U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, DC 20530*

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Jordan:

This letter responds to your letter to the Department of Justice (Department), as well as your letter to the Federal Bureau of Investigation (FBI), both dated April 18, 2023, requesting documents and information related to the extent and nature of interactions with social media platforms. The Department and the FBI appreciate your interest in these matters and our shared commitment to protecting the constitutional freedoms and legal rights of the American people.

The Department is committed to equal justice under law. There is no place for partisanship in the enforcement of the law. The Department, including the FBI, does not investigate or take enforcement actions on the basis of protected viewpoints or content. The Department has described publicly how it works with private sector partners to share information and help those partners prepare to detect illegal conduct on their sites and platforms.[1] The FBI also shares information with social media companies about conduct that may violate their own terms of service, such as foreign malign influence operations and potential criminal activity, in an effort to allow them to protect themselves and their users. But it is the companies themselves that have the responsibility and authority to make decisions based on their own terms of service and how to apply those terms to protect their platforms and users.

[1] *See, e.g.*, U.S. Dep't of Just., Report of the Attorney General's Cyber Digital Task Force, July 2, 2018, https://www.justice.gov/archives/ag/page/file/1076696/download ("[T]he Department maintains strategic relationships with social media providers that reflect the private sector's critical role in addressing this threat. Social media providers have unique insight into their own networks and bear the primary responsibility for securing their own products, platforms, and services. The FBI can assist the providers' voluntary efforts to identify foreign influence activity and to enforce terms of service that prohibit the use of their platforms for such activities. This approach is similar to the Department's recent approaches in working with providers to address terrorist use of social media, and more traditional collaboration to combat child pornography, botnets, Internet fraud, and other misuse of digital infrastructure. By providing information about potential threats, the Department can help social media providers respond to malign use of their platforms, identify foreign influence operations on those platforms, share information across diverse products and services, and better ensure their users are not exposed to unlawful foreign influence.").

To be clear, while social media platforms have increased the ability to engage and connect across society, domestic and foreign actors also use social media and other platforms in furtherance of a variety of criminal schemes that risk grave harm to Americans. For years, foreign actors have exploited social media platforms to engage in covert actions to affect U.S. political sentiment and public discourse, sow divisions in our society, or undermine confidence in our democratic institutions to achieve strategic geopolitical objectives. Social media has also become another venue for threats of violence against government officials throughout our country to disrupt official responsibilities such as law enforcement or election-related duties. Americans, including children, are now dying from fake pills that are poisoned with fentanyl and marketed and distributed over social media. And human traffickers and other predators use websites and social media to advertise, schedule, and purchase sexual encounters with children and traffic in child sexual abuse material. The Department, including the FBI, is dedicated to protecting Americans from these threats. Engagement with social media companies is critical to disseminate information about potentially ongoing criminal activities and to share strategic and tactical information to help the companies identify national security threats on their platforms.

As we describe more fully below, as to disinformation, the FBI and the broader Department interact with online content and social media platforms in connection with (1) countering foreign malign influence operations; (2) election-related time, place, and manner disinformation; (3) combatting terrorists' use of social media platforms; (4) cyber-criminal activity; and (5) other crimes and security threats online.

Countering Foreign Malign Influence Operations

The identification and disruption of foreign malign influence operations is a longstanding and critical concern for the Department and the FBI. Foreign influence operations include covert actions by foreign governments intended to affect U.S. political sentiment and public discourse, sow divisions in our society, or undermine confidence in our democratic institutions to achieve strategic geopolitical objectives. These concerns are not hypothetical.[2] For example, in 2018, the U.S. government obtained an indictment of Russian individuals and entities for federal crimes in connection with efforts to interfere in the 2016 election—an effort the Russian defendants referred to as "information warfare."[3] In 2020, then-Attorney General Barr joined numerous other officials in a joint statement advising: "We continue to work with all 50 states, U.S. territories, local officials, political parties, ***and private sector partners*** to keep elections free from foreign interference."[4] The statement continued: "Americans must also remain aware that foreign actors continue to try to influence public sentiment and shape voter perceptions. They spread false information and propaganda about political processes and candidates on social media in hopes to cause confusion and create doubt in our system."

---

[2] *See id.* at 1−21.

[3] Press Release, U.S. Dep't of Just., Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System (Feb. 16, 2018), https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[4] Press Release, Fed. Bureau of Investigation, Joint Statement from DOS, DOJ, DOD, DHS, ODNI, FBI, NSA, and CISA on Preparations for Super Tuesday (Mar. 2, 2020) (emphasis added), https://www.dni.gov/index.php/newsroom/press-releases/item/2104-joint-statement-from-dos-doj-dod-dhs-odni-fbi-nsa-and-cisa-on-preparations-for-super-tuesday.

