat Assessment: We have recently received indications from USG partners that they believe there is a risk of a hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma. Timing for something like this is uncertain, but could happen as soon as the first presidential debate on September 29th. While this assessment is still uncertain, an inoculating announcement about hack/leak now will mitigate the impact of such a leak if it does occur, and send a strong message about Facebook's proactive stance even if no such leak materializes.



“USG partners . . . believe there is a risk of a hack/leak operation . . . likely involving . . . evidence concerning links between the Biden family and Ukraine, including the oil company Burisma.”

—Sept. 21, 2020 internal Facebook email to senior Facebook executives

²¹ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), see Ex. 1; Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 21-25.

²² *Id.*

²³ Internal message from Facebook personnel to Nick Clegg (Oct. 15, 2020, 9:29 a.m.), see Ex. 2.

²⁴ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), see Ex. 1.

²⁵ *Id.*

²⁶ Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), see Ex. 3.

Wednesday, October 14, 2020

3:27 PM

All will receive Finance support
MSB and the Threat Hunting team across the company have these tenant IDs and are
watching activity
SSRF has been stood up - Epwiler - includes these and others
-Substance
Heavy exposure, as in many cases state and local gov attacks would impact election
systems
High risk, given the increase in ransomware cases combined with the poor patching
proficiency of this sector

-Hack & Leak

FBI tipped us all off last week that this Burisma story was likely to emerge, and today's call indicated that

FBI tipped us all off last week that this Burisma story was likely to emerge, and today's call indicated that

-23K machines in the US on Windows 7

MICROSOFT CONFIDENTIAL

MSFT_AUC_00000009

“FBI tipped us all off last week that this Burisma story was likely to emerge”
—Oct. 14, 2020, internal Microsoft notes on meeting between U.S. government and Big Tech

As documents produced to the Committee and the Select Subcommittee show, the U.S. government—particularly the FBI, while in possession of Hunter Biden’s laptop—provided detailed warnings of an anticipated future Russian influence operation that directly mirrored the contents of the laptop.²⁷ Documents and testimony also reveal that FBI personnel who were part of the FBI task force providing these warnings knew that the laptop was real prior to the release of the *New York Post* story.²⁸ Armed with evidence of Biden family corruption, the FBI worked for months to ensure that when this evidence emerged in the public sphere, Big Tech would be ready to downplay and censor it.

Big Tech’s immediate reactions to the October 14 *Post* story confirm how the companies were primed by the FBI’s months-long prebunking efforts. For example, internal Facebook communications show that the company almost immediately deemed the story to be a “hack/leak” of the sort Facebook was “expect[ing].”²⁹ On the morning of October 14, Facebook employees exchanged candid communications about the story, including:

- 8:37 AM ET: “About what we expected in the hack/leak department [...] it’s pretty much exactly what we pregamed.”³⁰
- 8:42 AM ET: “It looks like exactly the hack/leak scenario we’d expected.”³¹
- 9:06 AM ET: “Can we check with FBI Delaware if they have anything [on] this [...] Article claims that FBI has had the HDD [hard drive] since December.”³²

²⁷ See *infra* Section II.C.

²⁸ See *infra* Section II.A.

²⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 8:37 a.m.), see Ex. 4.

³⁰ *Id.*

³¹ Internal messages among Facebook personnel (Oct. 14, 2020, 8:42 a.m.), see Ex. 5.

³² Internal messages among Facebook personnel (Oct. 14, 2020, 9:06 a.m.), see Ex. 6.

- 9:09 AM ET: “Exact content expected for hack and leak.”³³
- 9:10 AM ET: “Right on schedule.”³⁴
- 9:14 AM ET: “[Facebook employee] is not in touch with the FBI on this. I’ll connect with Maryland and [Facebook employee] will raise at the [FBI’s Foreign Influence Task Force] meeting today.”³⁵
- 9:33 AM ET: “FYI. Our legal team is reaching out to FBI on this.”³⁶
- 10:40 AM ET: “We’re enqueueing the content with demotion and doing outreach to 3PFCs [third-party factcheckers]. No updated info from FBI, no outreach from the Biden campaign.”³⁷
- 10:55 AM ET: “is this the Oct surprise everyone was waiting for?”³⁸

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]>
To: [REDACTED]
Sent: 10/14/2020 1:46:46 PM
Subject: Message summary [{"otherUserFbId":null,"hreadFbId":3363689413641152}]
Attachments: sticker.png; sticker1.png

[REDACTED] (10/14/2020 05:42:09 PDT):
 > [REDACTED]: can you talk to your FBI counterparts and see what they say about this?

[REDACTED] (10/14/2020 05:42:11 PDT):
 ><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 05:42:26 PDT):
 >It looks like exactly the hack/leak scenario we’d expected.

[REDACTED] (10/14/2020 06:11:49 PDT):
 > [REDACTED] has reached out to FBI in Delaware. Let me make sure that my reaching out will not cause confusion or delay

“It looks like exactly the hack/leak scenario we’d expected”
 —Oct. 14, 2020, internal messages among Facebook personnel

Other documents suggest that key employees within the social media companies understood how their censorship would influence the election. Before the story broke, Facebook personnel understood that their response to an alleged hack and leak could sway the presidential election: in a July 2020 internal exchange, a member of Facebook’s Trust and Safety team said that “when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with [the U.S. Government] to plan for it.”³⁹ Nothing had

³³ Internal messages among Facebook personnel (Oct. 14, 2020, 9:09 a.m.), *see* Ex. 7.

³⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 9:10 a.m.), *see* Ex. 7.

³⁵ Internal messages among Facebook personnel (Oct. 14, 2020, 9:14 a.m.), *see* Ex. 6.

³⁶ Internal messages among Facebook personnel (Oct. 14, 2020, 9:33 a.m.), *see* Ex. 8.

³⁷ Internal messages among Facebook personnel (Oct. 14, 2020, 10:40 a.m.), *see* Ex. 7.

³⁸ Internal messages among Facebook personnel (Oct. 14, 2020, 10:55 a.m.), *see* Ex. 107.

³⁹ Internal messages among Facebook personnel (July 15, 2020, 3:17 p.m.), *see* Ex. 10.

changed by the time the story broke on October 14: the Head of Electoral and Emerging Risk for Facebook’s Trust and Safety reacted by noting that it was only “482 hours to first polls close.”⁴⁰

Message

From: [REDACTED]@fb.com

Sent: 7/15/2020 12:17:30 PM

To: [REDACTED]@fb.com

Subject: Message summary (Content Advisory: 0005:685627227494ad8a2null)

Attachments: 51969112_646151612471827_518749611597588704_n.gif; 51969112_646151612471827_518749611597588704_n.gif; 51969112_646151612471827_518749611597588704_n.gif

[REDACTED] (7/15/2020 11:57:20 PDT):
How is the meeting going? riveting?

[REDACTED] (7/15/2020 12:14:42 PDT):
I'm not engaged with those tech issues

[REDACTED] (7/15/2020 12:14:53 PDT):
Nothing relevant for us yet

[REDACTED] (7/15/2020 12:15:44 PDT):
Yes a really dry meeting

[REDACTED] (7/15/2020 12:16:00 PDT):
shared: 51969112_646151612471827_528749611597588704_n.gif

[REDACTED] (7/15/2020 12:16:05 PDT):

[REDACTED] (7/15/2020 12:17:05 PDT):
>But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG to plan for it.

[REDACTED] (7/15/2020 12:16:38 PDT):
Yeah, it's a little bit too high level.

[REDACTED] (7/15/2020 12:16:34 PDT):
Yeah

[REDACTED] (7/15/2020 12:17:05 PDT):
>But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG to plan for it.

[REDACTED] (7/15/2020 12:17:07 PDT):
I'm not going to encourage for read some academic studies on vote shifting after election day, before results are announced

[REDACTED] (7/15/2020 12:17:20 PDT):
I've read one, it's in at my college library

CONFIDENTIAL TREATMENT REQUESTED - NOT FOR DISTRIBUTION - MEMBERS & STAFF ONLY META-118HUC-0083532

“But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG [the U.S. Government] to plan for it.”
—July 15, 2020, internal messages among Facebook personnel

The FBI has defended its actions as information exchange with private-sector partners to prevent amorphous “foreign malign influence” operations.⁴¹ But if the FBI’s intent was truly to help social media companies combat actual foreign influence operations, the FBI should have shared the single most important fact: the influence-peddling allegations in the *Post* story were based off of real, credible information, including information in the FBI’s possession. The FBI failed to do so. While the FBI eventually conceded that it had no indication that the allegations in the *Post* story were Russian disinformation—only after an FBI agent mistakenly revealed to Twitter that the laptop was “real”—the FBI still withheld the fact that it had seized and authenticated Hunter Biden’s laptop months prior.⁴²

As a result, Twitter and Facebook continued to censor the most significant news story of the election cycle, limiting the reach of allegations of Biden family corruption and ultimately benefitting the Biden-Harris campaign.⁴³ Twitter suppressed the *Post* story by removing links to

⁴⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 11:11 a.m.), see Ex. 9.

⁴¹ OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, No. 24-080, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE’S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS (July 2024) at 7.

⁴² Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.), at 83-85.

⁴³ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), see Ex. 101.

it, applying “safety” warnings, and blocking the ability to send it via direct message.⁴⁴ Although Twitter lifted the ban on the story the next day, it continued to suspend the *Post*’s account until October 30.⁴⁵ For a week, Facebook manually demoted the content by 50 percent, substantially reducing the likelihood that users would see it in their feed.⁴⁶ During this week, over 30 million Americans cast their votes in the 2020 election—nearly one-fifth of the final vote total, and far more than the final reported margin of forty-five thousand votes that determined the outcome of the election.⁴⁷

* * *

The roots of the FBI’s 2020 prebunking scheme date back to the 2016 presidential election, after which emerged sensationalized accounts that foreign “disinformation” had affected the integrity of the election. Fueled by left-wing election denialism, a cottage industry of pseudoscientists, think tanks, and university centers sprung up to combat the alleged rise in misinformation and disinformation, which they held responsible for President Trump’s victory. The FBI formed the Foreign Influence Task Force to coordinate with social media companies and prevent alleged foreign disinformation from reaching American voters. These entities worked together and with social media companies to censor speech—disproportionately conservative speech—all in the name of stopping disinformation and, ironically enough, promoting democracy.

The FBI’s prebunking of allegations of Biden family influence peddling in the closing weeks of the 2020 presidential election was merely a continuation of its earlier efforts to stop President Trump. This is the same FBI that abused its foreign surveillance authorities to spy on President Trump’s campaign in 2016.⁴⁸ This is the same FBI that fabricated evidence to support warrantless surveillance on a Trump campaign associate.⁴⁹ This is the same FBI where senior officials bragged about an “insurance plan” to prevent Donald Trump from becoming president and promised each other they would “stop” him.⁵⁰ This is the same FBI that has purged conservative agents from its ranks and asked employees whether their colleagues are supporters

⁴⁴ Matt Taibbi (@mtaibbi), X (Dec. 2, 2022, 6:34 p.m.), <https://x.com/mtaibbi/status/1598822959866683394>.

⁴⁵ Bruce Golding, *How tweet it is: Twitter backs down, unlocks Post’s account*, N.Y. POST (Oct. 30, 2020).

⁴⁶ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 117; Internal messages among Facebook personnel (Oct. 14, 2020, 11:05 a.m.), *see* Ex. 7; *see also* Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), Ex. 101.

⁴⁷ *See* Brittany Renee Mayes et al., *The U.S. hit 73% of 2016 voting before Election Day*, WASH. POST (Nov. 3, 2020); Catherine Park, *More than 14M Americans have voted early in 2020 presidential election, data shows*, FOX 10 PHOENIX (Oct. 14, 2020); James M. Lindsay, *The 2020 Election by the Numbers*, COUNCIL ON FOREIGN RELS. (Dec. 15, 2020); Paul Waldman, *We came much closer to an election catastrophe than many realize*, WASH. POST (Nov. 18, 2020).

⁴⁸ *See* Bill Rivers, *FBI abuses in domestic surveillance of the Trump campaign eerily echo Red Scare raids*, NBC NEWS (Jan. 10, 2020); *Trump Really Was Spied On*, WALL ST. J. (Feb. 14, 2022).

⁴⁹ Press Release, U.S. Attorney’s Office, Dist. of Conn., FBI Attorney Admits Altering Email Used for FISA Application During “Crossfire Hurricane” Investigation (Aug. 19, 2020), <https://www.justice.gov/usao-ct/pr/fbi-attorney-admits-altering-email-used-fisa-application-during-crossfire-hurricane>.

⁵⁰ John Bowden, *FBI agent in texts: ‘We’ll stop’ Trump from becoming president*, THE HILL (June 14, 2018); Jim Geraghty, *Why Did Two FBI Officials Discuss an ‘Insurance Policy’ In Case of Trump’s Election?*, NAT. REVIEW (Dec. 14, 2017).

of President Trump.⁵¹ The FBI's protestations that it is not biased against conservatives ring hollow when it actively suppressed true and explosive allegations concerning the family of the Democrat nominee for president in 2020.

It is impossible to know what would have happened if the FBI had not prebunked the allegations about Biden family influence peddling. But it is unquestionable that the FBI's actions influenced the 2020 presidential election. And it cannot happen again.

⁵¹ See Josh Christenson, *FBI abuses security clearance to 'purge' conservatives, views them as 'unworthy' of employment: whistleblower*, N.Y. POST (July 2, 2024); STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, FBI WHISTLEBLOWER TESTIMONY HIGHLIGHTS GOVERNMENT ABUSE, MISALLOCATION OF RESOURCES, AND RETALIATION (Comm. Print May 18, 2023).

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
TABLE OF CONTENTS	10
I. Background.....	11
II. After the FBI obtained the laptop with information on Biden family corruption in late 2019, the FBI began to condition Big Tech to incorrectly treat it as Russian disinformation.....	13
A. The FBI case team that possessed and authenticated Hunter Biden’s laptop in late 2019 briefed the FITF about the laptop months before the <i>Post</i> story.	15
B. The FBI and Big Tech met 30-plus times in 2020 to discuss a potential “hack and leak” while Big Tech privately laughed about “influenc[ing] the 2020 elections.”.....	17
1. FITF Bilateral Meetings.....	18
2. USG-Industry Meetings.....	19
C. The FBI specifically warned Big Tech about a Russian hack-and-leak operation in fall 2020 involving “Burisma” and the Biden family.	24
D. Social media companies changed their policies on hacked materials and started “inoculating” the public for a “hack and leak.”	32
1. Facebook.....	32
2. Google.....	36
3. Twitter.....	37
E. The Aspen Institute hosted a tabletop exercise for Big Tech companies about a potential Russian hack-and-leak scenario involving the Bidens and Burisma.	38
III. Big Tech censored the true story, and the FBI hid key information, while millions voted.....	40
A. Big Tech quickly censored the true <i>New York Post</i> story, believing it was “exactly” what the FBI had warned about for months.....	41
B. Big Tech reached out to the FBI and the FBI hid key information.	46
1. The Twitter-FITF Bilateral Meeting.....	46
2. The FBI’s Internal Deliberations	48
3. The Facebook-FITF Bilateral Meeting	50
4. The USG-Industry Meeting	52
5. The FITF’s Follow-Up Discussions	53
C. Despite a lack of evidence, Big Tech continued to censor the story because of concerns about a potential Biden-Harris Administration.....	55
1. Facebook.....	55
2. Twitter.....	62
3. Other companies	65
D. FBI continued to withhold information as Big Tech continued to reach out.....	67
IV. Epilogue: The fight against FBI election interference continues.....	71
V. Appendix.....	76

I. Background

“Hack & Leak[.] FBI tipped us all off last week that this Burisma story was likely to emerge, and today’s call indicated that.”

—Oct. 14, 2020, 3:27 p.m. ET, internal notes from Microsoft summarizing a “USG-Industry” meeting on the day the *New York Post* published the story on the Biden family’s influence peddling.⁵²

As the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have revealed, following the 2016 election, offices within the Executive Branch launched efforts to covertly censor Americans’ free expression. The FBI formed the Foreign Influence Task Force (FITF) in the fall of 2017.⁵³ The Global Engagement Center (GEC), a multi-agency entity housed within the State Department established by President Obama in early 2016 to counter terrorism,⁵⁴ expanded its mandate in 2017 to include countering foreign disinformation.⁵⁵ Not to be outdone, the Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) formed the Countering Foreign Influence Task Force (CFITF) in 2018, which evolved into the “Mis, Dis, and Malinformation (MDM) Team” in 2021 to counter foreign *and American* speech.⁵⁶

Once the Biden-Harris Administration took power, these censorship efforts only further expanded. Senior members of the Biden-Harris White House immediately began a months-long pressure campaign on Facebook, YouTube, Amazon, and other companies to censor views disfavored by the Biden-Harris Administration.⁵⁷ The Office of the Director of National Intelligence (ODNI) launched ODNI’s Foreign Malign Influence Center in 2021.⁵⁸ DHS created the Orwellian Disinformation Governance Board in May 2022.⁵⁹ And CISA built out and met

⁵² Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), *see* Ex. 3.

⁵³ *Combatting Foreign Influence*, FEDERAL BUREAU OF INVESTIGATION, <https://www.fbi.gov/investigate/counterintelligence/foreign-influence> (last visited Oct. 18, 2024).

⁵⁴ Exec. Order No. 13,721, 81 C.F.R. 14943 (2016).

⁵⁵ *The Global Engagement Center: Leading the United States Government’s Fight Against Global Disinformation Threat: Hearing Before the Subcomm. on State Dep’t and USAID Management, Int’l Operations, and Bilateral Int’l Development of the S. Comm. on Foreign Rels.*, 116th Cong. (Mar. 5, 2020).

⁵⁶ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS* (Comm. Print June 26, 2023); *see also* STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH* (Comm. Print Nov. 6, 2023).

⁵⁷ STAFF OF H. COMM. ON THE JUDICIARY & SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, *THE CENSORSHIP-INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITIC OF THE BIDEN ADMINISTRATION*, (Comm. Print May 1, 2024).

⁵⁸ *Organization*, NAT’L COUNTERTERRORISM CENTER, <https://www.dni.gov/index.php/nctc-who-we-are/organization/340-about/organization/foreign-malign-influence-center> (last visited Oct. 18, 2024).

⁵⁹ Amanda Seitz, *Disinformation board to tackle Russia, migrant smugglers*, ASSOCIATED PRESS (Apr. 28, 2022).

with its MDM Advisory Subcommittee—featuring Big Tech executives and disinformation pseudo-scientists—throughout 2022.⁶⁰

The Executive Branch also began colluding with private and academic institutions on censorship during this period. The Committee and Select Subcommittee’s oversight of the censorship-industrial complex has revealed how a consortium of “disinformation” academics led by Stanford University’s Stanford Internet Observatory (SIO), called the Election Integrity Partnership (EIP), worked directly with CISA and the GEC to monitor and censor Americans’ online speech in advance of the 2020 presidential election.⁶¹ Created in the summer of 2020 “at the request of DHS/CISA,”⁶² the EIP enabled the federal government to launder its censorship activities through a university in hopes of bypassing both the First Amendment and public scrutiny.⁶³

This constellation of censorship organizations, alongside Big Tech, worked overtime to nominally “secure” the 2020 election from foreign interference.⁶⁴ In reality, this meant censoring election-related speech, including questions about the validity of unrestricted mail-in voting.⁶⁵ And it also meant “inoculating” the public against damaging stories about Biden family influence peddling.⁶⁶

⁶⁰ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND ‘DISINFORMATION’ PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

⁶¹ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

⁶² Email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 p.m.); *see* Ex. 123.

⁶³ *See* STAFF OF H. COMM. ON THE JUDICIARY & SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ FREE SPEECH (Comm. Print Nov. 6, 2023).

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

II. After the FBI obtained the laptop with information on Biden family corruption in late 2019, the FBI began to condition Big Tech to incorrectly treat it as Russian disinformation

“We have recently received indications from USG partners that they believe there is a risk of a hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma. Timing for something like this is uncertain, but could happen as soon as the first presidential debate on September 29th.”

—Sept. 21, 2020, 2:04 p.m. ET, internal Facebook email about a potential Russian hack-and-leak threat.⁶⁷

In 2019, the FBI obtained a hard drive from a laptop attributed to Hunter Biden.⁶⁸ Gary Shapley, an IRS whistleblower who spent years overseeing a tax evasion case against Hunter Biden, testified that by November 2019, the FBI had “verified [the laptop’s] authenticity” by “matching the device number against Hunter Biden’s Apple iCloud ID.”⁶⁹

As the *New York Post* later detailed, the laptop contained evidence of a variety of crimes, including extensive evidence of broad influence peddling schemes committed by the Biden family and Biden family business associates.⁷⁰ The laptop also included evidence of Hunter Biden’s use of illegal drugs while engaging in other illicit activities.⁷¹ The laptop has since been used as evidence in Hunter Biden’s recent felony conviction on federal gun charges.⁷²

In 2020, just a few months after the FBI authenticated Hunter Biden’s laptop, it began a months-long campaign to “prebunk” a potential news story about the laptop’s contents, conditioning Big Tech platforms to falsely believe that Hunter Biden and his shady business dealings with the Ukrainian oil company Burisma would be the subject of the next Russian hack-and-leak operation.⁷³ A hack-and-leak operation is when an actor obtains information from a hacking campaign, then releases, or “leaks,” that information via social media or other means for public consumption.

⁶⁷ *Id.*

⁶⁸ Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12; see also Marshall Cohen & Holmes Lybrand, *Special counsel plans to use infamous Hunter Biden laptop as evidence at gun trial*, CNN (May 22, 2024); Ingrid Jacques, *Trump right about Hunter’s ‘laptop from hell,’ though Biden claimed Russian disinformation*, USA TODAY (June 6, 2024); Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. POST (Oct. 14, 2020).

⁶⁹ Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12.

⁷⁰ See Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. POST (Oct. 14, 2020).

⁷¹ *Id.*

⁷² Marshall Cohen & Holmes Lybrand, *Special counsel plans to use infamous Hunter Biden laptop as evidence at gun trial*, CNN (May 22, 2024).

⁷³ See, e.g., Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), Ex. 1.

The FBI raised warnings about a potential hack-and-leak operation in meetings between the FBI’s Foreign Influence Task Force (FITF) and Big Tech companies. The FBI first began meeting with Big Tech companies during the 2018 election cycle to share information about potential foreign influence operations for which platforms should be on the lookout.⁷⁴ In 2020, the FBI began raising specific warnings about a potential Russian hack and leak of information related to the Biden family—namely Hunter Biden—and Burisma, which would appear through authentic news sources.⁷⁵

By September 2020, many platforms had actively prepared to address this specific potential hack-and-leak scenario. On September 1, 2020, Google began enforcing a new policy specifically designed to curtail the distribution of hacked political materials.⁷⁶ Later in the month, Facebook made an “inoculating announcement” to “mitigate the impact of such a leak if it does occur,”⁷⁷ and then changed its hack-and-leak policies in October “to ensure we are prepared for foreign-backed leak operations that may develop in the weeks to come.”⁷⁸ Also in September 2020, representatives from the country’s largest platforms, including many who were regularly attending FITF meetings, participated in a tabletop exercise—a meeting where participants engage with a hypothetical scenario and offer potential responses and solutions to the hypothetical problems—set up by the Aspen Institute to wargame a response to a potential scenario involving leaked documents concerning Hunter Biden’s work with Burisma.⁷⁹

By the time the *Post* published its story on Biden family influence peddling on October 14, 2020, Big Tech platforms had (1) been thoroughly primed to view the story as a Russian hack-and-leak influence operation; (2) developed and implemented new protocols for handling content relating to a potential hack and leak; and (3) brainstormed and practiced their new responses in tabletop exercises with other platforms and news outlets in the months prior.

Although the FBI conditioned Big Tech to believe any allegations about Hunter Biden were Russian disinformation, the social media companies are far from blameless. Internal messages obtained by the Committee and Select Subcommittee show that personnel at the social media platforms knew the dangerous consequences of their censorship decisions. In one message thread from July 2020, a member of Facebook’s Trust and Safety team said that when Facebook employees inevitably “get hauled up to the hill to testify on why we influenced the 2020 elections,” they would be able to say that they had “been meeting for YEARS with USG to plan for it.”⁸⁰

⁷⁴ Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

⁷⁵ Internal messages among Facebook personnel (Sept. 20, 2020, 6:26 p.m.), *see* Ex. 13; Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), *see* Ex. 3.

⁷⁶ *Hacked political materials policy global roll-out (November 2020)*, GOOGLE (Sept. 1, 2020), <https://support.google.com/adspolicy/answer/9991623>.

⁷⁷ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

⁷⁸ Internal Facebook email to CEO Mark Zuckerberg and COO Sheryl Sandberg (Oct. 5, 2020, 5:29 a.m.), *see* Ex. 75.

⁷⁹ *See infra* Section II.E; Email from Aspen Digital staff to Roundtable participants (Sept. 1, 2020, 7:44 p.m.), Ex. 99; *see also* Aspen Digital Hack-and-Dump Scenario Outline (Sept. 2020), Ex. 100.

⁸⁰ Internal messages among Facebook personnel (July 15, 2020, 3:17 p.m.), *see* Ex. 10.



[redacted] (7/15/2020 12:17:05 PDT):
>But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG to plan for it.



“But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG [the U.S. Government] to plan for it.”
—July 15, 2020, internal messages among Facebook personnel

These messages show that, while Big Tech may not have known that the FBI was priming them to censor a true story, they understood that their meetings with the U.S. government regarding online speech could very well influence the 2020 election.

A. The FBI case team that possessed and authenticated Hunter Biden’s laptop in late 2019 briefed the FITF about the laptop months before the *Post* story.

In late 2019, during the course of an ongoing investigation, the FBI seized and authenticated the hard drive of the laptop attributed to Hunter Biden, the subject of the October 14, 2020 *New York Post* article.⁸¹

Evidence obtained by the Committee and Select Subcommittee shows that the FBI case team was in contact with the FITF months prior to the *New York Post* story. The FBI Special Agent who served as the FITF’s Russia Unit Chief from mid-2019 to June 2021 testified that he received “three to five briefings” on the case because the Hunter Biden investigation was linked to Ukraine, which fell under the purview of the Russia Unit.⁸² The FITF Russia Chief further

⁸¹ Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12; see also Marshall Cohen & Holmes Lybrand, *Special counsel plans to use infamous Hunter Biden laptop as evidence at gun trial*, CNN (May 22, 2024); Ingrid Jacques, *Trump right about Hunter’s ‘laptop from hell,’ though Biden claimed Russian disinformation*, USA TODAY (June 6, 2024).

⁸² Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024), (on file with the Comm.) at 28-29.

testified that he first learned that the FBI was in possession of a laptop attributed to Hunter Biden in one of these briefings before the *Post* article was published.⁸³ Similarly, an FBI Criminal Investigative Division analyst detailed to the FITF in 2020 testified that he learned about the existence of the Hunter Biden investigation “a few months before” October 14, when he received an internal FBI document confirming it, though he did not learn about the laptop until the morning the *Post* article broke.⁸⁴

The FITF Russia Unit Chief’s testimony that members of the FITF knew that the FBI was in possession of Hunter Biden’s authenticated laptop prior to the *Post* story is consistent with other testimony received by the Committee and Select Subcommittee.⁸⁵ Laura Dehmlow, then-China Unit Chief of the FITF and now the Section Chief of the FITF, testified that she and others knew that the FBI was in possession of the laptop well before October 14, 2020.⁸⁶ Dehmlow testified to the Committee:

Q. When the information was relayed to you following the Twitter call that the first agent had said the laptop was real, just to clarify, you knew prior to that conversation that the laptop was real. Is that correct?

A. I did, yes.

Q. But you don’t recall when approximately you learned.

A. I don’t, sorry.

Q. Sitting here today, do you know when the FBI first determined that the laptop was real?

A. I don’t. I know that there is some information in the public record regarding when the FBI acquired the laptop, but I don’t, sitting here, remember that date.

Q. Do you know who else at FITF knew that the laptop was real?

A. I don’t actually. I would assume both my – yes, I would certainly say that Brad Benavides [then-Section Chief of the FITF] was aware.⁸⁷

⁸³ *Id.*

⁸⁴ Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 89-90.

⁸⁵ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.); Transcribed Interview of the Assistant Section Chief of the FITF, H. Comm. on the Judiciary (Apr. 24, 2024) (on file with Comm.); Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.).

⁸⁶ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 35-37.

⁸⁷ Even though two of the three FITF unit chiefs and the Assistant Section Chief testified that they knew that the FBI was in possession of the laptop in advance of the *Post* publishing its report, then-Section Chief Brad Benavides testified that he did not know the FBI was in possession of the laptop prior to the story. See Transcribed Interview of Bradley Benavides, H. Comm. on the Judiciary (Sept. 28, 2023) (on file with Comm.) at 146-160.

Q. What about the individuals on the Russia unit?

A. I would assume the unit chief was also aware. I'm pretty certain of that fact.

Q. For the individual --

DOJ Counsel: Just to clarify, do you know to a certainty that they were aware, or are you just making deductions?

A. I'm pretty certain that they were aware.⁸⁸

This testimony confirms that senior personnel of the FITF, the FBI task force providing warnings to Big Tech about a potential Russian hack-and-leak operation involving Hunter Biden and Burisma, knew that the FBI was in possession of the Hunter Biden laptop well before the *Post* article publicly disclosed the existence of the laptop or the evidence of influence peddling contained therein.

B. The FBI and Big Tech met 30-plus times in 2020 to discuss a potential “hack and leak” while Big Tech privately laughed about “influenc[ing] the 2020 elections.”

Throughout 2020, two parallel tracks emerged for information sharing between government agencies and Big Tech. In “FITF Bilateral Meetings,” FBI FITF staff would meet with individual social media platforms to discuss a number of topics, generally relating to ongoing or anticipated foreign influence operations. In “USG-Industry meetings,” the FBI’s FITF, other federal agencies, and social media companies convened as a large group to share information about potential foreign influence campaigns. Several of the FITF personnel who knew that the laptop was authentic prior to the release of the *New York Post* story attended these large group meetings.⁸⁹ Through both sets of meetings, the U.S. government shared specific warnings of a potential Russian hack-and-leak operation relating to Hunter Biden and Burisma, priming social media platforms to censor the *Post* story when it broke on October 14, 2020.⁹⁰

⁸⁸ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023), (on file with the Comm.), at 37.

⁸⁹ See, e.g., USG-Industry meeting invitation (Apr. 20, 2022, 6:00 p.m.), Ex. 45; USG-Industry meeting invitation (May 13, 2020, 4:00 p.m.), Ex. 47; USG-Industry meeting invitation (June 10, 2020, 6:00 p.m.), Ex. 51; USG-Industry meeting invitation (July 8, 2020, 6:00 p.m.), Ex. 71; USG-Industry meeting invitation (July 15, 2020, 6:00 p.m.), Ex. 57; USG-Industry meeting invitation (Aug. 12, 2020, 6:00 p.m.), Ex. 59; USG-Industry meeting invitation (Sept. 9, 2020, 6:00 p.m.), Ex. 72; USG-Industry meeting invitation (Sept. 16, 2020, 6:00 p.m.), Ex. 64; USG-Industry meeting invitation (Oct. 7, 2020, 6:00 p.m.), Ex. 68; USG-Industry meeting invitation (Oct. 14, 2020, 6:00 p.m.), Ex. 27; USG-Industry meeting invitation (Oct. 21, 2020, 6:00 p.m.), Ex. 73; USG-Industry meeting invitation (Oct. 28, 2020, 6:00 p.m.), Ex. 74.

⁹⁰ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), see Ex. 1; see also Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

1. FITF Bilateral Meetings

From February 10, 2020 to October 14, 2020, the FBI’s FITF met over two dozen times with Google, Twitter, Facebook, Microsoft, and other companies in one-on-one “FITF Bilateral Meetings”—including individual meetings with Facebook and Twitter on October 14, 2020, the day that the *Post* story published.⁹¹ These bilateral meetings have restarted in 2024.⁹²

FBI agents—typically Elvis Chan, Assistant Special Agent in Charge of the FBI’s San Francisco Field Office—scheduled FITF bilateral meetings with social media companies quarterly, with additional calls or meetings on an ad hoc basis.⁹³ Because the FBI would share technical threat intelligence and analysis, the social media platforms’ threat intelligence teams would generally be responsible for attending and participating in the FITF bilateral meetings.⁹⁴

While the FITF primarily shared technical, actor-focused information with Big Tech companies in these meetings, it also discussed high-level strategies and themes employed by foreign actors.⁹⁵ The Russia Unit Chief of the FITF testified that he was “certain” there was discussion of a potential “hack-and-leak” threat from Russia during these meetings.⁹⁶ He explained that in the FITF bilateral meetings, “we often talked about tactics that had happened in the past.”⁹⁷ Because “larger cyber actors” like Russia had shown a propensity for this kind of

⁹¹ See, e.g., Email from Elvis Chan to Yahoo personnel (Jan. 3, 2020, 3:46 p.m.), Ex. 19; Email from Elvis Chan to LinkedIn personnel (Jan. 3, 2020, 3:48 p.m.), Ex. 18; Email from Elvis Chan to Google personnel (Jan. 6, 2020, 8:25 p.m.), Ex. 15; Email from Elvis Chan to Yahoo personnel (Apr. 13, 2020, 4:15 p.m.), Ex. 20; Email from Elvis Chan to LinkedIn personnel (Apr. 13, 2020, 11:21 p.m.), Ex. 24; Email from Elvis Chan to Google personnel (Apr. 14, 2020, 9:51 p.m.), Ex. 21; Email from Elvis Chan to Facebook personnel (May 12, 2020, 5:29 p.m.), Ex. 22; Email from Elvis Chan to Google personnel (July 14, 2020, 10:59 a.m.), Ex. 26; Email from Elvis Chan to LinkedIn personnel (July 14, 2020, 11:02 a.m.), Ex. 31; Email from Elvis Chan to Yahoo personnel (July 14, 2020, 1:58 p.m.), Ex. 28; Email from Elvis Chan to Facebook personnel (July 16, 2020, 10:10 p.m.), Ex. 29; Email from Elvis Chan to Google personnel (Sept. 10, 2020, 2:13 p.m.), Ex. 33; Email from Elvis Chan to LinkedIn personnel (Sept. 10, 2020, 2:13 p.m.), Ex. 37; Email from Elvis Chan to Facebook personnel (Sept. 10, 2020, 5:12 p.m.), Ex. 36; Email from Elvis Chan to Yahoo personnel (Sept. 14, 2020, 5:21 p.m.), Ex. 34; Email from Elvis Chan to Google personnel (Sept. 29, 2020, 11:04 a.m.), Ex. 39; Email from Elvis Chan to Google personnel (Sept. 29, 2020, 11:04 a.m.), Ex. 40; Email from Elvis Chan to Yahoo personnel (Sept. 29, 2020, 11:09 a.m.), Ex. 70; Email from Elvis Chan to Reddit personnel (Sept. 29, 2020, 11:10 a.m.), Ex. 69; Email from Elvis Chan to LinkedIn personnel (Sept. 29, 2020, 2:08 p.m.), Ex. 41; Email from Elvis Chan to Facebook personnel (Oct. 4, 2020, 2:31 p.m.), Ex. 16; see also Ex. 42 (Emails from FBI to Big Tech participants scheduling FITF Bilateral meetings).

⁹² Kevin Collier & Ken Dilanian, *FBI Resumes Outreach to Social Media Companies Over Foreign Propaganda*, NBC NEWS (Mar. 20, 2024).

⁹³ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with the Comm.) at 22-23; Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 25.

⁹⁴ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 143.

⁹⁵ OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, NO. 24-080, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE’S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS (July 2024) at 17-18.

⁹⁶ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 21.

⁹⁷ *Id.*

campaign in the past via other hack-and-leak operations, “that’s certainly one of the tactics [the FITF] discussed” with social media companies.⁹⁸

Occasionally, Big Tech’s policy staff attended these bilateral meetings for awareness of the matters under discussion.⁹⁹ For example, the Russia Unit Chief specifically remembered that the Facebook employee who developed an updated hack-and-leak policy for the platform (and subsequently briefed CEO Mark Zuckerberg on these changes) sometimes attended FITF-Facebook bilateral meetings.¹⁰⁰ In Elvis Chan’s *Murthy v. Missouri* deposition, he confirmed that in bilateral meetings, the FBI discussed platforms’ policies regarding hacked materials and how the policies might apply to potential foreign influence operations.¹⁰¹

2. USG-Industry Meetings

A second set of standing meetings occurred among several government stakeholders (including the FBI, DOJ, CISA, DHS’s Office of Intelligence & Analysis, and ODNI) and a group of industry participants from many different companies (including Facebook, Google, Twitter, and Microsoft, among others). Based on the documents the Committee and Select Subcommittee have obtained, the first USG-Industry meeting for the 2020 election occurred no later than April of 2020.¹⁰² These meetings continued on a monthly—and then, as the election drew nearer, weekly—basis in the lead-up to the 2020 election, including on October 14, 2020—the day the *Post* story broke.¹⁰³ In 2024, CISA and the FBI resumed meetings with Big Tech.¹⁰⁴

The USG-Industry meetings were a regular forum for federal agencies and social media companies to exchange high-level information about foreign threats. Meeting agendas and other

⁹⁸ *Id.*

⁹⁹ *Id.* at 143-145.

¹⁰⁰ *Id.* at 145; *see e.g.*, Internal Facebook email to CEO Mark Zuckerberg and COO Sheryl Sandberg (Oct. 5, 2020, 5:29 a.m.), Ex. 75.

¹⁰¹ *Murthy v. Missouri*, No. 3:22-cv-01213, 2023 WL 43352270 (WD La. July 4, 2023) (Deposition of Elvis Chan), at 203-206.

¹⁰² USG-Industry meeting invitation (Apr. 20, 2020, 6:00 p.m.), *see* Ex. 45.

¹⁰³ *See, e.g.*, Email from CISA personnel to industry participants (May 12, 2020, 9:12 a.m.), Ex. 46; USG-Industry meeting invitation (May 13, 2020, 4:00 p.m.), Ex. 47; Internal Facebook readout of USG-Industry meeting (May 14, 2020, 11:31 a.m.), Ex. 48; Agenda emails between industry participants (June 9, 2020, 1:45 p.m.), Ex. 49; Scheduling email from Facebook personnel to industry group (June 9, 2020, 8:45 p.m.), Ex. 50; Internal Facebook readout of the USG-Industry meeting (June 10, 2020, 8:35 a.m.), Ex. 53; USG-Industry Meeting invitation (June 10, 2020, 6:00 p.m.), Ex. 51; Internal messages among Facebook personnel (June 30, 2020, 6:31 p.m.), Ex. 52; Internal messages among Facebook personnel (July 1, 2020, 4:14 p.m.), Ex. 54; Internal messages among Facebook personnel (July 10, 2020, 5:12 a.m.), Ex. 55; Scheduling email from Google personnel to industry group (July 14, 2020, 10:13 p.m.), Ex. 27; USG-Industry Meeting invitation (July 15, 2020, 6:00 p.m.), Ex. 57; Internal Facebook readout of the USG-Industry meeting (July 17, 2020, 7:17 a.m.), Ex. 58; USG-Industry Meeting invitation (Aug. 12, 2020, 6:00 p.m.), Ex. 59; Internal Facebook readout of the USG-Industry meeting (Aug. 13, 2020, 5:58 a.m.), Ex. 60; Agenda emails between CISA and Facebook personnel (Sept. 9, 2020, 11:41 a.m.), Ex. 66; Agenda emails between industry participants (Sept. 11, 2020, 12:40 p.m.), Ex. 61; Scheduling email from Facebook personnel to industry group (Sept. 11, 2020, 1:00 p.m.), Ex. 62; Agenda emails between CISA and Facebook personnel (Sept. 15, 2020, 8:06 a.m.), Ex. 63; USG-Industry Meeting invitation (Sept. 16, 2020, 6:00 p.m.), Ex. 64; Internal Facebook notes about USG-Industry meeting (Sept. 16, 2020), Ex. 65; Agenda emails between CISA and Facebook personnel (Oct. 5, 2020, 6:41 a.m.), Ex. 67; USG-Industry Meeting invitation (Oct. 7, 2020, 6:00 p.m.), Ex. 68.

¹⁰⁴ David DiMolfetta, *CISA, FBI resuming talks with social media firms over disinformation removal, Senate Intel chair says*, NEXTGOV/FCW (May 7, 2024).

documents obtained by the Committee and Select Subcommittee show that the federal agencies and Big Tech repeatedly discussed “Hack/Leak” in the meetings leading up to the 2020 election.

For example, a meeting on July 15, 2020, included “Hack/Leak and USG Attribution Speed/Process” as an agenda item listed under the heading “Deep Dive Topics.”¹⁰⁵

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]69D>
To: [REDACTED]@google.com; [REDACTED]@google.com; [REDACTED]@twitter.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@linkedin.com; [REDACTED]@verizonmedia.com; [REDACTED]@verizonmedia.com; [REDACTED]@verizonmedia.com; [REDACTED]@google.com; [REDACTED]@reddit.com; [REDACTED]@pinterest.com; [REDACTED]@pinterest.com; [REDACTED]@medium.com; [REDACTED]; [REDACTED]; [REDACTED]@microsoft.com; [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]; [REDACTED]; [REDACTED]@wikimedia.org; [REDACTED]@reddit.com; [REDACTED]@medium.com; [REDACTED]@twitter.com; [REDACTED]@linkedin.com; [REDACTED]@linkedin.com; [REDACTED]; [REDACTED]@verizonmedia.com
CC: [REDACTED]; [REDACTED]
Sent: 7/14/2020 3:11:43 PM
Subject: Dial In Information: 7/15 Monthly USG | Industry Call

Hello Everyone,

Three quick updates before tomorrow:

- Below please find the WebEx dial-in information for the Wednesday, 7/15 USG/Industry call.
- Starting in August onwards, we will migrate to using a BJN for our calls, and that information will be forthcoming.
- Here is the planned agenda (as discussed at our bi-weekly last Friday):
 - 10 minutes: Dial In/Opening
 - 30 minutes: Threat Updates
 - Threat update from USG (FBI, I&A)
 - Threat update from industry (FB, TW, GOOG)
 - 40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
 - Election process update from USG
 - Hack/Leak and USG Attribution Speed/Process
 - Vote-by-mail: How do we deal with the gap between Nov 3 and results?
 - 10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)

Thank you for your engagement and commitment here, and look forward to seeing you tomorrow.
USG/Industry Webex meeting.

“Hack/Leak and USG Attribution Speed/Process”
—July 15, 2020, USG-Industry meeting agenda

¹⁰⁵ USG-Industry meeting agenda (July 14, 2020, 3:11 p.m.), Ex. 76.

In a September 16, 2020, USG-Industry meeting, Big Tech and federal agencies discussed “hack and leak operations” again.¹⁰⁷ Facebook’s internal readout of the meeting explained that the discussion focused on “preparing for ‘hack and leak’ operations attempting to use platforms and traditional media to amplify unauthorized information drops,” among other topics.¹⁰⁸

Message

From: [REDACTED] [REDACTED]@fb.com
Sent: 9/17/2020 12:55:58 PM
To: lobbyists [REDACTED]@fb.com; [REDACTED] [REDACTED]@fb.com; [REDACTED] [REDACTED]@fb.com
CC: [REDACTED] [REDACTED]@fb.com; [REDACTED] [REDACTED]@fb.com; [REDACTED] [REDACTED]@fb.com; [REDACTED] [REDACTED]@fb.com
Subject: HPM USG-Industry Monthly Election Integrity Meeting (September)

Team,

Sharing our HPM from this week’s USG-Industry meeting on election integrity and the link to our successfully-landed Joint Industry Statement. Great XFN collaboration on this continues (many thanks to [REDACTED], [REDACTED], [REDACTED] & [REDACTED]).

Let us know if you have any questions.
[REDACTED]

United States: USG-Industry Monthly Election Integrity Meeting (September)

- **What happened:** On Wednesday, September 16, U.S. Public Policy along with Security Policy, Cybersecurity Legal, Law Enforcement Outreach, and our i3 Threat Team participated in our monthly U.S. Government-Industry Election Integrity call to coordinate security efforts for the U.S. 2020 election. We again successfully landed a Joint Industry Statement regarding our long-standing and ongoing efforts to secure US2020 in collaboration with the USG entities charged with securing the election, available here: <https://twitter.com/fbnewsroom/status/1306314722082349056?s=20>. Co-signatories included Facebook, Google, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, and Wikimedia. USG attendees included senior officials from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DOJ’s National Security Division, and the Office of the Director of National Intelligence (ODNI). This was the seventh such convening to prepare for US2020, the fifth call in our series of USG-Industry monthly calls leading up to the November election, and further strengthened and deepened our collaboration with industry and USG.
- **Why relevant:** The discussion focused on timely sharing accurate voting and election information, countering targeted attempts to undermine the election conversation, preparing for “hack and leak” operations attempting to use platforms and traditional media to amplify unauthorized information drops, and mitigation efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure.
- **Next Steps:** We will continue to participate in these calls with our tech peers & USG partners through the end of 2020. The next monthly convening will occur on October 7th. We will then transition to weekly calls to check-in & share information through the December 14th Electoral College meeting.

“[P]reparing for ‘hack and leak’ operations”
—Sept. 17, 2020 internal Facebook notes about USG-Industry meeting

¹⁰⁷ USG-Industry Meeting invitation (Sept. 16, 2020, 6:00 p.m.), see Ex. 64.

¹⁰⁸ Internal Facebook readout of USG-Industry meeting (Sept. 17, 2020, 12:55 p.m.), see Ex. 78.

Finally, on October 7, 2020, just one week before the *Post* article on Biden family influence peddling was published, the USG-Industry meeting agenda again included “Hack/Leak concerns” as a topic of discussion.¹⁰⁹

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Monday, October 5, 2020 7:21 AM
To: [REDACTED] <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: October 2020 USG/Industry Meeting (Draft Agenda)

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Good morning!

Wanted to follow-up to see if you were ok with the schedule as noted below. If so, we will circulate —as final—with industry today.

Thanks!

Sent from my iPhone

On Sep 29, 2020, at 2:41 PM, [REDACTED] <[REDACTED]@fb.com> wrote:

Gents,

We wanted to share the draft/proposed agenda in advance of our USG/Industry meeting scheduled from 2:00-3:30 PM EST on Wednesday, October 7th. Additionally, to facilitate the logistics for the call, we have included the dial-in information below.

Please let us know if you have any additions or concerns.

Thanks!

CONFIDENTIAL TREATMENT REQUESTED - META-118HJC-0000960
NOT FOR DISTRIBUTION - MEMBERS & STAFF ONLY

[REDACTED]

*******DRAFT AGENDA*******

- **10 minutes: Dial In/Opening**
- **30 minutes: Threat Updates (Including Pre/Post Presidential Debates)**
 - Threat update from USG -- Foreign Actor/Activity & Non-IO Cyber Threats
 - Threat update from industry (FB, Twitter, GOOG)
- **40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)**
 - Updates on USG Election Process
 - Election Day Virtual Coordination Center Update
 - Top 5 Delegitimization Claims To Counter
 - Hack/Leak Concerns
 - Election Official Reporting
- **10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)**

“*Deep Dive Topics . . . Hack/Leak Concerns*”
—Sept. 29, 2020, USG-Industry meeting draft agenda

¹⁰⁹ USG-Industry meeting draft agenda (Sept. 29, 2020, 2:41 p.m.), *see* Ex. 67.