The FBI established the Foreign Influence Task Force (FITF) in 2017 to identify and counteract foreign malign influence operations targeting the United States. The FITF investigates and seeks to disrupt actions including:

- Attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions;
- Targeting U.S. officials and other U.S. persons through traditional intelligence tradecraft;
- Criminal efforts to suppress voting and provide illegal campaign financing; and
- Cyber attacks against voting infrastructure, along with computer intrusions targeting elected officials and others.

The FBI's Counterintelligence Division leads the FITF, which is composed of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions.

The FITF's work includes information and intelligence sharing with federal, state, and local government agencies, as well as with U.S. private sector entities. As to U.S. social media platforms, for example, the FBI and its Intelligence Community partners may determine through investigation and intelligence gathering that an account purporting to be controlled by a U.S. person is, in fact, controlled by a covert foreign malign actor. In such cases, the FBI may share with the pertinent social media company the indicators or selectors regarding that spoof account or that foreign actor.[5] The information might include IP addresses, email accounts, social media accounts, website domain names, or file hash values. We share this information to assist a social media company's own independent investigation into whether there is a violation of their own terms of service.

While the Department does not enforce private companies' own rules relating to content on their platforms, the operation of a social media account by a foreign malign actor under a false identity is typically a violation of companies' terms of service. When the FBI shares the information described above, it is the FBI's practice to convey to the company that the information is being shared for whatever action the company deems appropriate. The FBI does not direct or coerce companies to take any action, and companies do not necessarily disclose to the FBI whether they took any action on a posting or account. The FBI sometimes learns that a company has subsequently taken action on a posting or account based on the company's own investigation. Other times, the FBI learns that a company did not take such action—which it is free to do.

A decision by the FITF to share information with a U.S. social media platform about a foreign malign actor's social media activity is not based on the content or particular viewpoint expressed in a posting. Instead, this decision is based on the conclusion that the account is part of

[5] In the context of the FITF's work leading up to the 2020 election, the FBI only shared information concerning accounts it attributed with high confidence to a foreign-state actor.

a *covert* effort by a *foreign* malign actor. Although the FBI is responsible for investigating violations of the Foreign Agents Registration Act (FARA)—and Department attorneys are responsible for prosecuting those violations—the FITF does not identify for U.S. social media companies *overt* postings by hostile foreign actors. That is true regardless of the content. For example, the FITF would not identify for a U.S. social media platform a posting or account overtly attributed to RT (formerly known as "Russia Today"), which is registered under FARA as an agent of a Russian government entity and maintains accounts on social media, including Facebook and Twitter.

The FITF's efforts to combat foreign malign influence operations are consistent with the findings of the current and prior administrations regarding U.S. national security and foreign policy. On September 12, 2018, President Trump issued Executive Order 13848, which states that the President found "that the ability of persons located, in whole or in substantial part, outside the United States to interfere in or undermine public confidence in United States elections including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States." Based on this finding, the President declared a national emergency in accordance with Section 202(d) of the National Emergencies Act, 50 U.S.C. § 1622(d), with respect to the threat of foreign interference in or undermining public confidence in United States elections. On September 10, 2019, and then again on September 10, 2020, President Trump found that this threat continued and therefore sustained the national emergency he previously declared. President Biden also found that this threat continues and therefore continued the national emergency declaration on September 7, 2021, and September 7, 2022.

In instances where the FBI uncovers evidence of foreign malign influence, through the FITF or otherwise, the Department's National Security Division (NSD) may pursue an enforcement matter using appropriate civil and criminal tools. NSD is the litigating component that supervises prosecution of cases affecting or relating to national security, including any cases involving foreign malign influence. That work includes enforcement against covert information operations by foreign governments seeking to distribute disinformation through social media, as well as other covert influence operations that might violate various criminal statutes.

Election-Related Time, Place, and Manner Disinformation

Consistent with the U.S. government's compelling interest in maintaining the integrity of election procedures, the FBI and the broader Department are responsible for enforcing several categories of laws protecting election integrity. For example, posting objectively false information on social media concerning the time, place, or manner of elections with the intent to prevent qualified voters from effectively voting may be a violation of relevant criminal statutes. For this reason, separate from the work of the FITF, the FBI and the Department work to counter efforts to prevent qualified voters from casting their votes by deceiving them as to the time, place, or manner of an election.

The FBI is responsible for investigating potential violations of federal election law. As part of its election integrity efforts, in the days immediately preceding a presidential or mid-term

election, the FBI stands up "command posts" at FBI Headquarters and in its field offices across the country. These command posts facilitate the Department's ability to address federal election crimes, including but not limited to civil rights violations.