According to Facebook’s readout, “[t]he discussion focused on efforts to identify and mitigate delegitimization claims against US2020 electoral outcomes, including potential hack/leak scenarios.”¹¹⁰

Message

From: ██████████@fb.com
Sent: 10/8/2020 10:24:28 AM
To: lobbyists ██████████@fb.com
CC: ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com
Subject: USG-Industry Monthly Election Integrity Meeting (October)

Team,

Sharing our HPM from this week’s USG-Industry meeting on election integrity. Great XFN collaboration on this continues (many thanks to ██████████, ██████████, ██████████ & ██████████).

Let us know if you have any questions.
██████████

United States: USG-Industry Monthly Election Integrity Meeting (October)

- **What happened:** On Wednesday, October 7, U.S. Public Policy along with Security Policy, Cybersecurity Legal, Law Enforcement Outreach, and our i3 Threat Team participated in our monthly U.S. Government-Industry Election Integrity call to coordinate security efforts for the U.S. 2020 election. Participants included Facebook, Google, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, and Wikimedia. USG attendees included senior officials from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DOJ’s National Security Division, and the Office of the Director of National Intelligence (ODNI). This was the eighth such convening to prepare for US2020, the sixth call in our series of USG-Industry monthly calls leading up to the November election, and further strengthened and deepened our collaboration with industry and USG.
- **Why relevant:** The discussion focused on efforts to identify and mitigate delegitimization claims against US2020 electoral outcomes, including potential hack/leak scenarios, operational readiness of states and localities for administering the vote, and timely election-related information sharing via elections operations.
- **Next Steps:** We will continue to participate in these calls with our tech peers & USG partners through the end of 2020. The meetings will now shift to a weekly 30 minute cadence where we will share information through the December 14th Electoral College meeting.

“The discussion focused on efforts to identify and mitigate...potential hack/leak scenarios”
—Oct. 8, 2020, internal Facebook notes on Oct. 7 USG-Industry meeting

C. The FBI specifically warned Big Tech about a Russian hack-and-leak operation in fall 2020 involving “Burisma” and the Biden family.

According to emails, meeting invitations, and internal readouts of meetings between U.S. government officials and Big Tech employees, foreign influence operations—and hack-and-leak threats specifically—were a recurring topic of discussion among the FBI and social media

¹¹⁰ Internal Facebook readout of USG-Industry meeting (Oct. 8, 2020, 10:24 a.m.), see Ex. 80.

companies.¹¹¹ In September 2020, the Big Tech companies participating in these meetings confirmed in a joint press statement that these discussions focused on “[w]ays to counter targeted attempts to undermine the election conversation before, during, and after the election,” including “preparing for possible so-called ‘hack and leak’ operations attempting to use platforms and traditional media to amplify unauthorized information drops.”¹¹²

“For several years, tech companies have worked together, and with U.S. government agencies tasked with protecting the integrity of elections, to counter election threats across our respective platforms. As we approach the November election, we continue to prepare, meet regularly, and share updates on the threats we see. At today’s meeting, we specifically discussed:

1. Ways to help provide real-time, clear information about the voting process and election results given expected logistical disruptions posed by COVID-19.
2. Ways to counter targeted attempts to undermine the election conversation before, during, and after the election. This includes preparing for possible so-called “hack and leak” operations attempting to use platforms and traditional media to amplify unauthorized information drops.
3. Detection efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure.

As the global pandemic poses unprecedented challenges for the 2020 U.S. election, we will continue this ongoing communication and close work between industry and U.S. institutions tasked with election security to share key findings and operational insights in the weeks to come.”

FACEBOOK Google reddit Microsoft verizon media Pinterest LinkedIn WIKIMEDIA FOUNDATION

“[W]e specifically discussed...preparing for possible so-called ‘hack and leak’ operations”
—Sept. 2020 statement from tech industry participants in USG-Industry meetings

While Big Tech issued public statements about how it was generally discussing potential hack-and-leak operations with the U.S. government, the discussions themselves were more specific. Indeed, according to internal Big Tech documents obtained by the Committee and Select Subcommittee, the FBI told Big Tech to expect a “hack/leak operation” that almost exactly matched the details of the *New York Post* reporting on Biden family influence peddling.¹¹³ The FBI got the date and the contents right: it repeatedly warned that the supposed hack-and-leak operation would come right before the election, likely as “an October surprise,”¹¹⁴ and that it would reveal “evidence” regarding “links between the Biden family and Ukraine,”

¹¹¹ See, e.g., USG-Industry meeting agenda (July 14, 2020, 3:11 p.m.), Ex. 76; Internal Facebook readout of USG-Industry meeting (Sept. 17, 2020, 12:55 p.m.), Ex. 78; USG-Industry meeting draft agenda (Sept. 29, 2020, 2:41 p.m.), Ex. 67; Internal Facebook readout of USG-Industry meeting (Oct. 8, 2020, 10:24 a.m.), Ex. 80.

¹¹² Statement from tech industry participants, see Ex. 11; see also Internal messages among Facebook personnel (Aug. 5, 2020), Ex. 12; Emails among tech industry participants (Sept. 15, 2020), Ex. 124.

¹¹³ See, e.g., Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), Ex. 1; Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), Ex. 3; see also Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

¹¹⁴ Internal message from Facebook personnel to Nick Clegg (Oct. 15, 2020, 9:29 a.m.), see Ex. 2.

including the oil company “Burisma.”¹¹⁵ In fact, the week before the *Post* story broke on October 14, the “FBI tipped [Big Tech] off” that “this Burisma story was likely to emerge.”¹¹⁶

Documents obtained by the Committee and Select Subcommittee show that Big Tech got the message loud and clear. One Facebook employee predicted that “in the next few weeks” there would be “leaks about Biden’s supposed link to Burisma.”¹¹⁷ This employee wrote that while Facebook would not “be able to prove” that these were hacks, the company would “have responsible USG players publicly saying this is part of a foreign influence operation,” and that their “secret squirrel partners”—apparently referring to U.S. government officials—would also say it was a Russian operation.¹¹⁸ He conceded that there would not be a “public smoking gun to prove” that the leaks were Russian operations, but that “the circumstantial public evidence will be quite strong.”¹¹⁹ Facebook employees even discussed how the company’s policies might apply to different scenarios that “provide precedent for how [Facebook] would analyze the dissemination of materials that may result from a hack of Burisma” and how to brief leadership on their options.¹²⁰

The statement proved prescient. Once the *Post* story was published just a few weeks later, Facebook’s “secret squirrel partners” did exactly what the platform expected.¹²¹ Fifty-one former intelligence community officials organized by Antony Blinken and the Biden campaign falsely claimed that the story bore “all the classic earmarks of a Russian information operation.”¹²² All the while, Big Tech censored the story even though it did not (and, of course, could not) prove that the story was Russian disinformation.

¹¹⁵ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

¹¹⁶ Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), *see* Ex. 3.

¹¹⁷ Internal messages among Facebook personnel (Sept. 9, 2020, 2:28 p.m.), *see* Ex. 81.

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ Internal messages among Facebook personnel (Sept. 9, 2020, 2:37 p.m.), *see* Ex. 81.

¹²¹ Internal messages among Facebook personnel (Sept. 9, 2020, 2:28 p.m.), *see* Ex. 81.

¹²² STAFF OF H. COMM. ON THE JUDICIARY, SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, AND H. PERMANENT SELECT COMM. ON INTELLIGENCE, 118TH CONG., THE INTELLIGENCE COMMUNITY 51: HOW CIA CONTRACTORS COLLUDED WITH THE BIDEN CAMPAIGN TO MISLEAD AMERICAN VOTERS (Comm. Print June 25, 2024); STAFF OF H. COMM. ON THE JUDICIARY, SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, AND H. PERMANENT SELECT COMM. ON INTELLIGENCE, 118TH CONG., THE HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY OFFICIALS AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN VOTERS (Comm. Print May 10, 2023); *see also* Brooke Singman, *Biden campaign, Blinken orchestrated intel letter to discredit Hunter Biden laptop story, ex-CIA official says*, FOX NEWS (Apr. 20, 2023).

[REDACTED] (9/19/2020 11:18:55 PDT):
>In the upcoming cycle, we're actually likely to be reasonably confident, but unable to prove publicly.

[REDACTED] (9/19/2020 11:19:03 PDT):
>So there is a question of our confidence tolerance.

[REDACTED] (9/19/2020 11:19:15 PDT):
>But if Russian actors drop a Burisma leak in the next two weeks

[REDACTED] (9/19/2020 11:19:25 PDT):
>(which is likely & we are actively prepping for it)

[REDACTED] (9/19/2020 11:19:32 PDT):
>I doubt we'll be able to prove it is hacked.

[REDACTED] (9/19/2020 11:20:34 PDT):
>It's Snowden versus Podesta, right? Snowden had lawful access to the materials. He unlawfully took them and shared with an unintended audience. Podesta never intentionally shared anything.

[REDACTED] (9/19/2020 11:22:23 PDT):
>So today we'd leave Snowden materials up but take Podesta materials down. Is that right?

[REDACTED] (9/19/2020 11:22:50 PDT):
>Or does Snowden's illegality play into our assessment?

[REDACTED] (9/19/2020 11:23:36 PDT):
>(Setting aside entirely the idea that we're going to know anything about any of this at the moment the materials appear on FB.)

[REDACTED] (9/19/2020 11:24:03 PDT):
>yeah fair question.

[REDACTED] (9/19/2020 11:24:41 PDT):
>1) i am not sure that Snowden had valid access to what he put out, or at least not all of it. so there would be that question

[REDACTED] (9/19/2020 11:25:09 PDT):
>2) obviously if there were confidential information, classified or PII would be removed

[REDACTED] (9/19/2020 11:25:49 PDT):
>3) but yes, there is a delicate balance of whether content leaked (by a whistleblower or otherwise) is allowed...

[REDACTED] (9/19/2020 11:26:45 PDT):
>Actually, it's Snowden + conclusive evidence that Snowden was in fact controlled by the Russians.

[REDACTED] (9/19/2020 11:26:54 PDT):
>And the Q is whether those two factors combined are sufficient for us to act.

[REDACTED] (9/19/2020 11:28:05 PDT):
>We are likely to have in the next few weeks a leak or series of leaks about Biden's supposed link to Burisma, where we won't be able to prove they were "hacked", but where we will have responsible USG players publicly saying this is part of a foreign influence operation, our own assessment will align that this is a Russian op, and we will hear from our trusted secret squirrel partners that this is a Russian op.

[REDACTED] (9/19/2020 11:28:24 PDT):
>I doubt we'll have a public smoking gun to prove that, but the circumstantial public evidence will be quite strong.

[REDACTED] (9/19/2020 11:29:04 PDT):
>The Q is whether in that case, we want to be empowered to take stronger action. I could see either (a) removal; or (b) position ourselves to put a label on the content.

“[W]e won't be able to prove they were 'hacked', but . . . we will hear from our trusted secret squirrel partners that this is a Russian op.”

—Sept. 19, 2020, internal messages among Facebook personnel

In a separate exchange of messages between Facebook employees on September 20, 2020, an employee shared a BBC article about a “documents leak” revealing “how Russian

The discussion continued with one Facebook employee noting that a leak may be “imminent.”¹²⁷ Another Facebook employee responded, “[we] expect this within the next 1-3 weeks.”¹²⁸ The date of the message—September 20, 2020—was just over three weeks before October 14th, the day that the *New York Post* story was published.

[REDACTED] (9/20/2020 15:50:57 PDT):
>this is extremely helpful to have a head's up on. Thank you. Do we have a sense of timing?

[REDACTED] (9/20/2020 15:51:10 PDT):
>Not yet, unfortunately

[REDACTED] (9/20/2020 15:51:31 PDT):
>the intel we're getting is pretty piecemeal, and my sense is the external folks also don't know whether this will happen, and if so, when

[REDACTED] (9/20/2020 15:51:45 PDT):
>our hypothesis would be that the riskiest period would be right before the first presidential debates

[REDACTED] (9/20/2020 15:51:54 PDT):
>and then the risk rises before each subsequent debate

[REDACTED] (9/20/2020 15:52:33 PDT):
>if we track 2016's wikileaks hack/leak, it could also drop if something damaging came out on the President

[REDACTED] (9/20/2020 15:52:48 PDT):
>the Podesta leaks, for example, were released the same day as the Access Hollywood tape

[REDACTED] (9/20/2020 15:54:01 PDT):
>Ah OK. that makes sense. I thought it was imminent. If there's a discussion underway about how to counter it with responsible news -- i.e. what my team works with -- I'm happy to walk through some options, including how we assess it from a news standpoint in real time once it's released

[REDACTED] (9/20/2020 15:54:15 PDT):
>definitely

[REDACTED] (9/20/2020 15:54:24 PDT):
>I think we'd expect this within the next 1-3 weeks

“I think we’d expect [the hack and leak] within the next 1-3 weeks”

—Sept. 20, 2020, internal messages among Facebook personnel, three weeks before the *New York Post* story on the Biden family’s influence peddling

On September 21, 2020, in a separate email to Facebook leadership, including Facebook’s then-Vice President of Global Affairs Nick Clegg and Vice President of Global Public Policy Joel Kaplan, a Facebook employee stated clearly who specifically was warning Facebook about a Russian hack-and-leak threat involving Burisma and the Biden family in advance of the 2020 election: “USG [U.S. Government] partners.”¹²⁹ In her description of communications with “USG partners,” the Facebook employee wrote that “they [the U.S. government partners] believe there is a high risk of a hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma.”¹³⁰ According to the Facebook

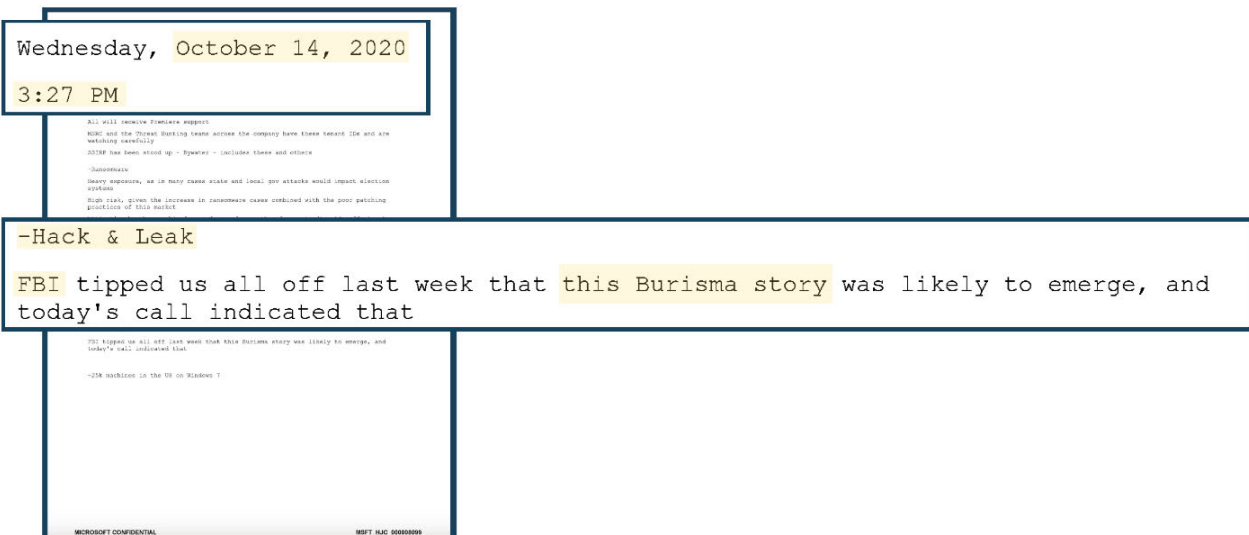
¹²⁷ Internal messages among Facebook personnel (Sept. 20, 2020, 6:54 p.m.), *see* Ex. 13.

¹²⁸ *Id.*

¹²⁹ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

¹³⁰ *Id.*; *see also* Internal messages among Facebook personnel (Sept. 18, 2020, 2:11 p.m.), Ex. 82; Internal messages among Facebook personnel (Sept. 21, 2020, 9:37 a.m.), Ex. 83.

Consistent with Facebook’s internal discussions, internal Microsoft notes taken during a USG-Industry meeting on October 14, 2020, confirm that the FBI led the prebunking efforts, stating that the “FBI tipped us all off last week that this Burisma story was likely to emerge, and today’s call indicated that.”¹³²



“FBI tipped us all off last week that this Burisma story was likely to emerge”
—Oct. 14, 2020, internal Microsoft notes on USG-Industry meeting

These documents confirm that the U.S. government—specifically, the FBI—had not only discussed the possibility of a hack-and-leak operation with Big Tech platforms months before the *Post* story was published, but had also shared specific details, including the type of operation (hack and leak), who the target would be (then-candidate Biden and his family), when it would happen (late September or October 2020), who would orchestrate the leak (Russia), what information would be leaked (the Biden family’s relationship with Burisma), and how the information might be disseminated (via authentic news sources). The FBI shared this information with Big Tech platforms in both bilateral and USG-Industry meetings. As the Committee and Select Subcommittee have learned from witness testimony, multiple FBI personnel assigned to the FITF, the FBI’s task force that provided these “hack-and-leak” warnings, were aware that the FBI had seized and authenticated Hunter Biden’s laptop months prior.¹³³

¹³² Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), see Ex. 3.

¹³³ See Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 28-29; Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 35-37.

D. Social media companies changed their policies on hacked materials and started “inoculating” the public for a “hack and leak.”

In response to the repeated discussions with, and warnings from, the FBI and other federal agencies, platforms began preparing ways to combat an impending hack and leak of information relating to the Bidens and Burisma. Some platforms prepared by attempting to “inoculate the audience *before* the leak,”¹³⁴ while other platforms began to change their content moderation policies to include more strict provisions regarding hacked materials—including changes designed specifically to target hacked political materials.¹³⁵ These efforts by social media platforms to prepare for a potential hack and leak culminated in September 2020, just one month before the *Post* published its story.

1. Facebook

Facebook used public statements to raise awareness about a potential Russian hack-and-leak operation and expanded its hack-and-leak policies to prepare for the potential operation. In September 2020, after receiving “indications from USG partners” that “there is a risk of a hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma,” Facebook determined that the best way to prepare for this potential hack/leak operation was to “inoculate the audience.”¹³⁶

To accomplish this goal of inoculation, Facebook leveraged the announcement of its takedown of three Russian networks perpetrating influence operations around the globe to “both inform the public of our findings and the hack/leak risk and reassure them that we are on top of it.”¹³⁷ Facebook employees described this inoculation—or prebunking—as “one of the most effective techniques to counter a hack/leak.”¹³⁸ Facebook designed the announcement to prime Facebook users to view any pre-election release of damaging information about the Bidens as a Russian hack-and-leak influence operation—much like the FBI was priming social media companies to do.¹³⁹ In September 2020, Facebook believed that “an inoculating announcement about hack/leak now will mitigate the impact of such a leak if it does occur, and send a strong message about Facebook’s proactive stance even if no such leak materializes.”¹⁴⁰

¹³⁴ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1 (emphasis in original).

¹³⁵ Emails between Google personnel and Democratic National Committee staff (Aug. 5, 2020, 5:27 p.m.), *see* Ex. 84.

¹³⁶ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

¹³⁷ *Id.*; *see also* Email from Facebook personnel to DNI staff (Sept. 24, 2020, 4:16 p.m.), Ex. 85.

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.*

hack/leak operation conducted by Russian actors, likely involving real or simulated evidence concerning links between the White House and Ukraine, including the role of former Russian President Vladimir Putin. Timing for announcing the story is uncertain, but could happen as soon as the first presidential debate in September 2020. While this announcement is still uncertain, an evolving conversation about hack/leak is now well beyond the point of just a leak of documents, and needs a strong message about Facebook's position before the 2020 US election.

Comms Plan: We are planning to announce these three networks off cycle on Thursday, they will also be included in our September report in early October. Because we know that one of the most effective techniques to counter a hack/leak is to inoculate the audience before the leak, we plan to act quickly here out of an abundance of caution, and use this takedown to both inform the public of our findings and the hack/leak risk and reassure them that we are on top of it. We plan to frame our public statements carefully to raise awareness, but neither hyperbolize the threat, nor guarantee that such an operation will occur. To land this narrative, we're engaging external researchers and pundits to inform their commentary and raise the importance of responsible coverage of hack/leak operations. We're working to land this story with broadcast and wires to amplify and shape our coverage.

Comms Plan: We are planning to announce these three networks off cycle on Thursday, they will also be included in our September report in early October. Because we know that one of the most effective techniques to counter a hack/leak is to inoculate the audience before the leak, we plan to act quickly here out of an abundance of caution, and use this takedown to both inform the public of our findings and the hack/leak risk and reassure them that we are on top of it. We plan to frame our public statements carefully to raise awareness, but neither hyperbolize the threat, nor guarantee that such an operation will occur. To land this narrative, we're engaging external researchers and pundits to inform their commentary and raise the importance of responsible coverage of hack/leak operations. We're working to land this story with broadcast and wires to amplify and shape our coverage.

1. [Redacted]

2. [Redacted]

3. [Redacted]

4. [Redacted]

5. [Redacted]

6. [Redacted]

7. [Redacted]

8. [Redacted]

9. [Redacted]

10. [Redacted]

11. [Redacted]

12. [Redacted]

13. [Redacted]

14. [Redacted]

15. [Redacted]

16. [Redacted]

17. [Redacted]

18. [Redacted]

19. [Redacted]

20. [Redacted]

21. [Redacted]

22. [Redacted]

23. [Redacted]

24. [Redacted]

25. [Redacted]

26. [Redacted]

27. [Redacted]

28. [Redacted]

29. [Redacted]

30. [Redacted]

31. [Redacted]

32. [Redacted]

33. [Redacted]

34. [Redacted]

35. [Redacted]

36. [Redacted]

37. [Redacted]

38. [Redacted]

39. [Redacted]

40. [Redacted]

41. [Redacted]

42. [Redacted]

43. [Redacted]

44. [Redacted]

45. [Redacted]

46. [Redacted]

47. [Redacted]

48. [Redacted]

49. [Redacted]

50. [Redacted]

51. [Redacted]

52. [Redacted]

53. [Redacted]

54. [Redacted]

55. [Redacted]

56. [Redacted]

57. [Redacted]

58. [Redacted]

59. [Redacted]

60. [Redacted]

61. [Redacted]

62. [Redacted]

63. [Redacted]

64. [Redacted]

65. [Redacted]

66. [Redacted]

67. [Redacted]

68. [Redacted]

69. [Redacted]

70. [Redacted]

71. [Redacted]

72. [Redacted]

73. [Redacted]

74. [Redacted]

75. [Redacted]

76. [Redacted]

77. [Redacted]

78. [Redacted]

79. [Redacted]

80. [Redacted]

81. [Redacted]

82. [Redacted]

83. [Redacted]

84. [Redacted]

85. [Redacted]

86. [Redacted]

87. [Redacted]

88. [Redacted]

89. [Redacted]

90. [Redacted]

91. [Redacted]

92. [Redacted]

93. [Redacted]

94. [Redacted]

95. [Redacted]

96. [Redacted]

97. [Redacted]

98. [Redacted]

99. [Redacted]

100. [Redacted]

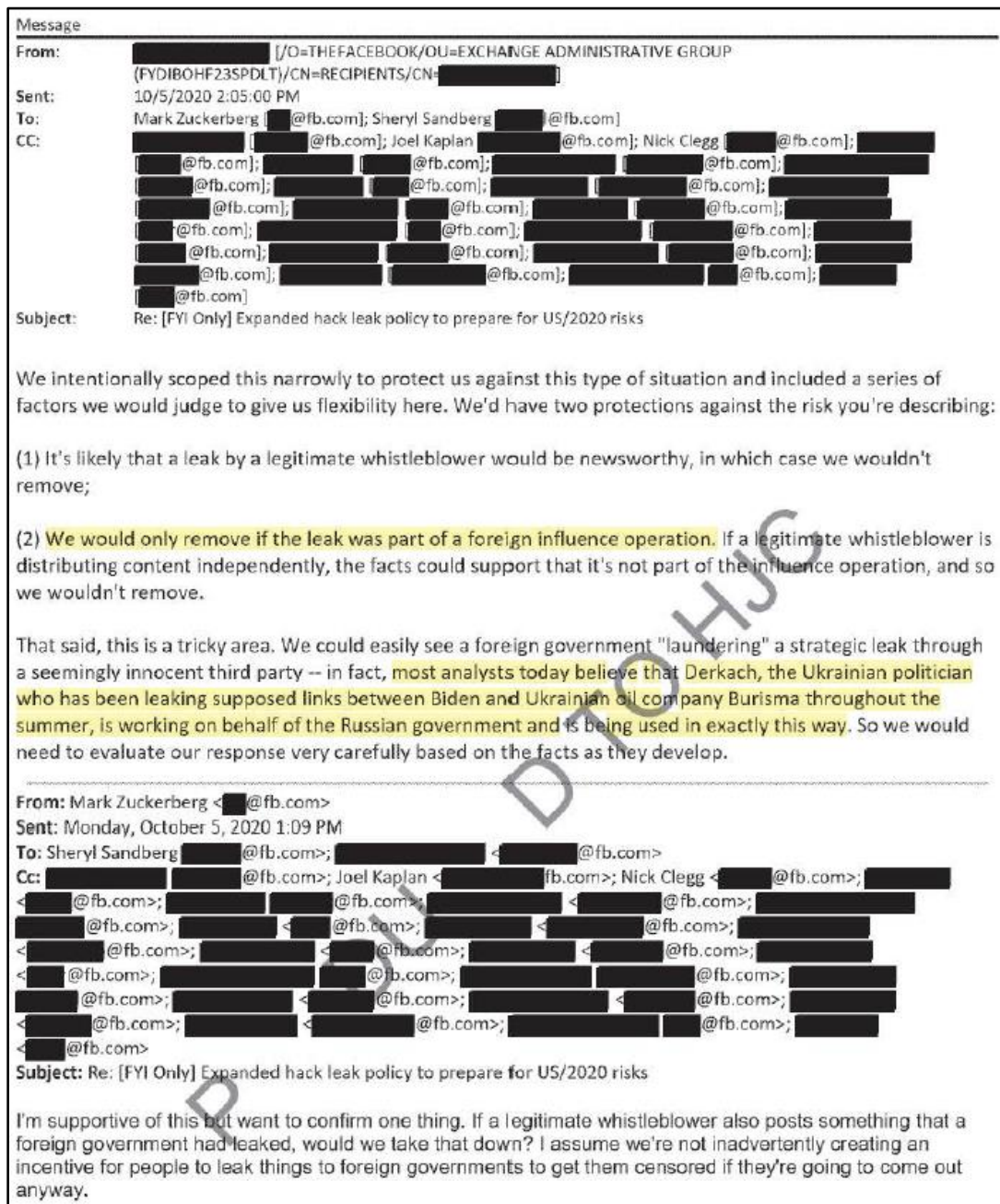
CONFIDENTIAL TREATMENT REQUESTED - NOT FOR DISTRIBUTION - MEMBERS & STAFF ONLY META 1184G-000222

“We know that one of the most effective techniques to counter a hack/leak is to inoculate the audience before the leak”
 —Sept. 21, 2020 internal messages among Facebook personnel

In addition to inoculating its users to anticipate a hack-and-leak operation, Facebook also expanded its hack-and-leak policies. On October 5, 2020, Facebook employees emailed CEO Mark Zuckerberg and COO Sheryl Sandberg to make them “aware of a policy change designed to ensure we are prepared for foreign-backed leak operations that may develop in the weeks to come.”¹⁴¹ The employees explained that the policy change would allow Facebook to “remove any leaked material (whether evidence of a hack exists or not) that is part of a foreign government influence operation.”¹⁴² This was a change from previous policy, which permitted the removal of material resulting from a hack, but allowed leaked content to stay up “because of the significant role of whistleblowers in exposing corruption and empowering accountability throughout history.”¹⁴³ Critically, the Facebook employees told Zuckerberg and Sandberg that the policy had a “narrow focus” and would “only apply to leaks targeting the US 2020 election.”¹⁴⁴

¹⁴¹ Internal Facebook email to CEO Mark Zuckerberg and COO Sheryl Sandberg (Oct. 5, 2020, 5:29 a.m.), see Ex. 75.
¹⁴² *Id.*
¹⁴³ *Id.*
¹⁴⁴ *Id.*

meetings, during which a potential Russian hack and leak involving the Bidens and Burisma had been discussed for months.¹⁴⁶ Facebook’s close interactions with the FBI allowed its employees to “anticipate that this policy change will be supported by the security community,” while admitting that it “may raise eyebrows by some free speech advocates.”¹⁴⁷



“I’m supportive of” the expansion of the “hack leak policy to prepare for US/2020 risks.”
—Oct. 5, 2020, email from CEO Mark Zuckerberg to Facebook personnel

¹⁴⁶ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with the Comm.) at 143.

¹⁴⁷ Internal Facebook email to Mark Zuckerberg and Sheryl Sandberg (Oct. 5, 2020, 5:29 a.m.), see Ex. 75.

Zuckerberg asked specifically about how the company’s new policy would apply “[i]f a legitimate whistleblower also posts something that a foreign government had leaked.”¹⁴⁸ Other than this one question, he was “supportive” of the policy expansion prior to the *Post* story breaking.¹⁴⁹ A Facebook employee responded that, in that situation, the company “would only remove if the leak was part of a foreign influence operation.”¹⁵⁰

The emails between Zuckerberg and his Facebook team demonstrate how the FBI, specifically the FITF, prompted Facebook to change its content moderation policies. In the months preceding the 2020 presidential election, the FBI’s FITF met with Facebook’s threat intelligence team to warn them of a Russian hack-and-leak operation targeting the 2020 election. Based on these briefings, the threat intelligence team recommended an update to Facebook’s internal policies that would allow the company to remove additional content from the site. Facebook anticipated that the FBI and others would support this change, and Facebook leadership approved the change before its rollout at the beginning of October 2020.

2. Google

Google also developed and implemented new policies prohibiting ads from linking to hacked political materials.¹⁵¹ U.S. enforcement of this new policy began on September 1, 2020—two months before the global policy went into effect.¹⁵² In August 2020, Google staff previewed this shift to employees of the Democratic National Committee (DNC), explaining that “[t]his policy is specifically related to the distribution of hacked political material.”¹⁵³ DNC staff responded approvingly, thanking Google for its “work to reduce the risk and impact of hack-and-dump operations.”¹⁵⁴

¹⁴⁸ Internal email from CEO Mark Zuckerberg to Facebook personnel (Oct. 5, 2020, 1:09 p.m.), *see* Ex. 75.

¹⁴⁹ *Id.*

¹⁵⁰ Internal Facebook email to CEO Mark Zuckerberg and COO Sheryl Sandberg (Oct. 5, 2020, 2:05 p.m.), *see* Ex. 75.

¹⁵¹ *Hacked political materials policy global roll-out (November 2020)*, GOOGLE (Sept. 1, 2020) <https://support.google.com/adspolicy/answer/9991623>.

¹⁵² *Id.*

¹⁵³ Emails between Google personnel and Democratic National Committee staff (Aug. 5, 2020, 5:27 p.m.), *see* Ex. 84.

¹⁵⁴ Emails between Google personnel and Democratic National Committee staff (Aug. 5, 2020, 9:57 p.m.), *see* Ex. 84.

with the hackers themselves,” and “likely would have restricted the sharing of links related to the hacked materials.”¹⁵⁵ Twitter adopted this policy because it “examined its role in the distribution of [former senior Clinton campaign official] John Podesta’s emails and other hacked materials” that were leaked in 2016.¹⁵⁶ Twitter “reached the conclusion that we [Twitter] needed to have a policy restricting that type of behavior,”¹⁵⁷ and because of concerns raised by the U.S. intelligence community about vulnerabilities that might be exploited in the future.¹⁵⁸ These policies enabled the platform to later censor content based on the FBI’s warnings about a Russian hack and leak in 2020 involving the Bidens and Burisma.¹⁵⁹

E. The Aspen Institute hosted a tabletop exercise for Big Tech companies about a potential Russian hack-and-leak scenario involving the Bidens and Burisma.

Non-governmental third parties, though likely not privy to key information such as the fact that the FBI had Hunter Biden’s laptop, also were part of the prebunking campaign. Most notably, on June 25, 2020, Aspen Digital—a program of the Aspen Institute, a think-tank that has done significant work relating to so-called “information disorder”¹⁶⁰—hosted a “Hack and Leak Roundtable” that included “journalists, ethicists, First Amendment attorneys, and platform executives” for a discussion about “standards and ethics when it comes to publication and coverage in hack and leak scenarios.”¹⁶¹

Documents obtained by the Committee and Select Subcommittee show that Facebook employees who had met with the FITF in 2020 were instrumental in developing and facilitating this roundtable and the subsequent tabletop exercise described below.¹⁶² The roundtable participants discussed how traditional news media and Big Tech platforms would handle materials that they obtained as a result of an alleged hack and leak, how to assess the motivation for hack and leaks, the role government actors could play in confirming whether the materials were authentic or had been manipulated in some way, and whether it was appropriate to apply information labels to related content.¹⁶³ Other attendees included representatives from Twitter, Reddit, Wikimedia Foundation, NBC News, CNN, NPR, the *Washington Post*, and the *New York Times*.¹⁶⁴

¹⁵⁵ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.) at 21.

¹⁵⁶ *Id.* at 20. John Podesta served as Hillary Clinton’s campaign manager in 2016.

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ *See infra* Section III.C.2.

¹⁶⁰ *Commission on Information Disorder*, ASPEN INSTITUTE, <https://www.aspeninstitute.org/programs/commission-on-information-disorder/> (last visited Oct. 18, 2024).

¹⁶¹ Aspen Digital Hack and Leak Roundtable agenda (June 25, 2020), *see* Ex. 86.

¹⁶² *See* Emails between Aspen Institute and Facebook personnel (May 19, 2020, 5:48 p.m.), Ex. 91; Emails between Aspen Institute, Facebook, and Stanford personnel (June 25, 2020), Ex. 92; Emails between Aspen Institute and Facebook personnel (July 13, 2020), Ex. 93; Email from Aspen Institute personnel to Facebook personnel (Sept. 28, 2020, 12:01 p.m.), Ex. 94.

¹⁶³ *Id.*; Aspen Digital Hack and Leak Roundtable meeting readout (July 2, 2020, 12:54 p.m.), *see* Ex. 87; *see also* Opening remarks from Aspen Institute roundtable, Ex. 88; Emails from Aspen Institute staff to industry participants (July 14, 2020), Ex. 89; Emails from Aspen Institute staff to industry participants (June 22, 2020), Ex. 90.

¹⁶⁴ Aspen Digital Hack and Leak Roundtable participant list (June 25, 2020), *see* Ex. 95.

A few months later, in September 2020, Aspen Digital hosted a tabletop exercise about a hack-and-leak scenario.¹⁶⁵ In a tabletop exercise, participants simulate their responses to a hypothetical set of facts, reacting to the responses of other participants and new information revealed incrementally throughout the exercise. Unlike the roundtable, which broadly discussed how companies handle materials related to a hack and leak, this exercise revolved around a specific hypothetical scenario involving a leak of Burisma documents tied to Hunter Biden.¹⁶⁶ Once again, Facebook personnel who had met with the FITF in 2020 were the primary drafters of the exercise.¹⁶⁷ According to internal Facebook messages and emails, one Facebook employee even rewrote the scenario as the date of the exercise approached.¹⁶⁸

The final exercise outline laid out a hypothetical day-by-day developing story, beginning on October 5, 2020, in which a news outlet obtained and published leaked documents involving Hunter Biden and Burisma, and various government actors and campaign officials began to respond.¹⁶⁹ The scenario was designed to give social media platforms and news outlets the opportunity to “think through out loud” how they would respond and “game out how various tech platforms and news organizations would respond in real time as the story unfolded.”¹⁷⁰

This exercise gave social media companies the opportunity to stress test the hack-and-leak responses they had proposed—and in some cases finalized—after the FBI’s warnings to expect one in September or October 2020. Even more, the scenario set forth by Aspen Digital closely mirrored the warnings given by the FBI and the details of the actual news story published by the *Post* just one month later.

* * *

By early October 2020, the stage had been set. In individual and group meetings with Big Tech platforms, the FBI’s FITF had repeatedly warned of an impending Russian hack and leak of documents alleging a Biden family influence peddling scheme relating specifically to Hunter Biden and Burisma. The social media platforms had deliberated and implemented new policies designed to limit the visibility of these documents if they did emerge. And in a tabletop exercise, the platforms had simulated how they would spike the exact story that the *Post* would ultimately publish. The prebunking was complete. When October 14 came, the platforms were ready to censor.

¹⁶⁵ Email from Aspen Institute staff to industry participants (Aug. 12, 2020, 12:49 p.m.), *see* Ex. 96.

¹⁶⁶ *Id.*

¹⁶⁷ Internal messages among Facebook personnel (Sept. 20, 2020, 8:03 p.m.), Ex. 97; Email from Aspen Institute personnel to Facebook and Twitter personnel (Aug. 7, 2020, 6:44 a.m.), Ex. 98.

¹⁶⁸ *Id.*

¹⁶⁹ Email from Aspen Digital staff to Roundtable participants (Sept. 1, 2020, 7:44 p.m.), Ex. 99; *see also* Aspen Digital Hack-and-Dump Scenario Outline (Sept. 2020), Ex. 100.

¹⁷⁰ *Id.*

III. Big Tech censored the true story, and the FBI hid key information, while millions voted

“Obviously, our calls on this [*New York Post* story] could colour the way an incoming Biden administration views us more than almost anything else.”

—October 14, 2020, WhatsApp message from Facebook’s then-Vice President of Global Affairs Nick Clegg to Vice President of Global Public Policy Joel Kaplan about Facebook’s censorship of the *New York Post* story.¹⁷¹

Early on October 14, 2020, the *New York Post* published an article, sourced from the contents of Hunter Biden’s abandoned laptop, exposing Biden family influence-peddling in Ukraine and around the world.¹⁷² For months, the FBI had conditioned social media companies to expect a Russian hack-and-leak operation that would target the Bidens and Burisma. The companies had developed responses for this scenario and had war-gamed the best way to apply them. The scenario they had been expecting, it seemed, was finally playing out.

Conditioned to assess that the story was the product of a hack and leak, social media companies’ initial response to the *Post* story was to censor it. Some companies wanted more information, though, and reached out to the FBI to be certain that this was the hack and leak they had been warned of before making final decisions about whether to continue their censorship of the story and the content within. But the FBI refused to acknowledge that it possessed and had authenticated the laptop.

Having not received this critical information from the FBI about the provenance of the laptop, social media platforms continued doing what they had been primed to do since early 2020: censor the *Post*’s true article. Twitter blocked the URL to the story and prohibited it from being shared on the platform, citing violations of its hacked materials policies. Facebook manually demoted the story in its algorithm, making users less likely to see it. Although platforms used different tools to achieve their goal, each invoked the warnings they received from their meetings with the government to explain why they censored the story.¹⁷³

But the FBI’s warnings were not the only thing motivating Big Tech. Platforms were keenly aware that their “calls on this [*New York Post* story] could colour the way an incoming Biden administration views us more than almost anything else.”¹⁷⁴ Platforms knew that if they

¹⁷¹ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), Ex. 101.

¹⁷² Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. Post (Oct. 14, 2020).

¹⁷³ See, e.g., Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[T]he FBI warned us about a potential Russian disinformation operation about the Biden family and Burisma in the lead up to the 2020 election. . . . It’s since been made clear that the [*New York Post*] reporting was not Russian disinformation, and in retrospect, we shouldn’t have demoted the story.”); Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

¹⁷⁴ *Id.*

did not act to suppress the story, their failure to censor it would threaten their relationship with a potential Biden-Harris Administration in 2021 and beyond.

This censorship of true election-related material denied millions of voters access to crucial information as they cast their vote for president. When the *Post* article came out nearly three weeks before Election Day, early and mail-in voting had already opened in many states. According to public reporting, between October 14—the day the *Post* published its story—and October 21—the day Facebook’s demotion was finally lifted¹⁷⁵—over 30 million Americans cast their ballots in the election.¹⁷⁶ Roughly one-fifth of all votes in the 2020 presidential election were cast during the week that Facebook censored an article about the Biden family’s involvement in an influence-peddling scheme with foreign powers.¹⁷⁷ This story was particularly relevant to voters making a decision about who to trust in the Oval Office. And, to add to the potential significance of Big Tech’s decision to censor the most important story of the election, the outcome of the 2020 election was fewer than forty-five thousand votes—just 0.1 percent of the votes cast during the time Facebook censored the story.¹⁷⁸

A. Big Tech quickly censored the true *New York Post* story, believing it was “exactly” what the FBI had warned about for months.

The technical and policy teams within the platforms who had been meeting with the FBI immediately recognized the October 14 *Post* story as “exactly” the one the FBI had been warning about in detail.¹⁷⁹ Contemporaneous internal messages among Facebook employees show that the company’s first reaction was to suspect a Russian hack-and-leak operation. For example:

- 8:37 AM ET: “About what we expected in the hack/leak department [...] it’s pretty much exactly what we pregamed.”¹⁸⁰
- 8:42 AM ET: “It looks like exactly the hack/leak scenario we’d expected.”¹⁸¹
- 9:06 AM ET: “Can we check with FBI Delaware if they have anything on this [...] Article claims that FBI has had the HDD [hard drive] since December.”¹⁸²
- 9:09 AM ET: “Exact content expected for hack and leak.”¹⁸³

¹⁷⁵ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 123.

¹⁷⁶ Brittany Renee Mayes et al., *The U.S. hit 73% of 2016 voting before Election Day*, WASH. POST (Nov. 3, 2020); Catherine Park, *More than 14M Americans have voted early in 2020 presidential election, data shows*, FOX 10 PHOENIX (Oct. 14, 2020); James M. Lindsay, *The 2020 Election by the Numbers*, COUNCIL ON FOREIGN RELS. (Dec. 15, 2020).

¹⁷⁷ *Id.*

¹⁷⁸ Brittany Renee Mayes et al., *The U.S. hit 73% of 2016 voting before Election Day*, WASH. POST (Nov. 3, 2020); Catherine Park, *More than 14M Americans have voted early in 2020 presidential election, data shows*, FOX 10 PHOENIX (Oct. 14, 2020).

¹⁷⁹ Paul Waldman, *We came much closer to an election catastrophe than many realize*, WASH. POST (Nov. 18, 2020).

¹⁸⁰ *See, e.g.*, Internal messages among Facebook personnel (Oct. 14, 2020, 8:42 a.m.), Ex. 5.

¹⁸¹ Internal messages among Facebook personnel (Oct. 14, 2020, 8:37 a.m.), *see* Ex. 4.

¹⁸² Internal messages among Facebook personnel (Oct. 14, 2020, 8:42 a.m.), *see* Ex. 5.

¹⁸³ Internal messages among Facebook personnel (Oct. 14, 2020, 9:06 a.m.), *see* Ex. 6.

¹⁸⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 9:09 a.m.), *see* Ex. 7.

- 9:10 AM ET: “Right on schedule.”¹⁸⁴
- 9:14 AM ET: “[Facebook employee] is not in touch with the FBI on this. I’ll connect with Maryland and [Facebook employee] will raise at the FITF meeting today.”¹⁸⁵
- 9:33 AM ET: “FYI. Our legal team is reaching out to FBI on this.”¹⁸⁶
- 10:40 AM ET: “We’re enqueueing the content with demotion and doing outreach to 3PFCs. No updated info from FBI, no outreach from the Biden campaign.”¹⁸⁷
- 10:55 AM ET: “is this the Oct surprise everyone was waiting for?”¹⁸⁸
- 11:11 AM ET: “482 hours to first polls close...”¹⁸⁹

[REDACTED] (10/14/2020 05:42:26 PDT):
>It looks like exactly the hack/leak scenario we’d expected.

[REDACTED] (10/14/2020 06:09:51 PDT):
>Exact content expected for hack and leak, but sounds like so far, not much for us to do:
>
>1. No evidence of foreign interference operation
>2. Coming directly from press
>
>Sounds like next steps are to see if FBI contacts have any context for us, and to wait.
[REDACTED] (10/14/2020 06:10:33 PDT):
>Right on schedule.

[REDACTED] (10/14/2020 08:11:58 PDT):
>482 hours to first polls close . . .

“Exact content expected for hack and leak . . . Right on schedule.”
—Oct. 14, 2020 internal messages among Facebook personnel

Documents show that Facebook employees thought the story was “about what we expected in the hack/leak department,” but many also realized that there was “[n]o where [*sic*] near enough evidence to determine this is ‘part of a foreign govt influence op’ . . . other than [*sic*] circumstantial instinct.”¹⁹⁰ Meta’s President of Global Affairs Nick Clegg testified to the Committee and Select Subcommittee that the “team was very anxious to take a rapid decision,” and that the company had been preparing for “the risk of foreign interference” and for “hack-and-leak operations” for some time.¹⁹¹

¹⁸⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 9:10 a.m.), *see* Ex. 7.

¹⁸⁵ Internal messages among Facebook personnel (Oct. 14, 2020, 9:14 a.m.), *see* Ex. 6.

¹⁸⁶ Internal messages among Facebook personnel (Oct. 14, 2020, 9:33 a.m.), *see* Ex. 8.

¹⁸⁷ Internal messages among Facebook personnel (Oct. 14, 2020, 10:40 a.m.), *see* Ex. 7.

¹⁸⁸ Internal messages among Facebook personnel (Oct. 14, 2020, 10:55 a.m.), *see* Ex. 107.

¹⁸⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 11:11 a.m.), *see* Ex. 9.

¹⁹⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 8:37 a.m.), *see* Ex. 4; *see also* Internal Facebook Hack/Leak Policy Assessment (Oct. 20, 2020), Ex. 102.

¹⁹¹ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 123.

As confusion reigned, platforms immediately reached out to the FBI. For example, Facebook’s law enforcement outreach team contacted the FBI’s Baltimore field office, which was leading the Hunter Biden investigation.¹⁹² Critically, many of them had a prescheduled FITF meeting on the calendar for that day.¹⁹³ Internally, Facebook employees said that information from the FITF “would have huge implications on our next steps.”¹⁹⁴

Timestamp	Sender	Recipients	Message text
2020-10-14 06:05:00	[REDACTED] (whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	[REDACTED] -- looking at the calendar today, I see the FITF meeting. I don't recall whether I forwarded the invita to the rest of the group. Did you?
2020-10-14 06:40:20	[REDACTED] (@s.whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	I did not. I'll be able to dial in on the phone, but balancing a couple things today. Do we have an agenda for today?
2020-10-14 06:40:59	[REDACTED] (whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	The agenda is TBD. They may have OGA at the meeting, but not yet certain.
2020-10-14 06:41:57	[REDACTED] (whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	Think we want to get more info on the email leak in the NY Post from today and also on China based on the DNI's statement that they are much more prolific at ICs now than Russia

“[L]ooking at the calendar today, I see the FITF meeting. . . . Think we want to get more info on the email leak in the NY Post from today.”

—Oct. 14, 2020 internal messages among Facebook personnel

As Big Tech platforms began assessing how to implement their content moderation policies, including their newly updated hacked materials policies, they preemptively censored the story. Lacking evidence of a hack and leak, Facebook did not apply its newly developed hack-and-leak policy, and instead elected to contort its general misinformation policies to apply to the

¹⁹² Internal messages among Facebook personnel (Oct. 14, 2020, 9:14 a.m.), see Ex. 104.

¹⁹³ See, e.g., Emails among Elvis Chan and Google personnel (Sept. 29, 2020, 11:04 a.m.), Ex. 40; Emails among Elvis Chan and Facebook personnel (Oct. 4, 2020, 2:31 p.m.), Ex. 16; see also Internal messages among Facebook personnel (Oct. 14, 2020, 12:32 p.m.), Ex. 103; Internal messages among Facebook personnel (Oct. 14, 2020, 12:35 p.m.), Ex. 103; Internal messages among Facebook personnel (Oct. 14, 2020), Ex. 56; Internal messages among Facebook personnel (Oct. 14, 2020), Ex. 108.

¹⁹⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 1:19 p.m.); see Ex. 109.

New York Post story.¹⁹⁵ This meant that Facebook took two steps “in the ensuing hour or two” after the *Post* article was published: (1) it manually flagged the article for review by fact checkers, or enqueued it, and (2) manually buried the story in users’ feeds, or demoted it, by 50 percent for seven days.¹⁹⁶ Notably, Facebook’s automated processes were not triggered—the article was *manually* targeted for demotion and fact-checking by decision-makers on the Trust and Safety team.¹⁹⁷

```
Joel Kaplan <[REDACTED]@s.whatsapp.net>
We have to decide whether to undo this demotion. None of [REDACTED], [REDACTED], [REDACTED], [REDACTED], or I think this was appropriate/justified. But Unwinding will likely leak and be a story (conversely, doing things that might be perceived as anti-conservative, like demoting the content, never seem to leak).

Nick Clegg <[REDACTED]@s.whatsapp.net>
Yea I see - unwinding it now will unfortunately create more headaches than it's worth. Calling now

Joel Kaplan <[REDACTED]@s.whatsapp.net>
One thing to clarify—The difficult issue is that the demotion was NOT automatic (we manually demoted it). That’s what makes it hard—if it were automatic, it would be sort of an easy call not to intervene.
```

“The difficult issue is that the demotion was NOT automatic (we manually demoted it).”
—Oct. 14, 2020 internal messages between Vice President of Global Public Policy Joel Kaplan told then-Vice President of Global Affairs Nick Clegg regarding Facebook’s censorship of the *New York Post* story

Twitter, in contrast, decided to apply the company’s hacked materials policies despite the lack of specific evidence of a hack and leak, and began removing content and blocking the URL.¹⁹⁸ This initial censorship was seen as a stopgap to help the platforms limit the spread of the story by “slowing it down so that the researchers can take time to validate and peel through the layers around the release.”¹⁹⁹ Limiting the spread of the story also allowed platforms to ask for more information from the FBI.²⁰⁰ While companies wanted to wait for any additional information from the FBI to make their ultimate plans about how to handle the story about Biden family influence peddling, they began censoring the content immediately so they did not face backlash for inaction, particularly from “the press/left.”²⁰¹

¹⁹⁵ Transcribed Interview of Meta’s Director of Global Threat Disruption, H. Comm. on the Judiciary (May 16, 2023) (on file with Comm.) at 71-75.

¹⁹⁶ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 117-123; Internal messages among Facebook personnel (Oct. 14, 2020, 11:05 a.m.), Ex. 7.

¹⁹⁷ *Id.*; Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101; Internal messages among Facebook personnel (Oct. 14, 2020, 12:54 p.m.), *see* Ex. 9; Internal messages among Facebook personnel (Oct. 14, 2020, 5:25 p.m.), *see* Ex. 9

¹⁹⁸ Matt Taibbi (@mtaibbi), X (Dec. 2, 2022, 6:34 p.m.), <https://x.com/mtaibbi/status/1598822959866683394>.

¹⁹⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 11:09 p.m.), *see* Ex. 105.

²⁰⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 1:33 p.m.), *see* Ex. 106.

²⁰¹ Internal messages among Facebook personnel (Oct. 14, 2020, 6:26 p.m.), *see* Ex. 115.

B. Big Tech reached out to the FBI and the FBI hid key information.

While social media companies scrambled internally to analyze the possible foreign influence risks of the *Post* article, they turned to the FBI with questions. After all, the platforms had met with the FITF about foreign interference and potential hack-and-leak operations dozens of times throughout 2020 in anticipation of just such an event. In light of this practice of information sharing, the social media companies thought the FBI would provide details to help the platforms determine which of their content moderation policies to apply.

By happenstance, the FBI had at least three meetings with social media companies already scheduled for October 14, 2020—two bilateral FITF meetings (one with Facebook and one with Twitter) and a USG-Industry meeting—which provided the social media platforms with opportunities to directly confront the FBI for more information.²⁰²

1. The Twitter-FITF Bilateral Meeting

The first meeting occurred between the FITF and Twitter.²⁰³ An FBI analyst present at the meeting testified that Twitter’s Head of Trust and Safety, Yoel Roth, began the meeting by informing the FBI that Twitter had “seen the *New York Post* story about Hunter Biden’s laptop,” assessed it “as a Russian disinformation effort,” and planned to “suppress the story.”²⁰⁴ The analyst then testified that after an “awkward pause,” the FITF’s Russia Unit Chief made a few general comments about Russian disinformation and hack-and-leak threats, after which the analyst jumped in and, referencing the Hunter Biden laptop, said “that’s part of a separate matter.”²⁰⁵ However, according to testimony from two other senior FBI employees with knowledge of the meeting, that FBI analyst actually responded by saying something to the effect of “the laptop is real.”²⁰⁶ The analyst was quickly stopped by an FBI lawyer from the Office of

²⁰² USG-Industry Meeting invitation (Oct. 14, 2020, 6:00 p.m.), *see* Ex. 27; Email from Elvis Chan to Google personnel (Sept. 29, 2020, 11:04 a.m.), *see* Ex. 40; Scheduling emails between FBI and Facebook personnel (Oct. 4, 2020, 2:31 p.m.), *see* Ex. 16; *see also* Internal messages among Facebook personnel (Oct. 14, 2020, 12:57 p.m.), Ex. 79. Though there were four meetings scheduled for October 14, 2020, witness testimony and documents containing contemporaneous notes obtained by the Committee have confirmed so far that at least three took place: Twitter-FITF, Facebook-FITF, and the USG-Industry meeting. It is unclear whether the Google-FITF meeting took place and, if so, whether anyone from Google asked whether the laptop was real.

²⁰³ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 65-80; *see also* Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-33; Internal FBI meeting notes (Oct. 14, 2020), Ex. 44.

²⁰⁴ Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 32-33, 45.

²⁰⁵ *Id.* at 45; The separate matter referenced was the Hunter Biden investigation. While the analyst who confirmed the existence of the laptop in the Twitter-FITF meeting had known about the Hunter Biden investigation for several months, he learned that the FBI possessed Hunter Biden’s authenticated laptop only on the morning of October 14. Shortly after the *Post* story broke, a colleague at a nearby desk told the analyst and others that he was surprised to see the laptop’s contents in a media report because the laptop was part of the Hunter Biden investigation, which the colleague oversaw as a Program Manager covering the Baltimore Field Office. *Id.* at 28.

²⁰⁶ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 66-67; Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-33.

General Counsel, who said “no further comment” and shut down all subsequent conversation on the topic.²⁰⁷ In her interview before the Committee, Laura Dehmlow explained:

Q. Are you familiar with the October 2020 *New York Post* story on Hunter Biden’s laptop?

A. I am.

Q. Do you recall whether any of these social media companies you were meeting with asked you any questions about it?

A. I do.

Q. And what is your recollection? Who –

A. So I remember having a conversation with or being involved in a conversation with Twitter, and I honestly can’t recall if this was repeated to me – I might have been a few minutes late to the meeting – or if – or if I was – I actually overheard it.

But it was – it was relayed to me later that somebody from Twitter – I don’t recall who. I’m not sure who. Somebody from Twitter essentially asked whether the laptop was real. And one of the FBI folks who was on the call did confirm that, yes, it was before another participant jumped in and said no further comment.

Q. Was this individual affiliated with FITF?

A. Again, it was somebody from the Criminal Investigative Division who is embedded with us.

Q. So yes?

A. Yes.

Q. And did this question occur in the context of a bilateral meeting?

A. It did.

Q. Do you recall how soon after the story broke that this meeting occurred?

A. I don’t remember. I believe it was the same week, but I don’t remember the specific day.

²⁰⁷ *Id.*

Q. On that call with that IA [Intelligence Analyst] who's in the Criminal Investigative Division, that was the individual who said, "yes, the laptop is authentic"? Is that correct?

A. I don't believe it was that specific. Again, I don't recall hearing the conversation itself. I know it was relayed to me afterwards. But my understanding is that we confirmed that, yes, the laptop was a real laptop.

Q. And then you said another FBI individual came on and said, "No further comment."

A. Yes.

Q. Is that correct?

A. That's correct.

Q. Who was that individual?

A. It was some -- it was one of our lawyers who was on the call.²⁰⁸

The then-Russia Unit Chief of the FITF provided similar testimony to the Committee. He explained:

Q. During the FITF-Twitter call on the 14th, was there any discussion about the New York Post story or Hunter Biden's laptop?

A. I recall that when the question came up, an intelligence analyst assigned to the Criminal Investigative Division said something to the effect of, "Yes, the laptop is real." And then I believe it was an OGC attorney assigned to the FITF stepped in and said, "We will not comment further on this topic."²⁰⁹

2. The FBI's Internal Deliberations

FBI personnel testified that after the Twitter bilateral meeting, the FITF had internal discussions about how to respond to future questions about the contents of Hunter Biden's abandoned laptop and the *Post* article.²¹⁰ Various members of the FITF were involved in these

²⁰⁸ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-31.

²⁰⁹ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 66-67.

²¹⁰ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 65-80; *see also* Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-33.

conversations, and the FITF Section Chief was made aware.²¹¹ The FITF decided on this course of action because the laptop was a part of an ongoing investigation.²¹² The then-Russia Unit Chief of the FITF testified:

Q. Was there a decision made during these internal deliberations about how the FBI would respond going forward to future questions?

A. The characterization that is – it’s true, we absolutely talked about it, but more to firm up with everyone that it’s a longstanding policy. It wasn’t like this is something that wasn’t known, that we don’t talk about ongoing investigations.

So there was sort of that reiteration of, okay, if they ask about ongoing investigations, we don’t talk about ongoing investigations.

So from that point forward, again, we reiterated that it will be “no comment” when something like that comes up. So as you can imagine, that kind of continued that way.²¹³

For most of the Congress, when the Committee asked for the name of the FBI employee who made the decision that the FBI would have no comment to the social media companies going forward, the Justice Department forbid FBI witnesses from providing it. For example, during FITF Section Chief Dehmlow’s transcribed interview, she testified that she knew the identity of the FBI employee but the Justice Department prohibited her from disclosing the employee’s name:

Q. Who made the decision that the FBI would have no comment to the social media companies going forward?

DOJ Counsel. So I want to be clear. Ms. Dehmlow, obviously, can answer the question as long as it doesn’t get into internal deliberations or advice from a lawyer or anything.

A. Yeah, and, unfortunately I can’t answer that with any further detail on that advice.

Q. So you can’t tell us who made the decision?

²¹¹ *Id.*

²¹² *Id.*

²¹³ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 78-79.

- A. I can say there were internal deliberations with a number of parties, and then -- but I can't get into that further.²¹⁴

3. The Facebook-FITF Bilateral Meeting

Following the FITF's internal deliberations after the FITF-Twitter bilateral meeting, the FITF held a prescheduled bilateral meeting with Facebook and a full USG-Industry meeting, during which the FBI would not officially comment on questions about the laptop or the *Post* article.²¹⁵ The article was brought up in both meetings, but the FBI's "no comment" response ended the discussion and the meetings continued with other matters.²¹⁶ FITF Section Chief Dehmlow testified to the Committee and Select Subcommittee:

Q When the Facebook employee asked the question, do you recall exactly what they asked?

A. I don't.

Q. Do you know if it was about the laptop?

A. Yes. It was essentially whether or not we -- yes, it was something about the laptop. I don't remember -- I know that my answer was "no comment" because -- and the question doesn't stick in my mind because it was something about the laptop. And I said, "No comment."

Again, that was not my decision. It wasn't my final call. There were other agency, other departments, other FBI equities at stake, investigative equities, and so pretty typical for us to come to that conclusion.²¹⁷

Through unofficial FBI channels, Facebook personnel were able to obtain more information than the "no comment" they were offered in the FITF bilateral meeting. According to internal Facebook messages, an FBI official told Facebook that the laptop existed and that it was "part of a criminal matter."²¹⁸

²¹⁴ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 33.

²¹⁵ *Id.* at 65-80; *See also* Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-33.

²¹⁶ *Id.*; *see also* Internal messages among Facebook personnel (Oct. 14, 2020, 9:05 a.m.), Ex. 56; Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), Ex. 3.

²¹⁷ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 36.

²¹⁸ Internal messages among Facebook personnel (Oct. 14, 2020, 3:45 p.m.), *see* Ex. 7; Internal messages among Facebook personnel (Oct. 14, 2020, 8:23 p.m.), *see* Ex. 7; Internal messages among Facebook personnel (Oct. 14, 2020, 1:50 p.m.), *see* Ex. 108. The Russia Unit Chief of the FITF testified to the Committee that he did not know who at the FBI shared with Facebook that the laptop was part of a criminal matter. *See* Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 155.

██████████ (10/14/2020 12:45:15 PDT):
 >For awareness, additional context from ██████████ from the FBI meeting (somewhat sensitive so wasn't shared on the broader IPOC threads):
 >
 >Officially FBI said "The FBI has no information indicating foreign sponsorship, direction, or coordination of the hunter laptop issue" and ██████████ shared that with the US 2020 Esc thread...on the side in the same call however, they did confirm that FBI has the laptop and it's being review "as part of a criminal matter" but didn't give us details.

Timestamp	Sender	Recipients	Message text
2020-10-14 10:50:22	██████████ (s.whatsapp.net)	██████████ @s.whatsapp.net); System Message: ██████████	And I thought he said he could confirm it existed
2020-10-14 10:50:40	██████████ (s.whatsapp.net)	██████████ @s.whatsapp.net); System Message: ██████████ @s.whatsapp.net)	I distinctly remember he said it was a crim matter

"[T]hey did confirm that FBI has the laptop and it's being review [sic] 'as part of a criminal matter'"

—Oct. 14, 2020 internal messages among Facebook personnel

Despite the FBI's limited revelations as well as obvious facts, such as the failure of the Biden campaign to deny the laptop's authenticity, Facebook still chose to censor the *Post* story about Biden family influence peddling.²¹⁹

Joel D. Kaplan (10/14/2020 17:23:48 PDT):
 >I agree that Twitter is in a much more coherent position right now and thus easier to defend. I think either removal or labeling (on newsworthiness grounds) is defensible, if not equally well-received. I think a demotion tied to possible falsity, when none of the parties are actually suggesting the emails/images are false, at least so far-will be increasingly hard to defend. (The fact that the FBI apparently has the laptops may explain why no one in the Biden campaign is denying the authenticity).

"The fact that the FBI apparently has the laptop[] may explain why no one in the Biden campaign is denying the authenticity."

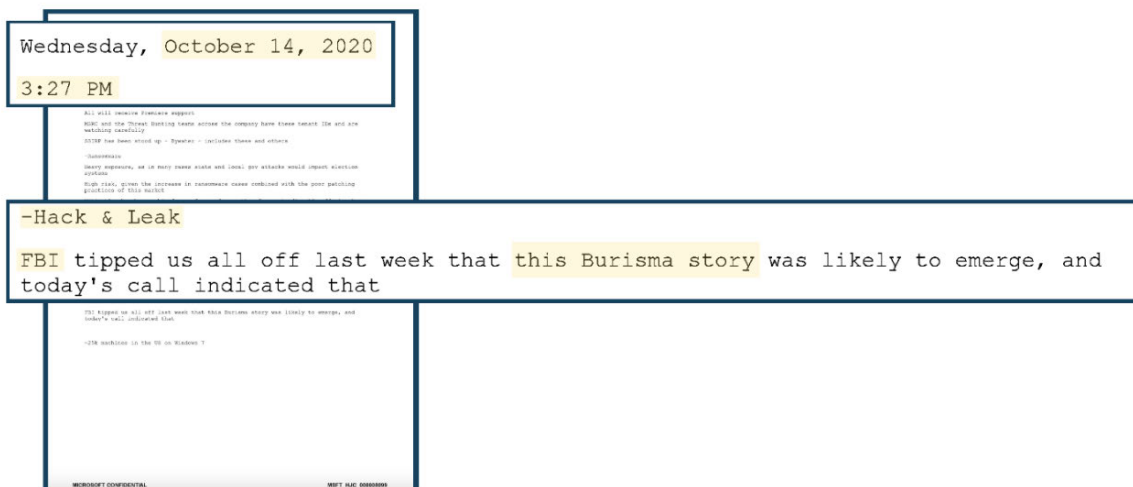
—Oct. 14, 2020 internal message from Facebook's Vice President of Global Public Policy Joel Kaplan to Facebook employees

²¹⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 8:23 p.m.), see Ex. 7.

4. The USG-Industry Meeting

The laptop again came up during the USG-Industry meeting scheduled for the afternoon of October 14.²²⁰ Like he did at the start of the Twitter-FITF meeting earlier that day, Twitter’s Head of Trust and Safety, Yoel Roth, once again shared that Twitter assessed the *Post* story to be Russian disinformation and intended to censor it.²²¹ Afterwards, Elvis Chan “pitched the response over” to the same analyst who had confirmed the laptop’s existence in the Twitter-FITF meeting; that analyst then responded in this USG-Industry meeting “no comment.”²²²

Notably, the analyst’s testimony contradicts Chan’s testimony from his *Murthy v. Missouri* deposition, in which Chan said he “was confident that [he] was not a party to any meeting with social media companies where Hunter Biden was discussed outside of the [Facebook-FITF bilateral meeting].”²²³ Likewise, Chan’s testimony that he had “no internal knowledge of [the Hunter Biden] investigation” was contradicted by the analyst, who testified to the Committee that he messaged Chan and “mentioned that there was an ongoing investigation” on the morning of October 14.²²⁴ The Justice Department continues to prohibit Chan from testifying to the Committee and Select Subcommittee.²²⁵



“FBI tipped us all off last week that this Burisma story was likely to emerge”
—Oct. 14, 2020, internal Microsoft notes on USG-Industry meeting

²²⁰ Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), *see* Ex. 3.

²²¹ Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 107-108.

²²² Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 38.

²²³ *Murthy v. Missouri*, No. 3:22-cv-01213, 2023 WL 43352270 (WD La. July 4, 2023) (Deposition of Elvis Chan), at 216.; *see also* Rep. Jim Jordan (@Jim_Jordan), X (Aug. 7, 2023, 10:11 a.m.), https://x.com/Jim_Jordan/status/1688553364211056640 (Facebook Files Part 4) (identifying other contradictions between Elvis Chan’s deposition testimony and documents obtained by the Committee and Select Subcommittee).

²²⁴ *Id.* at 214; Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 47.

²²⁵ *See* House Judiciary GOP (@JudiciaryGOP), X (Sept. 15, 2023, 4:17 p.m.), <https://x.com/JudiciaryGOP/status/1702778803037057503>.

In minutes from this USG-Industry meeting, describing the discussion of the *New York Post* story with the FBI, Microsoft wrote that the “FBI tipped us all off last week that this Burisma story was likely to emerge, and today’s call indicated that.”²²⁶

5. The FITF’s Follow-Up Discussions

The FITF’s Russia Unit Chief testified that during the course of the FITF’s meetings with social media platforms on October 14, 2020, he felt there was significant confusion around the *Post* article and that it “felt necessary to reach out to some of the more major companies and have a follow-up discussion with them,” particularly in light of the FBI analyst’s apparent confirmation of the laptop’s existence to Twitter.²²⁷ The Russia Unit Chief testified that he had a joint “follow-up discussion” with one representative each from Twitter, Facebook, Google, and Microsoft.²²⁸ In this meeting, he shared a prepared statement that he had “cleared” with superiors while “trying to skirt multiple policies and be within bounds legally.”²²⁹ The statement, he later explained to the Committee and Select Subcommittee, “was something to the effect of: The FBI has nothing in its possession to suggest that the laptop is a hack or a leak.”²³⁰ The Russia Unit Chief also testified that he rebuffed any potential follow-up questions with a response of “I’ve told you everything I can tell you on this matter.”²³¹ He testified that while the FBI “had more information” than just the fact that the laptop was not the product of a hack and leak, he could not share more due to the FBI’s policies.²³² He explained:

Q. After these FITF meetings take place, do you recall any follow-up outreach to you or other members of the FITF with the social media companies asking for more information?

A. Yes. Specifically, I felt that there was some confusion after this meeting or around that time because of that sort of comment that was made outside of policy, and then sort of having to cut it off.

Again, like, when we normally answer “no comment,” we can’t say, “because we have an open investigation,” because that, in and of itself, is revealing that we have an investigation.

So in this case, there was some confusion and I felt necessary to reach out to some of the more major companies and have a follow-up discussion with them.

Q. Which companies did you reach out to?

²²⁶ Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), Ex. 3.

²²⁷ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 83.

²²⁸ *Id.*

²²⁹ *Id.* at 84.

²³⁰ *Id.*; *see also* Internal messages among Facebook personnel (Oct. 14, 2020, 1:41 p.m.), Ex. 109; Internal messages among Facebook personnel (Oct. 18, 2020, 2:05 p.m.), Ex. 110.

²³¹ *Id.*

²³² *Id.* at 85.

A. I don't remember all of them. I'm pretty sure there was – I usually – I remember that it was, like, one person from each company, and I'm pretty sure Facebook, Google, and Twitter were represented.

Q. Did you do –

A. There may have been one or two other companies, but I don't remember. Maybe Microsoft. But I don't want to speculate, like, exactly which companies were sort of deemed pertinent or that we should give them somewhat of an update.

Chairman Jordan. What did you tell them?

A. So I told them -- I cleared a phrase, trying to skirt multiple policies and be within bounds legally and within policy, of what I could communicate to them, and came up with a phrase that I could share.

And the phrase, I don't have it verbatim, but it was something to the effect of: The FBI has nothing in its possession to suggest that the laptop is a hack or a leak.

And what I intended to communicate with that was that we did not know that the laptop was hacked. And I was very deliberate with my words because there's all sorts of things I could add that would either indicate that it's an ongoing investigation or somehow communicate to them that I know more than I did.

So at that time what I knew was the laptop was not hacked, because we had it in our possession. So I was very deliberate in that statement.

Obviously there was follow-on questions. We expected there would be follow-on questions. So also came up with sort of a follow-on statement. And, again, I don't know this verbatim, but something to the effect of: I've told you everything I can tell you on this matter. Sort of beyond "no comment" but basically no comment otherwise.

So obviously that phrase of we have nothing in FBI holdings to suggest that the laptop is hack-and-leak generally communicates that, as much as I can tell them, to try to clear up at least that element of the situation.²³³

The FITF's Russia Unit Chief testified that he felt an especially strong need to convey this statement to the major social media platforms because of the confusion from the Twitter-

²³³ *Id.* at 83-84 (emphasis added).

FITF meeting, in which an FBI analyst appeared to confirm the existence of the laptop with a statement “made outside of policy” before his superiors intervened.²³⁴ Had the analyst not spoken out of turn, it is unlikely that the FBI ever would have told the platforms anything about the true nature of the Hunter Biden laptop on October 14.²³⁵

Ultimately, in response to questions from Big Tech platforms—who had been primed for months to view this exact story as a Russian operation—about whether the *Post* article was a hack-and-leak operation, the FBI merely responded with “no comment” and “[t]he FBI has nothing in its possession to suggest that the laptop is a hack or a leak.”²³⁶ The FBI gave these answers even though it had possession of the laptop and had authenticated its contents and “knew [that] the laptop was not hacked.”²³⁷

C. Despite a lack of evidence, Big Tech continued to censor the story because of concerns about a potential Biden-Harris Administration.

Even after meeting with the FBI, social media platforms—particularly Facebook—doubled down on their decision to censor the *New York Post* story about Biden family influence peddling. While the FBI clarified that it had no specific evidence of a Russian hack-and-leak operation, it failed to disclose that it possessed and had authenticated the laptop—a key fact that likely would have ended any justification for censorship. Instead, because the FBI’s statements on the laptop failed to clarify the situation, and because the platforms knew that their “calls on this could colour the way an incoming Biden administration views us more than almost anything else,”²³⁸ major platforms, such as Facebook, censored the story.

1. Facebook

After the initial steps to apply Facebook’s misinformation policies by demoting and enqueueing the *Post* story for fact checking, a broader debate emerged on whether to invoke Facebook’s newly developed hacked material policies. This provision required there to be evidence of a hack, but contained an exception allowing materials considered “newsworthy” to remain on the site.²³⁹

Many Facebook employees were initially convinced that the article was the product of a hack and leak, but they had differing degrees of confidence. One employee wrote in an internal message that the story was the “exact content expected for hack-and-leak, but sounds like so far, there is not much for us to do: 1. No evidence of foreign interference operation[,] 2. Coming directly from press[.] Sounds like next steps are to see if FBI contacts have any context for us and to wait.”²⁴⁰

²³⁴ *Id.* at 83.

²³⁵ *Id.* at 83-85.

²³⁶ *Id.* at 83-84

²³⁷ *Id.*

²³⁸ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

²³⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 7:03 p.m.), *see* Ex. 7.

²⁴⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 9:09 a.m.), *see* Ex. 7.

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS /CN=28E865DE754F42D3ACBCF1C8052D0B8F>
To: [REDACTED]; Nick Clegg; [REDACTED]
Joel Kaplan;
Sent: 10/14/2020 9:56:34 PM
Subject: Message summary [{"otherUserFbId":null,"threadFbId":3940241416047689}]
Attachments: 121161847_1316086545401657_7329363007398542195_n.png;
121440254_1251840195175940_3016984524154928067_n.jpg;
121523296_4486187921454030_1191778544254324768_n.png;
121570689_337558230646825_1230117776855863053_n.png; sticker.png; sticker1.png

[REDACTED] (10/14/2020 06:03:24 PDT):
>'Morning, the NY Post published an article on what are allegedly leaked Hunter Biden-Burisma emails. SR ([REDACTED] and team) will send FYI.
>
><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 06:09:51 PDT):
>Exact content expected for hack and leak, but sounds like so far, not much for us to do:
>
>1. No evidence of foreign interference operation
>2. Coming directly from press
>
>Sounds like next steps are to see if FBI contacts have any context for us, and to wait.

[REDACTED] (10/14/2020 06:10:33 PDT):
>Right on schedule.

[REDACTED] (10/14/2020 07:01:16 PDT):
>Has it been referred to 3PFC?

Nick Clegg (10/14/2020 07:11:08 PDT):
>Looks fairly dodgy: <https://mobile.twitter.com/JuddLegum/status/1316376280103825409>

[REDACTED] (10/14/2020 07:15:15 PDT):
>Has not been referred yet, asked the team to refer now (but [REDACTED]'s assessment FWIW is that this is couched in a way that would be very difficult for 3PFC to rate).

[REDACTED] (10/14/2020 07:40:10 PDT):
>We're enqueueing the content with demotion and doing outreach to 3PFCs. No updated info from FBI, no outreach from the Biden campaign. Trump is running ads on the claim.

Joel D. Kaplan (10/14/2020 07:42:35 PDT):
>Do we always apply a demotion when we manually enqueue?

[REDACTED] (10/14/2020 07:43:02 PDT):
>No. We have standards for doing so and this met the test.

"Exact content expected for hack and leak . . . Right on schedule."

—Oct. 14, 2020, internal messages among Facebook personnel

Others turned immediately to the hack-and-leak framework as Facebook contemplated a response. In a separate message thread, one Facebook employee wrote "(1) we need to assess whether the content violates our policies against hacked materials (sounds like that is how Twitter is handling) and (2) is the content newsworthy?"²⁴¹ Another Facebook employee

²⁴¹ Internal messages among Facebook personnel (Oct. 14, 2020, 2:06 p.m.), *see* Ex. 9.

responded, after conducting an analysis, that the content “violates hacked policy,” subject to a determination of whether the content met the newsworthiness exception.²⁴²

```
[REDACTED] (10/14/2020 11:06:02 PDT):  
>Yes, I think (1) we need to assess whether the content violates our policies against  
hacked materials (sounds like that is how twitter is handling) and (2) is the content  
newsworthy?  
  
[REDACTED] (10/14/2020 11:06:25 PDT):  
>got it. moving out now.
```

```
[REDACTED] (10/14/2020 11:54:54 PDT):  
>what's the tldr?  
  
[REDACTED] (10/14/2020 11:55:42 PDT):  
>Violates hacked policy, we are not in favor of the NW allowance but are providing  
arguments on both sides
```

“[W]e need to assess whether the content violates our policies against hacked materials[.]”
—Oct. 14, 2020, internal messages among Facebook personnel

Facebook employees determined what qualified for the newsworthiness exception on a case-by-case basis by “weighing the public interest in seeing content against the risk of harm.”²⁴³ Stories that were uninteresting or harmful “would be removed,” while high-interest or low-harm stories “would either stay up or be labeled, depending on what [Facebook] decide[d].”²⁴⁴ One employee wrote that “it seems like the vast majority of the content obtained from the laptop of a candidate’s child would not be newsworthy,”²⁴⁵ and another concurred, writing that “both [public interest and harm] are pretty low here. It’s not really news that Hunter Biden has done drugs or engaged in other bad behavior.”²⁴⁶

Others in the company disagreed with this assessment. Joel Kaplan, Facebook’s Vice President of Global Public Policy, in particular, pushed back, writing: “Years of stories about the adult family members of Presidents would suggest that that content is newsworthy.”²⁴⁷

```
[REDACTED] (10/14/2020 16:17:04 PDT):  
>Yes, I would remove these images and link to the images. They are from the same source we  
determined is a hack under our rules and they do not have a public interest value.  
  
Joel D. Kaplan (10/14/2020 16:17:44 PDT):  
>We are going to remove the content of every publisher who published pictures of the  
candidate’s son doing drugs as not newsworthy? Years of stories about the adult family  
members of Presidents would suggest that that content is newsworthy.
```

“Years of stories about the adult family members of Presidents would suggest that that content is newsworthy”

—Oct. 14, 2020, internal message from Joel Kaplan to Facebook personnel

²⁴² Internal messages among Facebook personnel (Oct. 14, 2020, 2:55 p.m.), *see* Ex. 9.

²⁴³ Internal messages among Facebook personnel (Oct. 14, 2020, 7:44 p.m.), *see* Ex. 7.

²⁴⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 7:03 p.m.), *see* Ex. 7.

²⁴⁵ Internal messages among Facebook personnel (Oct. 14, 2020, 7:07 p.m.), *see* Ex. 7.

²⁴⁶ Internal messages among Facebook personnel (Oct. 14, 2020, 7:44 p.m.), *see* Ex. 7.

²⁴⁷ Internal messages among Facebook personnel (Oct. 14, 2020, 7:17 p.m.), *see* Ex. 7.

The Facebook employees also debated whether Hunter Biden could be considered a “prominent person in public life”—another consideration in Facebook’s policy on hacked materials.²⁴⁸ Many Facebook employees argued that Hunter Biden did not meet that threshold as the son of a presidential candidate who was not a public figure in his own right.²⁴⁹ Again, Joel Kaplan pushed back, writing: “I don’t really buy how the adult son of a VP who is being accused of influence peddling for a foreign company is not considered a prominent person in public life.”²⁵⁰

Joel D. Kaplan (10/14/2020 16:48:39 PDT) :
>I don't really buy how the adult son of a VP who is being accused of influence peddling for a foreign company is not considered a prominent person in public life. And if Fox concludes that misconduct is newsworthy—pretty consistent with the standards that have applied to adult children of presidents for decades—I don't really buy it's not newsworthy either.

“I don’t really buy how the adult son of a VP who is being accused of influence peddling for a foreign company is not considered a prominent person in public life.”

—Oct. 14, 2020, internal message from Joel Kaplan to Facebook personnel

Before the newsworthy analysis became determinative, though, Facebook would have had to conclude that the contents of the *Post* article were the result of a hack. The company quickly determined that it did not have evidence to conclude that the *Post* story was the result of a hack.²⁵¹

Because of the lack of evidence of a hack and leak, and because the FBI told Facebook that it also did not have any evidence to suggest such a conclusion, Facebook could not censor the story under its hacked materials policy.²⁵² Instead, the platform contorted its misinformation framework to trigger an automatic seven-day demotion while the story was sent to third-party factcheckers for their review. “Demotion is an appropriate and effective mitigation for what we’re almost certainly observing here,” one Facebook employee wrote in an internal chat.²⁵³ “We’re slowing it down so that the researchers can take time to validate and peel through the layers around the release.”²⁵⁴

Soon after Facebook’s decision to demote and enqueue content concerning Hunter Biden’s laptop and Biden family influence peddling, key decision-makers within the company began to express significant concerns with how the platform handled the situation and the public attention it was receiving. In an internal message thread, Vice President of Global Public Policy Joel Kaplan told then-Vice President of Global Affairs Nick Clegg that the company’s handling

²⁴⁸ Internal messages among Facebook personnel (Oct. 14, 2020, 7:46 p.m.), *see* Ex. 7.

²⁴⁹ *Id.*

²⁵⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 7:48 p.m.), *see* Ex. 7.

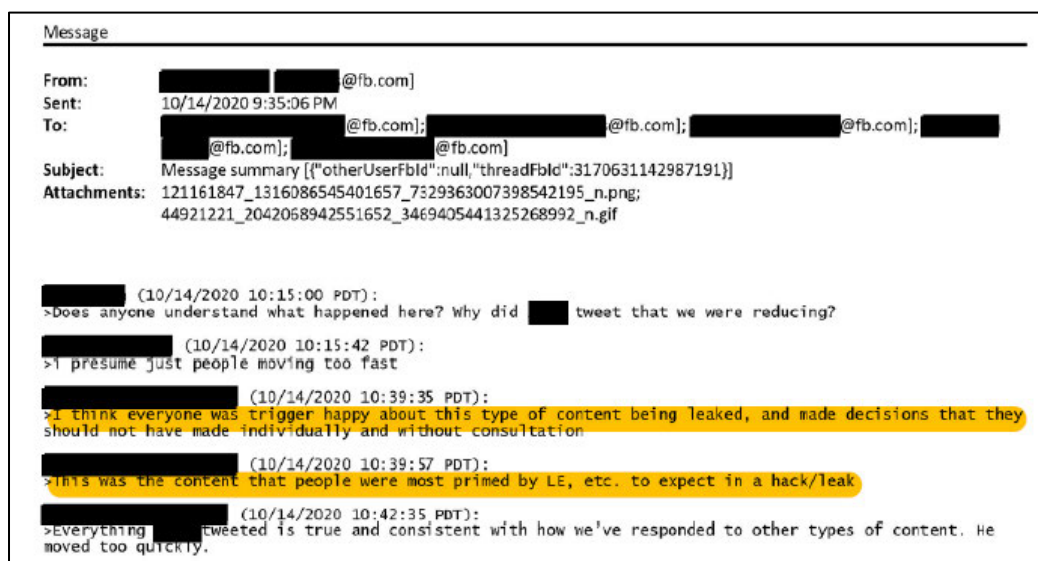
²⁵¹ Transcribed Interview of Meta’s Director of Global Threat Disruption, H. Comm. on the Judiciary (May 16, 2023) (on file with Comm.) at 71-75.

²⁵² *Id.*

²⁵³ Internal messages among Facebook personnel (Oct. 14, 2020, 11:09 p.m.), Ex. 105; *see also* Internal messages among Facebook employees (Oct. 14, 2020, 1:00 p.m.), Ex. 9.

²⁵⁴ *Id.*

of the *Post* article had been “outrageous.”²⁵⁵ These concerns were shared at lower levels of the company: another employee wrote, “I think everyone was trigger happy about this type of content being leaked, and made decisions that should not have been made individually and without consultation.”²⁵⁶ Facebook employees were so “trigger happy” because “this was the content that people were most primed by LE [law enforcement], etc. to expect in a hack/leak.”²⁵⁷ The FBI’s prebunking had worked.



“This was the content that people were most primed by LE, etc. to expect in a hack/leak”
 —Oct. 14, 2020, internal messages among Facebook personnel

The internal conflict over Facebook’s initial demotion of the content spurred discussion of potential alternative courses of action. In his transcribed interview before the Committee and Select Subcommittee, Meta’s President of Global Affairs Nick Clegg testified that there were suggestions to shorten the amount of time the story was demoted for from seven days to five or six, especially “in the absence of any fact checker finding fault with the content.”²⁵⁸ Clegg testified that COO Sheryl Sandberg was in favor of demoting the content for the full seven days, arguing that the company had already taken the action and should not reverse course; meanwhile CEO Mark Zuckerberg “was keen that we sort of cleaved as closely as possible” to the company’s standards, but “deferred very much” to Clegg.²⁵⁹

In an internal message thread, Facebook’s Vice President of Global Public Policy Joel Kaplan and then-Vice President of Global Affairs Nick Clegg discussed other specific concerns with Facebook’s handling of content related to allegations of Biden family influence peddling. Kaplan highlighted a perceived double-standard: Facebook allowed leaked content that was politically damaging to one party, like the *New York Times* story about President Trump’s tax

²⁵⁵ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

²⁵⁶ Internal messages among Facebook personnel (Oct. 14, 2020, 1:39 p.m.), *see* Ex. 115.

²⁵⁷ *Id.*

²⁵⁸ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 124.

²⁵⁹ *Id.* at 123-126.

returns, while demoting leaked content like the *Post* story that might be damaging to the other party.²⁶⁰

From: Sender Unspecified
To: Joel Kaplan <[REDACTED]@s.whatsapp.net>; Nick Clegg <[REDACTED]@s.whatsapp.net>; System Message <>
Sent:
Subject: (No Subject)
Attachments: rsmf.zip

Nick Clegg <[REDACTED]@s.whatsapp.net>
Which team is responsible for checking how/whether this could be a false hack/leak?
<https://mobile.twitter.com/JuddLegum/status/1316376280103825409>

Nick Clegg <[REDACTED]@s.whatsapp.net>
Ignore - see it's shared on 2020 thread

Joel Kaplan <[REDACTED]@s.whatsapp.net>
I think it's actually kinda outrageous that we are all freaking out about a NY Post cover story, enqueing and demoting because liberals are tweeting about it, with no evidence whatsoever. We did not do this when the NYT dunced an expose on Trump's tax returns citing leaked documents that they wouldn't even share.

“We did not do this when the NYT [dumped] [sic] an expose on Trump’s tax returns citing leaked documents that they wouldn’t even share.”

—Oct. 14, 2020, internal messages between Nick Clegg and Joel Kaplan

Similarly, as reflected in internal communications obtained by the Committee and Select Subcommittee, Facebook’s communications team understood that the traditional media employed a double-standard where Big Tech would face criticism *not* based on whether it fairly enforced its policies, but only on whether its enforcement hurt or helped President Trump.²⁶¹ As one Facebook Communications Vice President wrote as the company decided whether and how to censor the *New York Post* story: “Golden Rule: The Press is only as good to you as you are bad to Trump.”²⁶²

[REDACTED] (10/14/2020 19:50:24 PDT):
>I like it. Also, this thread is helpful

[REDACTED] (10/14/2020 19:50:29 PDT):
><https://twitter.com/kantrowitz/status/1316569785824612353?s=21>

[REDACTED] (10/14/2020 19:51:06 PDT):
>(Golden Rule: The Press is only as good to you as you are bad to Trump)

[REDACTED] (10/14/2020 20:15:26 PDT):
>I miss nuance

“Golden Rule: The Press is only as good to you as you are bad to Trump.”

—Oct. 14, 2020, internal messages from Facebook Communications Vice President

²⁶⁰ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

²⁶¹ Internal messages among Facebook personnel (Oct. 14, 2020, 10:51 p.m.), *see* Ex. 115.

²⁶² *Id.*

Internal Facebook messages also suggest that Facebook’s leadership decided to continue to demote the *New York Post* story because of public pressure and concerns about how changing course would affect the company’s relationship with a potential Biden-Harris Administration. In the message thread, Kaplan told Clegg that the platform needed to “decide whether to undo this demotion” but that “Unwinding will likely leak and be a story (conversely, doing things that might be perceived as anti-conservative, like demoting the content, never seem to leak).”²⁶³ Clegg agreed and responded by saying “unwinding it now will unfortunately create more headaches than it’s worth.”²⁶⁴

```
Joel Kaplan <[REDACTED]@s.whatsapp.net>
We have to decide whether to undo this demotion. None of [REDACTED], [REDACTED], [REDACTED], [REDACTED], or I think this was appropriate/justified. But Unwinding will likely leak and be a story (conversely, doing things that might be perceived as anti-conservative, like demoting the content, never seem to leak).

Nick Clegg <[REDACTED]@s.whatsapp.net>
Yea I see - unwinding it now will unfortunately create more headaches than it's worth. Calling now

Joel Kaplan <[REDACTED]@s.whatsapp.net>
One thing to clarify-The difficult issue is that the demotion was NOT automatic (we manually demoted it). That's what makes it hard-if it were automatic, it would be sort of an easy call not to intervene.
```

“Unwinding it now will unfortunately create more headaches than it’s worth.”
—Oct. 14, 2020, internal messages between Nick Clegg and Joel Kaplan

Later in the message thread Clegg recognized that Facebook’s “calls on this could colour the way an incoming Biden administration views us more than anything else.”²⁶⁵

```
Nick Clegg <[REDACTED]@s.whatsapp.net>
Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else...
```

“Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else”
—Oct. 14, 2020, internal messages between Nick Clegg and Joel Kaplan

Facebook seemed to be more concerned about its relationship with a potential Biden-Harris Administration than protecting the free speech of its users on its platform. So, while the FBI had confirmed that there was no evidence that the laptop was a Russian influence operation, Facebook continued with its decision to reduce the story by 50 percent on its platform for seven

²⁶³ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

²⁶⁴ *Id.*

²⁶⁵ *Id.*

days.²⁶⁶ During these seven days of Facebook censorship, over 30 million Americans voted in the 2020 presidential election—representing nearly one-fifth of the total votes cast.²⁶⁷ After nearly four years, in August 2024, CEO Mark Zuckerberg told the Committee and Select Subcommittee in a letter that Facebook “shouldn’t have demoted the story.”²⁶⁸

2. Twitter

The Twitter Files, a series of reports authored by independent journalists and released shortly after Elon Musk acquired the company, show that Twitter quickly began applying its hacked materials policy to the *Post* article after its release.²⁶⁹ Twitter’s enforcement actions included suppressing the article, removing links, applying safety warnings, and blocking the ability to send it via direct message.²⁷⁰ Twitter even locked then-White House Press Secretary Kayleigh McEnany out of her account for tweeting about the *Post* article and prevented the Committee from tweeting a link to the *Post* article.²⁷¹

Despite the quick and aggressive enforcement of the hacked materials policy, decision-makers at Twitter did have concerns about the platform’s response. Twitter’s Vice President of Global Communications asked whether Twitter could “truthfully claim that this [the *Post* article] is part of the [hacked materials] policy?”²⁷² Twitter’s Deputy General Counsel responded, acknowledging that the company probably needed “more facts to assess whether the materials were hacked,” but that “it is reasonable for us to assume that they may have been and that caution is warranted.”²⁷³ Like Facebook, Twitter censored the story, relying on the warnings it had received from the FBI prior to the story’s publication.

Some decision-makers at Twitter outright disagreed with the decision. Twitter’s former Head of Trust and Safety, Yoel Roth, testified to the Committee and Select Subcommittee that he reviewed the *Post* article and other relevant data, found it to be an ambiguous case, and thus “didn’t believe that the activity in question warranted enforcement under Twitter’s distribution of Hacked Materials Policy,” though he did believe the story should not be promoted.²⁷⁴ Mr. Roth testified to the Committee:

²⁶⁶ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 117-123; Internal messages among Facebook personnel (Oct. 14, 2020, 11:05 a.m.), *see* Ex. 7.

²⁶⁷ Brittany Renee Mayes et al., *The U.S. hit 73% of 2016 voting before Election Day*, WASH. POST (Nov. 3, 2020); Catherine Park, *More than 14M Americans have voted early in 2020 presidential election, data shows*, FOX 10 PHOENIX (Oct. 14, 2020); James M. Lindsay, *The 2020 Election by the Numbers*, COUNCIL ON FOREIGN RELS. (Dec. 15, 2020).

²⁶⁸ Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024).

²⁶⁹ Matt Taibbi (@mtaibbi), X (Dec. 2, 2022, 6:34 p.m.), <https://x.com/mtaibbi/status/159882295986683394>.

²⁷⁰ *Id.*; *see also* Noah Manskar, *Twitter, Facebook censor Post over Hunter Biden exposé*, N.Y. POST (Oct. 14, 2020).

²⁷¹ Steven Nelson, *WH press secretary locked out of Twitter for sharing Post’s Hunter Biden story*, N.Y. POST (Oct. 14, 2020); House Judiciary GOP (@JudiciaryGOP), X (Oct. 15, 2020, 9:13 a.m.), <https://x.com/JudiciaryGOP/status/1316728942523547653>.

²⁷² Matt Taibbi (@mtaibbi), X (Dec. 2, 2022, 6:34 p.m.), <https://x.com/mtaibbi/status/159882295986683394>.

²⁷³ *Id.*

²⁷⁴ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.) at 29.

Q. Once you found out about the story, again, to your recollection, walk me through what you did next.

A. Yeah. My first step was to ask a member of my team to develop what we called a policy assessment of the situation, a brief document that compiled the available evidence about what had happened and to make a recommendation under Twitter's rules for what the company should do.

I recall the situation at that point being pretty ambiguous. There was one article or perhaps a series of articles from the *New York Post* discussing the incident, but there wasn't a lot of available factual evidence at the time.

And so my recollection is that the member of my team working on the policy assessment struggled to identify what the right course of action here would be.

From that point, I discussed the issue with Del Harvey, who was my supervisor, and I represented to her that I didn't believe that the activity in question warranted enforcement under Twitter's Distribution of Hacked Materials Policy.

But, based on the available evidence that seemed to indicate a laptop of unknown provenance, a laptop that potentially had been broken into and the contents of which were being divulged, I made the recommendation to my supervisor that Twitter should take steps to not recommend or amplify the circulation of this content.

That is, I didn't recommend that Twitter delete the story or block its distribution entirely, just that Twitter take steps to not actively recommend it to users, which was a content moderation action we would take in ambiguous cases.

It's my understanding that Ms. Harvey discussed that with Ms. Gadde, and the decision was communicated to me at some point in first half of the day – but I couldn't exactly say when – that Ms. Gadde had decided that the content was a violation of Twitter's policy and that we should enforce against it under the Distribution of Hacked Materials Policy.²⁷⁵

In 2023, Twitter executives testified before Congress and called the company's treatment of the *Post* article a "mistake."²⁷⁶

²⁷⁵ *Id.* at 29-30.

²⁷⁶ Laura Romero, *Former Twitter execs tell House committee that removal of Hunter Biden laptop story was a 'mistake'*, ABC NEWS (Feb. 8, 2023); see also Kelsey Vlamis, *Twitter's former trust and safety chief said it was a mistake to censor the Hunter Biden laptop story: 'We didn't know what to believe'*, BUSINESS INSIDER (Nov. 30, 2022).

In November 2020, in the aftermath of the *Post* debacle, Twitter amended its policy on the distribution of hacked materials.²⁷⁷ First, Twitter changed the scope of the policy “to much more narrowly focus on situations in which there was a clearly confirmed hack that had taken place.”²⁷⁸ Second, the platform changed the kind of enforcement action it would take against hacked materials.²⁷⁹ Instead of removing the content that was the result of a hack, Twitter would merely apply a label to the content with additional information.²⁸⁰ Finally, Twitter added considerations to the policy about what kinds of sources were distributing the content at issue.²⁸¹ Twitter realized that its previous policy failed to account for mainstream media coverage of hacking stories and only focused on stopping the hackers themselves.²⁸² The new policy would “no longer remove hacked content unless it is directly shared by hackers or those acting in concert with them.”²⁸³ In explaining this new hacked material policy, Mr. Roth testified to the Committee:

Q Okay. Did Twitter during your time there have a policy as it related to hacked materials?

A. It did. Twitter had a Distribution of Hacked Materials Policy.

Q. And when was that policy first developed?

A. To the best of my recollection, it was developed and introduced in 2018.

Q. And did it change during your time at Twitter?

A. It did. The policy was substantially changed in 2020.

Q. And how did it change in 2020?

A. Following Twitter’s decision to restrict the *New York Post*’s coverage of Hunter Biden’s laptop, the company made a decision to change the scope of Hacked Materials Policy to much more narrowly focus on situations in which there was a clearly confirmed hack that had taken place and to change the remedy under the policy from being the removal of content to the application of labels that would provide additional information.

Q. And when did this change occur?

A. The updated policy was developed in October and November of 2020. I don’t remember exactly when it was introduced within that window. To the

²⁷⁷ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.) at 19-20.

²⁷⁸ *Id.* at 20.

²⁷⁹ *Id.* at 19-20.

²⁸⁰ *Id.*

²⁸¹ *Id.* at 21.

²⁸² *Id.*

²⁸³ Vijaya Gadde (@vijaya), X (Oct. 15, 2020, 10:06 p.m.), <https://x.com/vijaya/status/1316923557268652033>.

best of my recollection, it would have been in October 2020, but there were public announcements from the company that would have the exact date.

Q. Okay. And who at the company signed off on this change?

A. The policy was developed by me and by members of my team and ultimately was signed off on by Del Harvey and by Vijaya Gadde.

Q. Was there any part of the policy that took into account whether the source being hacked was a public figure?

A. No, that was not a consideration under the policy.

Q. Was there any part of the policy that covered whether the hacking itself was considered newsworthy?

A. That was one of the clarifications that was made in 2020, not whether the hack itself was newsworthy but the sources covering the content.

In the initial drafting of the policy, Twitter had been focused primarily on the activity that we saw in 2016, which were Russian hackers sharing it themselves. The hackers created Twitter accounts in their own personas and were directly laundering the content on social media using aliases like Guccifer 2.0 and DCLeaks.

And so we were focused on restricting that kind of direct distribution. Twitter didn't consider the possibility that the hack would take place or – excuse me – the disclosure of the hack would take place through a mainstream media outlet.²⁸⁴

But this policy update did not change the damage that had occurred: Twitter censored the article detailing the Biden family's influence peddling less than one month before an election, in part because Twitter had been primed by the FBI to expect the story would be part of a Russian hack-and-leak operation.

3. Other companies

The FBI's prebunking efforts notwithstanding, other social media platforms did not follow Facebook and Twitter's lead and came to different conclusions about how to act in response to the *New York Post* article.

In testimony before the Committee and Select Subcommittee, a member of Google's Threat Analysis Group (TAG) explained that shortly after the story was published, he and his

²⁸⁴ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.) at 19-21.

team conducted an analysis of whether the article or laptop were part of a Russian hack-and-leak operation.²⁸⁵ He testified that TAG “did not find any evidence that it was part of a foreign hack-and-leak operation.”²⁸⁶ Accordingly, YouTube “largely did nothing” to censor the *Post* story, per public reporting.²⁸⁷ The TAG member also testified that he consulted with other contacts in the industry, such as Yoel Roth at Twitter and personnel at Apple, to see if they had any evidence that the content was the result of a hack and leak, but found that those platforms had no “direct evidence of specific foreign involvement or hack-and-leak.”²⁸⁸ Google’s TAG staffer testified:

Q. Once [the *New York Post*] story was released, did your team conduct an assessment of whether materials from the story of the laptop were part of an either Russian hack-and-leak or hack-and-dump operation?

A. Yes.

Q. And what were your team’s findings?

A. My team’s findings was that we did not find any evidence that it was part of a foreign hack-and-leak operation.

Q. The story came out on October 14, 2020, early in the morning. . . . [D]o you recall how soon from when the story first broke – at least in the United States, it received a good amount of news coverage – from how soon the story first broke to when your team first began its assessment?

A. Pretty quickly.

Q. Same day?

A. Same day or day after probably.

Q. And then how long did it take your team to reach an initial assessment?

A. I’d say we did an initial assessment based on the information we had access to within a few – within hours.²⁸⁹

After completing its analysis, TAG communicated the finding to Google’s Vice President of Trust and Safety.²⁹⁰ The TAG staffer testified that later the same day, he was asked to join a call with the Vice President of Trust and Safety and “a number of other VPs and some lawyers

²⁸⁵ Transcribed Interview of the Senior Director of Google’s Threat Analysis Group, H. Comm. on the Judiciary (July 19, 2023) (on file with Comm.) at 23-26.

²⁸⁶ *Id.*

²⁸⁷ *A Misinformation Test for Social Media*, N.Y. TIMES (Oct. 21, 2020); see also Siva Vaidhyanathan, *The Hunter Biden story was a test for tech platforms. They barely passed*, THE GUARDIAN (Oct. 19, 2020).

²⁸⁸ Transcribed Interview of the Senior Director of Google’s Threat Analysis Group, H. Comm. on the Judiciary (July 19, 2023) (on file with Comm.) at 28.

²⁸⁹ *Id.* at 23-24.

²⁹⁰ *Id.* at 24.

from various products,” including YouTube, to provide a short verbal brief on TAG’s understanding of the article and to answer a few questions.²⁹¹ According to his testimony, questions during this call revolved around whether TAG had found evidence of a foreign hack and leak or heard of any evidence from industry partners.²⁹² The TAG staffer testified that he had not found any direct evidence of a foreign hack-and-leak operation, nor had he received any from industry contacts at other companies.²⁹³ He testified that “the only thing I heard was speculation. I hadn’t heard any evidence” from others in the industry.²⁹⁴

Today, Facebook and Twitter point to the FBI’s warnings when explaining their censorship decisions.²⁹⁵ But other companies’ approach shows that even with the FBI’s prebunking, if Facebook and others had followed their proper protocols, the *New York Post* story should have never been censored.²⁹⁶

Because the FBI primed platforms to look out for a Russian hack and leak targeting the Bidens and Burisma, when the *Post* story was published, some platforms jumped at the chance to censor it and failed to follow all of their applicable policies or the evidence. “[T]rigger happy” companies like Facebook and Twitter “made decisions that should not have been made individually and without consultation.”²⁹⁷

D. FBI continued to withhold information as Big Tech continued to reach out.

In the days following the publication of the *Post* article on Biden family influence peddling, social media platforms continued to seek new information or additional clarity from the FBI. Despite repeated requests, the FBI continually refused to provide more details.

²⁹¹ *Id.* at 26.

²⁹² *Id.* at 28.

²⁹³ *Id.*

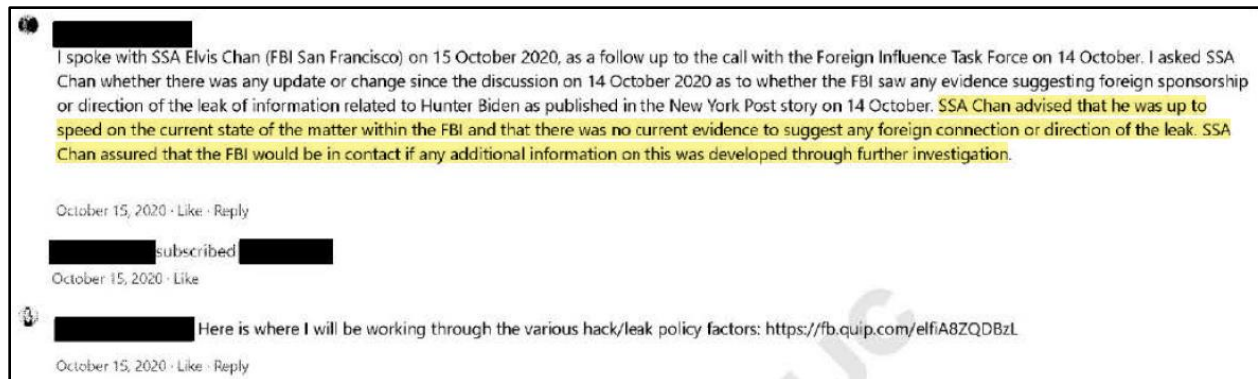
²⁹⁴ *Id.*

²⁹⁵ *See, e.g.*, Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[T]he FBI warned us about a potential Russian disinformation operation about the Biden family and Burisma in the lead up to the 2020 election. . . . It’s since been made clear that the [*New York Post*] reporting was not Russian disinformation, and in retrospect, we shouldn’t have demoted the story.”); Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

²⁹⁶ *See, e.g.*, Transcribed Interview of Google’s Director of Global Elections Integrity, H. Comm. on the Judiciary (May 22, 2023) (on file with Comm.) at 72. While Alphabet did not censor the *Post* story, they have generally been just as censorious as other platforms. The Committee and Select Subcommittee have demonstrated that in 2021, YouTube altered its content moderation policies at the behest of the Biden-Harris Administration. *See* STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE CENSORSHIP-INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITICS OF THE BIDEN ADMINISTRATION (Comm. Print May 1, 2024). More recently, Google Search’s autocomplete function suppressed information about the July 13, 2024 assassination attempt on President Donald Trump, and YouTube censored a video in which former FBI agent Marcus Allen, a Select Subcommittee witness, described his religious and political beliefs and prayed the rosary. *See* Letter from Rep. Jim Jordan, Chairman, H. Comm on the Judiciary, to Sundar Pichai, CEO, Alphabet (Aug. 5, 2024); Letter from Rep. Jim Jordan, Chairman, H. Comm on the Judiciary, to Sundar Pichai, CEO, Alphabet (Oct. 7, 2024).

²⁹⁷ Internal messages among Facebook personnel (Oct. 14, 2020. 1:39 p.m.), *see* Ex. 115.

On October 15, 2020, a Facebook employee (and former FITF official) called Elvis Chan “as a follow up to the call with the Foreign Influence Task Force on 14 October.”²⁹⁸ The Facebook employee reported back to his colleagues in an internal message thread that he “asked SSA Chan whether there was any update or change since the discussion . . . as to whether the FBI saw any evidence suggesting foreign sponsorship or direction of the leak of information related to Hunter Biden.”²⁹⁹ Chan told the Facebook employee that he (Chan) was “up to speed” on what the FBI knew and “that there was no current evidence to suggest any foreign connection or direction of the leak.”³⁰⁰ Chan assured the Facebook employee that he “would be in contact” if any additional information came to light.³⁰¹



“SSA Chan advised that . . . there was no current evidence to suggest any foreign connection or direction of the leak”
—Oct. 15, 2020, internal messages among Facebook personnel

The same day, key Facebook decision-makers communicated about hearing “murmurs from the IC [intelligence community] substantiating the Burisma hack” and “the concern that this would be dumped in an October surprise.”³⁰²

²⁹⁸ Internal messages among Facebook personnel (Oct. 15, 2020), *see* Ex. 117.

²⁹⁹ *Id.*

³⁰⁰ *Id.*

³⁰¹ Internal messages among Facebook personnel (Oct. 15, 2020), *see* Ex. 117; *see also* Emails between Facebook personnel and FBI personnel (Oct. 15, 2020, 10:03 a.m.), Ex. 118; Internal messages among Facebook personnel (Oct. 15, 2020, 5:14 p.m.), Ex. 119.

³⁰² Internal messages among Facebook personnel (Oct. 15, 2020, 8:56 a.m.), *see* Ex. 120.

Message

From: [REDACTED]@fb.com
 Sent: 10/15/2020 12:40:59 PM
 To: [REDACTED]@fb.com; Joel Kaplan [REDACTED]@fb.com; [REDACTED]@fb.com; [REDACTED]@fb.com; [REDACTED]@fb.com; [REDACTED]@fb.com
 Subject: Message summary [{"otherUserFbId":null,"threadFbId":3268602856582649}]

[REDACTED] (10/15/2020 05:56:35 PDT):
 >@silent FYI: starting to get stronger murmurs from the IC substantiating the Burisma hack by the GRU and the concern that this would be dumped in an October surprise. Nothing definite yet (and certainly nothing to share w/Rubio), but multiple sources beginning to strengthen the possible link to Russian actors.

Joel D. Kaplan (10/15/2020 05:57:59 PDT):
 >@silent The NY Post is running stories this am with emails about dealings with China. Are the rumors about the entire database of emails, or just about emails related to Burisma?

[REDACTED] (10/15/2020 06:00:23 PDT):
 >@silent about a specific, substantiated Burisma hack, then those emails behind combined with (a) other stolen Biden files; and (b) manipulated files mixed in among them.

[REDACTED] (10/15/2020 06:07:41 PDT):
 >@silent it's worth noting, though, there has been separate reporting of a hack of a prominent law firm that repped Biden, among others. That's another possible source of some of this info. I'll keep an eye as the community digs into this, and flag if we see analysis develop today.

“FYI: starting to get stronger murmurs from the IC substantiating the Burisma hack”
 —Oct. 15, 2020, internal messages among Facebook personnel

Three days later, on October 18, 2020, a Facebook employee reached out to the Russia Unit Chief of the FITF flagging a story furthering the false Russian hack-and-leak narrative, asking “does that change anything in your posture?”³⁰³ The Russia Unit Chief asked for the Facebook employee to give him a call to discuss, still failing to reveal that the FBI possessed and had authenticated Hunter Biden’s laptop.³⁰⁴

Facebook reached out to the FBI for additional information repeatedly. But rather than telling the companies that it was in possession of the laptop, the FBI repeatedly fed the platform its pre-approved message: “The FBI has nothing in its possession to suggest that the laptop is a hack or a leak.”³⁰⁵ Of course, the FBI did not have information suggesting the laptop was a hack or a leak; to the contrary, the FBI possessed and had authenticated the laptop, so “at that time . . . knew . . . the laptop was not hacked.”³⁰⁶

The FBI was not the only government actor that tried to muddy the waters surrounding the provenance of the laptop—the intelligence community also tried to falsely paint this story as a Russian influence operation. On October 19, 2020, fifty-one former intelligence officials issued

³⁰³ Emails between FBI staff to Facebook employee (Oct. 18, 2020, 1:36 p.m.), *see* Ex. 121; *see also* Allison Quinn, *Rudy’s ‘Russian Agent’ Pal Teases ‘Second Laptop’ With Hunter Biden Kompromat*, THE DAILY BEAST (Oct. 18, 2020).

³⁰⁴ *Id.*

³⁰⁵ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 84.

³⁰⁶ *Id.* at 83-84.

a statement falsely claiming that the Biden family influence peddling story bore all the hallmarks of a Russian influence operation.³⁰⁷ As the Committee has detailed in two reports coauthored with the House Permanent Select Committee on Intelligence, the statement was a coordinated influence operation set in motion by a senior Biden campaign official, now-Secretary of State Antony Blinken.³⁰⁸ High-level CIA officials—up to and potentially including then-Director Gina Haspel—were made aware of the statement before its publication.³⁰⁹

Companies asked repeatedly for more information about the laptop in the days following the *Post* article. The intelligence community colluded to falsely dismiss the story about Biden family influence peddling as Russian disinformation. And still, the FBI sat on the one fact that could have ended the confusion and set the record straight: the FBI was in possession of the laptop and had authenticated its contents. The FBI's failure to do so ensured that platforms continued to censor—a potentially election-altering decision.

³⁰⁷ STAFF OF H. COMM. ON THE JUDICIARY, SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, AND H. PERMANENT SELECT COMM. ON INTELLIGENCE, 118TH CONG., THE INTELLIGENCE COMMUNITY 51: HOW CIA CONTRACTORS COLLUDED WITH THE BIDEN CAMPAIGN TO MISLEAD AMERICAN VOTERS (Comm. Print June 25, 2024); STAFF OF H. COMM. ON THE JUDICIARY, SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, AND H. PERMANENT SELECT COMM. ON INTELLIGENCE, 118TH CONG., THE HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY OFFICIALS AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN VOTERS (Comm. Print May 10, 2023); *see also* Brooke Singman, *Biden campaign, Blinken orchestrated intel letter to discredit Hunter Biden laptop story, ex-CIA official says*, FOX NEWS (Apr. 20, 2023).

³⁰⁸ *Id.*

³⁰⁹ STAFF OF H. COMM. ON THE JUDICIARY, SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, AND H. PERMANENT SELECT COMM. ON INTELLIGENCE, 118TH CONG., THE INTELLIGENCE COMMUNITY 51: HOW CIA CONTRACTORS COLLUDED WITH THE BIDEN CAMPAIGN TO MISLEAD AMERICAN VOTERS (Comm. Print June 25, 2024) at 2.

IV. Epilogue: The fight against FBI election interference continues

The FBI, through the FITF, engaged in a months-long campaign to influence the 2020 election by prebunking the story about Biden family influence peddling, as supported by material recovered from Hunter Biden’s laptop. In over thirty meetings with social media platforms before October 14, 2020, the FBI primed the Big Tech platforms for exactly what would happen: shortly before the election, an established media outlet would publish an article about documents implicating the Biden family and Burisma in a far-reaching influence peddling scheme. Then, when the *Post* published that very story, Big Tech did what the FBI had been priming them to do for months and censored the story.

Since 2020, independent watchdogs have criticized the lack of protocol that allowed the FBI to successfully prebunk the true *Post* story. In July 2024, the Office of the Inspector General of the Department of Justice (DOJ OIG) found that the FITF operates in a “risky legal space” because social media companies may feel compelled to censor speech at its behest.³¹⁰ In the same report, the DOJ OIG concluded that in 2020, the Justice Department and the FBI did not have adequate guardrails governing the FITF’s interactions with Big Tech: “neither the Department nor the FBI had a specific policy or guidance applicable to information sharing with social media companies.”³¹¹

In January 2024, the FBI issued a Standard Operating Procedure (SOP) to govern its discussions with social media companies about content moderation and to formalize steps for sharing information with social media companies.³¹² This SOP requires FBI personnel to include a lengthy disclaimer telling social media companies that “no adverse action will be taken by the FBI based on your company’s decision about whether or how to respond” to the FBI’s communications.³¹³ FBI personnel also are not permitted to ask social media companies what actions have been taken in response to FBI communications.³¹⁴ The DOJ and FBI have refused to make the SOP publicly available and provide the American public with transparency into how the country’s most powerful law enforcement agency attempts to self-regulate its interactions with the companies hosting the modern town square.³¹⁵

While this SOP marks an improvement over the previous protocol (or lack thereof), it does not allay the Committee’s concern that the FBI may be continuing to coerce platforms to censor content. Platforms undoubtedly remain aware of the FBI’s enforcement powers and retaliation capacity. As Stanford Internet Observatory Director Alex Stamos testified to the

³¹⁰ OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, NO. 24-080, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE’S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS (July 2024), at 18.

³¹¹ *Id.* at 8.

³¹² *Id.*

³¹³ COUNTERINTELLIGENCE DIV., FEDERAL BUREAU OF INVESTIGATION, PROVIDING FOREIGN MALIGN INFLUENCE THREAT INFORMATION TO SOCIAL MEDIA PLATFORMS (STANDARD OPERATING PROCEDURE) (Jan. 2024), *see* Ex. 125.

³¹⁴ *Id.*

³¹⁵ *Id.*

Committee, “you can’t have a casual chat with an FBI agent when you’re an executive at a company. It’s not safe.”³¹⁶

The coordination meetings between the FBI and Big Tech stopped for a brief time after the U.S. District Court for the Western District of Louisiana issued, and a unanimous panel of the U.S. Court of Appeals for the Fifth Circuit largely affirmed, a preliminary injunction against the DOJ and FBI that prohibited them from coercing or significantly encouraging social media companies to censor lawful content.³¹⁷ This injunction prevented the FBI and various other federal agencies from having contact with Big Tech regarding the moderation of lawful content.

Unfortunately, the same meetings that led to the prebunking of the laptop story in 2020 have resumed in 2024.³¹⁸ After the Supreme Court stayed the lower courts’ injunction,³¹⁹ the FITF “resumed outreach” to social media companies sometime in early 2024.³²⁰ According to an FBI spokesperson, the purpose of this outreach is “to facilitate sharing information about foreign malign influence with social media companies”—the same mandate that facilitated the FBI’s prebunking of the *Post* story.³²¹ Given this past misconduct, it is concerning that the FBI is once again engaging in a similar manner with the entities responsible for administering the digital town square.

During the course of its investigation, the Committee has issued subpoenas for documents to agencies and companies involved in the prebunking campaign, including the DOJ, the FBI, and major social media and technology platforms.³²² Because the subpoenas are continuing in nature, they require these entities to turn over documents relating to the current, ongoing meetings on a rolling basis.

As these meetings have occurred in 2024, the Committee and Select Subcommittee have begun to receive documents from many platforms and agencies.³²³ These documents show that,

³¹⁶ Transcribed Interview of Alex Stamos, H. Comm. on the Judiciary (June 23, 2023) (on file with Comm.) at 188.

³¹⁷ Kevin Collier & Ken Dilanian, *FBI Resumes Outreach to Social Media Companies Over Foreign Propaganda*, NBC NEWS (Mar. 20, 2024).

³¹⁸ *Id.*

³¹⁹ *See* *Murthy v. Missouri*, No. 23A243 (23-411), 601 U.S. ___, (Oct. 13, 2023) (granting application for stay); *but see* *Murthy v. Missouri* 601 U.S. ___ (Oct. 20, 2023) (Alito, J., dissenting) (“At this time in the history of our country, what the Court has done, I fear, will be seen by some as giving the Government a green light to use heavy-handed tactics to skew the presentation of views on the medium that increasingly dominates the dissemination of news. That is most unfortunate.”).

³²⁰ Kevin Collier & Ken Dilanian, *FBI Resumes Outreach to Social Media Companies Over Foreign Propaganda*, NBC NEWS (Mar. 20, 2024).

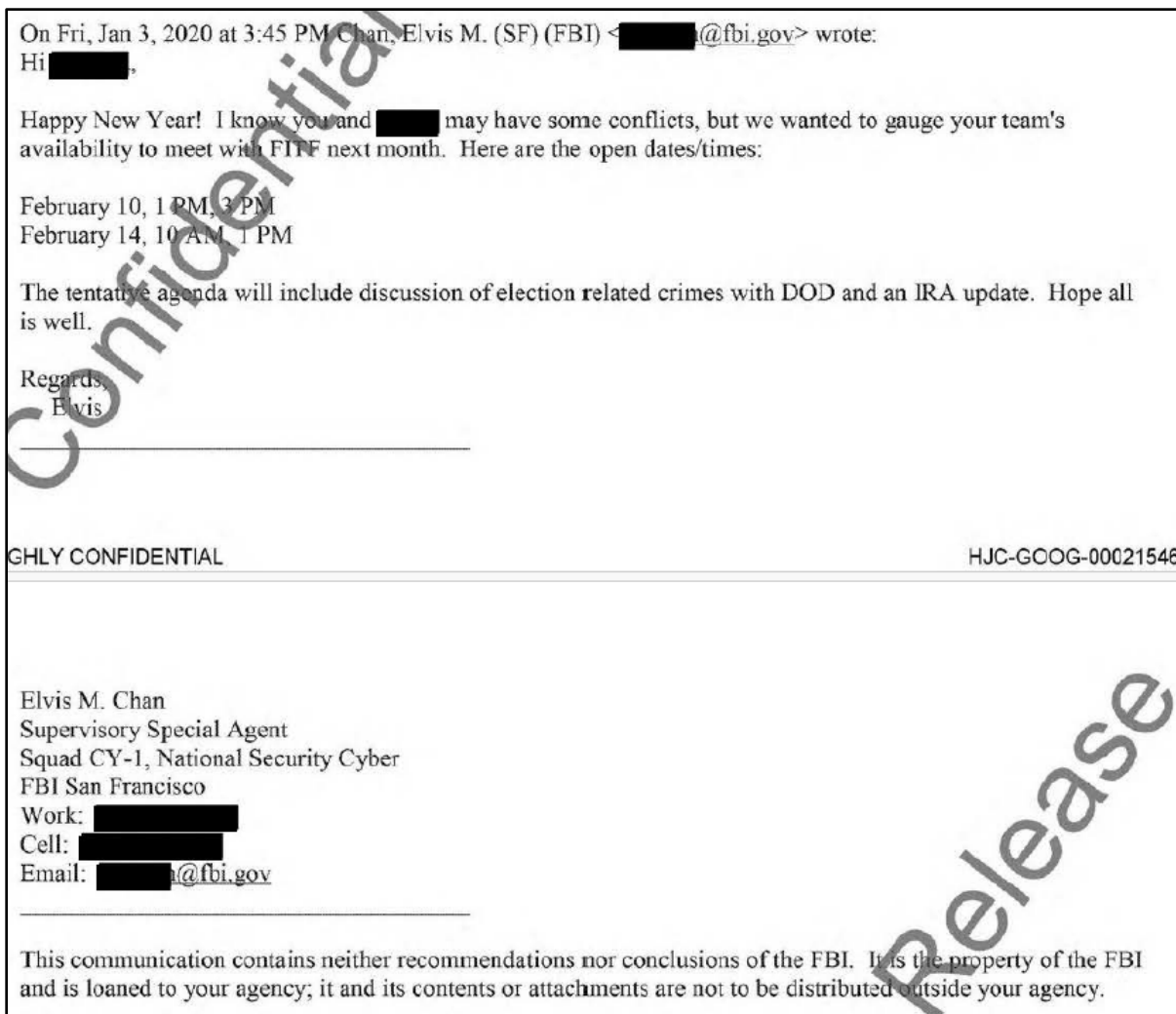
³²¹ *Id.*

³²² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., Dep’t of Justice (Aug. 17, 2023) (attaching subpoena) (on file with Comm.); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Jen Easterly, Dir., Cybersecurity and Infrastructure Security Agency (Apr. 28, 2023) (attaching subpoena) (on file with Comm.); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mark Zuckerberg, CEO, Meta (Feb. 15, 2023) (attaching subpoena) (on file with Comm.); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Sundar Pichai, CEO, Alphabet (Feb. 15, 2023) (attaching subpoena) (on file with Comm.); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Satya Nadella, CEO, Microsoft (Feb. 15, 2023) (attaching subpoena) (on file with Comm.).

³²³ *See, e.g.*, Email from FBI staff to Facebook personnel (Apr. 24, 2024, 10:26 a.m.), Ex. 122.

as in 2020, Elvis Chan remains the primary point of contact at the FBI for the meetings.³²⁴ They also show that the FBI, consistent with its new SOP, has added a more robust disclaimer at the end of its emails about the ostensibly voluntary nature of social media companies' interactions with the FBI.³²⁵

Previously, the FBI only sometimes included a disclaimer in its communications with Big Tech.³²⁶ When it did so, the disclaimer was only two sentences long and stated that the information provided contained “neither the recommendations nor conclusions of the FBI” and that the contents were the property of the FBI and were not to be distributed.³²⁷



“This communication contains neither the recommendations nor conclusions of the FBI. . . . it and its contents or attachments are not to be distributed outside your agency.”
—Jan. 3, 2020, email from Elvis Chan to Google, showing the FBI’s disclaimer at the time

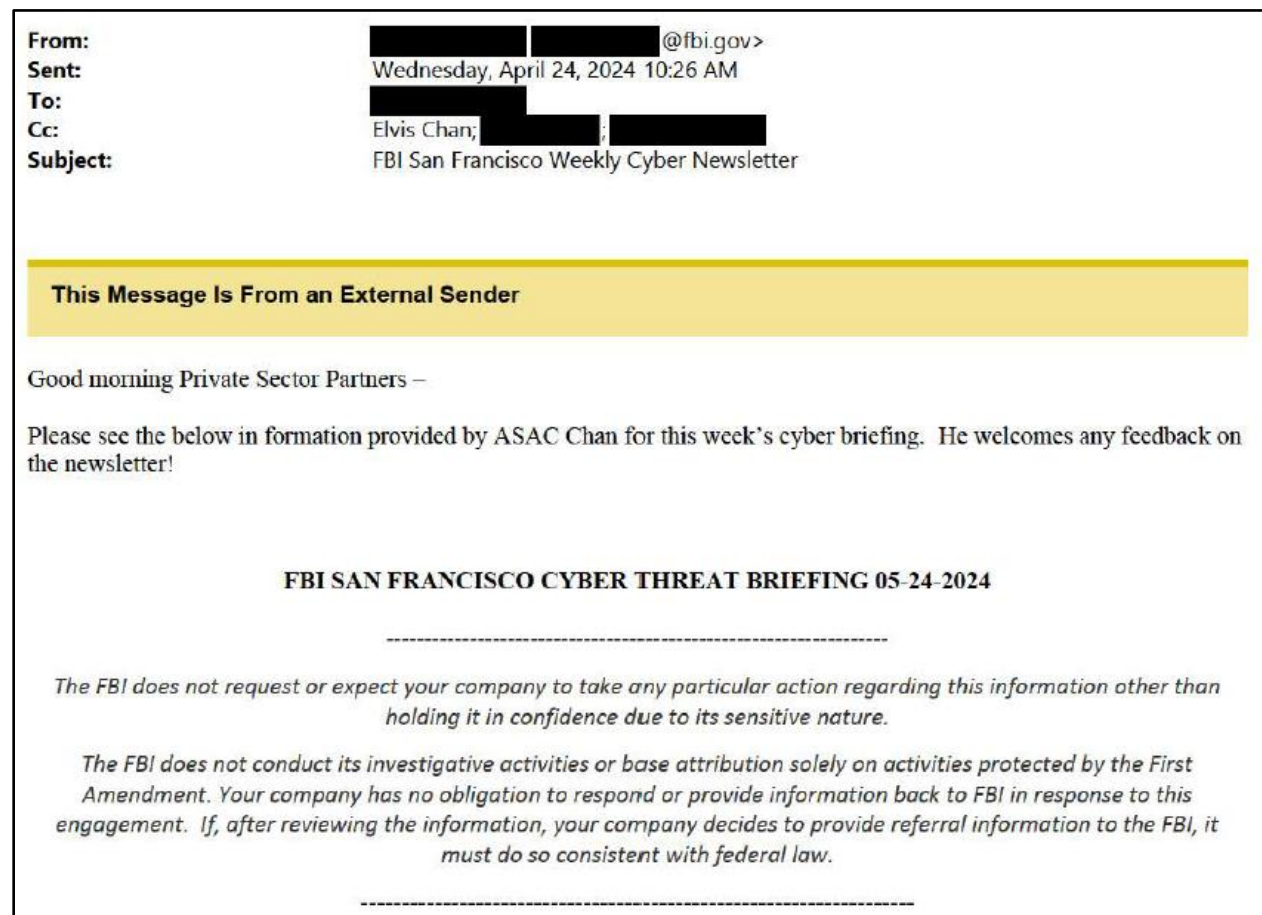
³²⁴ *Id.*

³²⁵ *Id.*

³²⁶ See Email from Elvis Chan to Google personnel (Jan. 6, 2020, 3:45 p.m.); Ex. 15.

³²⁷ *Id.*

In the wake of the Committee’s and Select Subcommittee’s oversight, and increased public attention on the FBI’s censorship activities in 2020, the FBI appended a new disclaimer to its emails with Big Tech. The new disclaimer is twice as long and attempts to assure social media companies that they have “no obligation to respond or provide information back to FBI” in response to its outreach.³²⁸



“The FBI does not request or expect your company to take any particular action regarding this information other than holding it in confidence due to its sensitive nature.”

—Apr. 24, 2024 email from FBI staff to Facebook personnel

The disclaimer, by itself, does not sufficiently resolve the First Amendment implications created by federal law enforcement engaging with Big Tech. Social media platforms, like any company, have a strong incentive to comply with requests from the FBI given its enforcement powers.³²⁹ So long as the FBI continues to engage with the companies that provide and oversee

³²⁸ Email from FBI staff to Facebook personnel (April 24, 2024, 10:26 a.m.); see Ex. 122.

³²⁹ See generally OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, NO. 24-080, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE’S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS (July 2024).

the digital town square, the risk of government infringement on Americans' free expression will remain.³³⁰

* * *

Documents and testimony obtained by the Committee and Select Subcommittee show the FBI's interactions with Big Tech in the months, weeks, days, and hours leading up to and surrounding the publication of the *New York Post*'s explosive October 14, 2020 story about Biden family influence peddling. Internal documents from Big Tech in particular show a months-long FBI campaign priming Big Tech companies to expect a Russian hack and leak about Hunter Biden and Burisma shortly before the election. When the true *Post* story matching the FBI's warnings emerged, the Big Tech companies followed the FBI's specific warnings and censored it, despite internal concerns that the story might not have been the product of a hack and leak. Even when it became clear the story was not Russian disinformation, Facebook and other platforms continued to censor the story out of concerns of how they may be viewed by a future Biden-Harris Administration. For a pivotal week, the most important story of the 2020 presidential election was censored.

The Committee and Select Subcommittee will continue to conduct oversight of the FBI's interactions with social media companies regarding content moderation. The modern town square must be free from direct and indirect government pressure. Government involvement will necessarily distort debate and lead to devastating policy outcomes.³³¹ A prosperous and functioning democracy depends on free expression so that ideas and viewpoints succeed and fail on their merits. The First Amendment demands nothing less.

³³⁰ *Id.*

³³¹ See STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE CENSORSHIP-INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITICS OF THE BIDEN ADMINISTRATION* (Comm. Print May 1, 2024).

V. Appendix

Table of Contents

Exhibit 1: Internal emails among Facebook personnel (Sept. 21, 2020).....	83
Exhibit 2: Internal message from Facebook personnel to Nick Clegg (Oct. 15, 2020).....	87
Exhibit 3: Microsoft internal meeting notes (Oct. 14, 2020).....	89
Exhibit 4: Internal messages among Facebook personnel (Oct. 14, 2020).....	91
Exhibit 5: Internal messages among Facebook personnel (Oct. 14, 2020).....	99
Exhibit 6: Internal messages among Facebook personnel (Oct. 14, 2020).....	102
Exhibit 7: Internal messages among Facebook personnel (Oct. 14, 2020).....	104
Exhibit 8: Internal messages among Facebook personnel (Oct. 14, 2020).....	117
Exhibit 9: Internal messages among Facebook personnel (Oct. 14, 2020).....	119
Exhibit 10: Internal messages among Facebook personnel (July 15, 2020).....	155
Exhibit 11: Statement from tech industry participants.....	157
Exhibit 12: Internal messages among Facebook personnel (Aug. 5, 2020).....	159
Exhibit 13: Internal messages among Facebook personnel (Sept. 20, 2020).....	166
Exhibit 14: Internal messages among Facebook personnel (Oct. 13, 2020).....	169
Exhibit 15: Emails between Google personnel and FBI staff (Jan. 6, 2020).....	173
Exhibit 16: Internal emails among Facebook personnel (Oct. 14, 2020).....	176
Exhibit 17: Email from FBI Counsel to Google personnel (Jan. 31, 2020).....	180
Exhibit 18: Emails between FBI and Microsoft personnel (Jan. 9, 2020).....	182
Exhibit 19: Email between Elvis Chan and Yahoo personnel (Feb. 12, 2020).....	185
Exhibit 20: Email between Elvis Chan and Yahoo personnel (Apr. 13, 2020).....	188
Exhibit 21: Emails between Elvis Chan and Google personnel (Apr. 14, 2020).....	191

Exhibit 22: Scheduling emails between FBI and Facebook personnel (May 12, 2020).....	193
Exhibit 23: Emails between Elvis Chan and Yahoo personnel (May 18, 2020).....	195
Exhibit 24: Scheduling emails between LinkedIn and FBI personnel (May 20, 2020).....	197
Exhibit 25: Emails between Elvis Chan and Yahoo personnel (July 14, 2020).....	200
Exhibit 26: Emails between Elvis Chan and Google personnel (July 14, 2020).....	204
Exhibit 27: Emails between Elvis Chan and Google personnel (July 14, 2020).....	208
Exhibit 28: Emails between Elvis Chan and Yahoo personnel (July 24, 2020).....	211
Exhibit 29: Scheduling emails between FBI and Facebook personnel (Aug. 10, 2020).....	215
Exhibit 30: Emails between FBI and Facebook personnel about FITF meeting attendees (Aug. 11, 2020).....	219
Exhibit 31: Scheduling emails between LinkedIn and FBI personnel (July 14 – Aug. 12, 2020)	224
Exhibit 32: Emails between Elvis Chan and LinkedIn personnel (Sept. 10, 2020).....	227
Exhibit 33: Emails between Elvis Chan and Google personnel (Sept. 10-11, 2020).....	231
Exhibit 34: Emails between Elvis Chan and Yahoo personnel (Sept. 14, 2020).....	234
Exhibit 35: Emails between Elvis Chan and Google personnel (Sept. 18, 2020).....	238
Exhibit 36: Scheduling emails between FBI and Facebook personnel (Sept. 10-21, 2020).....	240
Exhibit 37: Scheduling emails between Elvis Chan and LinkedIn personnel (Sept. 10-22, 2020)	246
Exhibit 38: Emails between Elvis Chan and Yahoo personnel (Sept. 24, 2020).....	250
Exhibit 39: Emails between Elvis Chan and Google personnel (Sept. 29, 2020).....	254
Exhibit 40: Emails between Elvis Chan and Google personnel (Sept. 29 – Oct. 14, 2020)	257
Exhibit 41: Emails between Elvis Chan and LinkedIn personnel (Sept. 29 – Oct. 13, 2020)	260

Exhibit 42: Emails from FBI to Big Tech participants scheduling FITF Bilateral meetings (Oct. 2020).....	263
Exhibit 43: Internal messages among Facebook personnel (Oct. 14, 2020).....	329
Exhibit 44: Internal FBI meeting summary notes from Twitter-FITF meeting (Oct. 14, 2020)	333
Exhibit 45: Emails between Google personnel and FBI staff (Apr. 20, 2020).....	358
Exhibit 46: Emails between Brian Scully and industry participants (May 11-12, 2020).....	361
Exhibit 47: Scheduling emails from Facebook personnel to industry group (May 13, 2020)	366
Exhibit 48: Internal Facebook readout of USG-Industry meeting (May 14, 2020).....	368
Exhibit 49: Agenda emails between industry participants (June 9, 2020).....	370
Exhibit 50: Scheduling email from Facebook personnel to industry group (June 9, 2020).....	373
Exhibit 51: Scheduling email from Google personnel to industry group (June 10, 2020).....	377
Exhibit 52: Internal messages among Facebook personnel (June 30, 2020).....	379
Exhibit 53: Internal Facebook readout of the USG-Industry meeting (June 10, 2020).....	382
Exhibit 54: Internal messages among Facebook personnel (July 1, 2020).....	384
Exhibit 55: Internal messages among Facebook personnel (July 10, 2020).....	386
Exhibit 56: Internal messages among Facebook personnel (Oct. 14, 2020).....	388
Exhibit 57: Scheduling email from Google personnel to industry group (July 15, 2020).....	394
Exhibit 58: Internal Facebook readout of the USG-Industry meeting (July 17, 2020).....	396
Exhibit 59: Scheduling email from Google personnel to industry group (Aug. 12, 2020).....	398
Exhibit 60: Internal Facebook readout of the USG-Industry meeting (Aug. 13, 2020).....	400
Exhibit 61: Agenda emails between industry participants (Sept. 11, 2020).....	408
Exhibit 62: Scheduling email from Facebook personnel to industry group (Sept. 11, 2020)	411

Exhibit 63: Agenda emails between CISA and Facebook personnel (Sept. 1-15, 2020).....	413
Exhibit 64: Scheduling email from Google personnel to industry group (Sept. 16, 2020)...	418
Exhibit 65: Internal Facebook notes about USG-Industry meeting (Sept. 16, 2020).....	420
Exhibit 66: Agenda email between CISA and Facebook personnel (Sept. 9, 2020).....	424
Exhibit 67: Agenda emails between CISA and Facebook personnel (Sept. 29 – Oct. 5, 2020)	426
Exhibit 68: Scheduling email from Facebook personnel to industry group (Oct. 7, 2020)...	429
Exhibit 69: Emails between Elvis Chan and Reddit personnel (Sept. 29, 2020).....	431
Exhibit 70: Emails between Elvis Chan and Yahoo personnel (Sept. 29, 2020).....	434
Exhibit 71: USG-Industry meeting invitation (July 8, 2020).....	438
Exhibit 72: USG-Industry meeting invitation (Sept. 9, 2020).....	440
Exhibit 73: USG-Industry meeting invitation (Oct. 21, 2020).....	443
Exhibit 74: USG-Industry meeting invitation (Oct. 28, 2020).....	447
Exhibit 75: Internal Facebook emails between Mark Zuckerberg, Sheryl Sandberg, and Facebook personnel (Oct. 5, 2020).....	451
Exhibit 76: USG-Industry meeting agenda (July 14, 2020).....	454
Exhibit 77: USG-Industry meeting invitation (July 14, 2020).....	457
Exhibit 78: Internal Facebook readout of USG-Industry meeting (Sept. 17, 2020).....	461
Exhibit 79: Internal messages among Facebook personnel (Oct. 14, 2020).....	463
Exhibit 80: Internal Facebook readout of USG-Industry meeting (Oct. 8, 2020).....	465
Exhibit 81: Internal messages among Facebook personnel (Sept. 9, 2020).....	467
Exhibit 82: Internal messages among Facebook personnel (Sept. 18, 2020).....	475
Exhibit 83: Internal messages among Facebook personnel (Sept. 21, 2020).....	479
Exhibit 84: Emails between Google personnel and Democratic National Committee staff (Aug. 5, 2020).....	485

Exhibit 85: Emails between Facebook personnel and DNI staff (Sept. 24, 2020).....	488
Exhibit 86: Aspen Digital Hack-and-leak Roundtable agenda (June 25, 2020).....	491
Exhibit 87: Aspen Digital Hack-and-leak Roundtable meeting readout (July 2, 2020).....	493
Exhibit 88: Memo from Aspen Institute roundtable	495
Exhibit 89: Emails from Aspen Institute staff to industry participants (July 14, 2020).....	499
Exhibit 90: Emails from Aspen Institute staff to industry participants (June 22, 2020).....	501
Exhibit 91: Emails between Aspen Institute and Facebook personnel (May 6-19, 2020)....	504
Exhibit 92: Emails between Aspen Institute, Facebook, and Stanford personnel (June 15-25, 2020).....	507
Exhibit 93: Emails between Aspen Institute and Facebook personnel (July 13, 2020).....	513
Exhibit 94: Email from Aspen Institute personnel to Facebook personnel (Sept. 28, 2020)	516
Exhibit 95: Aspen Digital Hack-and-leak Roundtable participant list (June 25, 2020).....	518
Exhibit 96: Email from Aspen Institute staff to industry participants (Aug. 2, 2020).....	521
Exhibit 97: Internal messages among Facebook personnel (Sept. 20, 2020).....	523
Exhibit 98: Email from Aspen Institute personnel to Facebook and Twitter personnel (Aug. 7, 2020).....	528
Exhibit 99: Emails from Aspen Digital staff to Roundtable participants (Aug. 12 – Sept. 1, 2020)	530
Exhibit 100: Aspen Digital Hack-and-Dump Scenario Outline (Sept. 2020).....	533
Exhibit 101: Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020).....	538
Exhibit 102: Internal Facebook Hack/Leak Policy Assessment (Oct. 20, 2020).....	542
Exhibit 103: Internal messages among Facebook personnel (Oct. 14, 2020).....	553
Exhibit 104: Internal messages among Facebook personnel (Oct. 14, 2020).....	555
Exhibit 105: Internal messages among Facebook personnel (Oct. 14, 2020).....	557

Exhibit 106: Internal messages among Facebook personnel (Oct. 14, 2020).....	560
Exhibit 107: Internal messages among Facebook personnel (Oct. 14, 2020).....	562
Exhibit 108: Internal messages among Facebook personnel (Oct. 14, 2020).....	568
Exhibit 109: Internal messages among Facebook personnel (Oct. 14, 2020).....	578
Exhibit 110: Internal messages among Facebook personnel (Oct. 14, 2020).....	580
Exhibit 111: Internal email between Facebook employees (Oct. 14, 2020).....	583
Exhibit 112: Email from Elvis Chan to Google personnel (Jan. 3, 2020).....	585
Exhibit 113: Internal messages among Facebook personnel (Oct. 14, 2020).....	587
Exhibit 114: Internal messages among Facebook personnel (Oct. 14, 2020).....	594
Exhibit 115: Internal messages among Facebook personnel (Oct. 14, 2020).....	596
Exhibit 116: Internal messages among Facebook personnel (Oct. 14, 2020).....	601
Exhibit 117: Internal messages among Facebook personnel (Oct. 14, 2020).....	606
Exhibit 118: Emails between Facebook personnel and FBI personnel (Oct. 15, 2020).....	610
Exhibit 119: Internal messages among Facebook personnel (Oct. 15, 2020).....	612
Exhibit 120: Internal messages among Facebook personnel (Oct. 15, 2020).....	618
Exhibit 121: Email from FBI staff to Facebook employee (Oct. 18, 2020).....	620
Exhibit 122: Email from FBI staff to Facebook personnel (April 24, 2024).....	622
Exhibit 123: Email between Atlantic Council personnel (July 20-31, 2020).....	625
Exhibit 124: Emails among tech industry participants (Sept. 15, 2020).....	629
Exhibit 125: FBI Standard Operating Procedure: Providing Foreign Malign Influence Threat Information to Social Media Platforms (2024).....	633