If an FBI field office is notified—for example, by a state election official—of a posting on a social media platform that contains objectively false information about the time, place, or manner of an election, the field office conducts an initial review as to whether the posting appears to constitute a criminal violation or evidence of such a violation. If so, the field office will relay the information to the FBI Headquarters command post. The FBI and Department personnel at the command post review the report and determine whether the posting appears to constitute a criminal violation, or at least evidence of a violation. If it does, the report is typically passed to the FBI's San Francisco Division command post, which then relays the information to the social media platform. Relaying the information for awareness to the social media platform helps minimize the scope of victims misled by the information in the first place, rather than solely relying on potential prosecution to protect the public. Again, the FBI does not pressure or coerce platforms into taking any action. The FBI relies on the platforms to take the actions they deem appropriate under their terms of service. Separately, if the conduct at issue implicates federal criminal statutes, following an investigation, the Department's Criminal or Civil Divisions may prosecute violations as appropriate for a given violation.

Combatting Terrorists' Use of Social Media Platforms

The Department, including the FBI, also works to protect our nation from violent terrorist attacks.

The FBI investigates potential terrorist conduct. Many terrorist organizations use digital communication platforms, including social media, to reach individuals they believe may be susceptible and sympathetic to violent terrorist messages. Terrorists disseminate propaganda and training materials—both physical and virtual—to attract easily influenced individuals around the world to their cause. With the broad distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable people of all ages across the globe.

No group has been as successful at drawing people into its perverse ideology as the Islamic State in Iraq and Syria (ISIS), which has proven dangerously competent at employing social media. ISIS uses traditional media platforms, as well as widespread social media campaigns to propagate its ideology. Like other foreign terrorist groups, ISIS advocates for lone offender attacks in the United States and Western countries. They use videos and other English language propaganda that have, at times, specifically advocated for attacks against civilians, the military, law enforcement, and Intelligence Community personnel.

While the FBI leaves the social media companies to police their own platforms' rules, promotion or facilitation of terrorist activity is routinely a violation of social media platforms' terms of service. In some circumstances, the FBI provides social media platforms with notice

that foreign terrorists or those promoting terrorism are using their platforms.[6] The FBI does so with the expectation that the platform will consider the information and independently determine whether to take any action it deems appropriate.

As in other contexts, the FBI's practice is to not pressure or coerce companies to take any action, and companies do not necessarily disclose to the FBI whether they took any action at all after receiving information from the FBI. Both Congress and the Executive Branch have for years recognized that private platforms' enforcement of their own terms of service can be important in opposing activities of foreign adversaries, such as the ISIS terrorist organizations, which have sought to use social media platforms to disseminate anti-American propaganda and encourage terrorist activity. And in our experience, social media companies appear to share our collective interest in combatting terrorism. They enforce their terms of service to prevent this activity on their platforms. For example, in a February 5, 2016 blog post, Twitter reported that, since mid-2015, it had suspended more than 125,000 accounts for threatening or promoting terrorist acts, primarily related to ISIS. [7]

Cyber-Criminal Activity on Social Media Platforms

Over recent years, the Department has seen a wider-than-ever range of malicious cyber actors threaten Americans' safety, security, livelihoods, and our confidence in a digitally connected world.

These threats include profit-driven efforts to steal trade secrets and military technology, as well as state-sponsored actors targeting critical infrastructure. For example, in 2021, the People's Republic of China engaged in a malicious cyber campaign using vulnerabilities in the Microsoft Exchange Server to target thousands of victims around the world.[8] Likewise, North Korean government actors have robbed central banks and cryptocurrency platforms, stealing hundreds of millions of dollars while evading international sanctions designed to limit their weapons programs.[9] Cyber-enabled threats also include individual lone actors who hack, extort, and disrupt American lives for personal gain.

The FBI is adept at investigating and disrupting malicious cyber activities by nation states, their proxies, and transnational criminal groups. As part of that disruption work, and while working in parallel to unmask and arrest perpetrators, the FBI collects and shares related intelligence with victims and other private sector partners.

---

[6] The FBI may learn of this activity through its national security investigations, from other members of the U.S. Intelligence Community, through foreign partners, or by other means. Social media activity by foreign terrorist organizations may or may not constitute a crime under U.S. law and may or may not be readily accessible to people in the United States. Some U.S. social media platforms, like Facebook, are popular across the globe, and foreign terrorist organizations or supporters may create Facebook groups in which they post terrorist propaganda in their native languages.

[7] *See, Combating Violent Extremism*, Twitter (Feb. 5, 2016), https://blog.twitter.com/en_us/a/2016/combating-violent-extremism.

[8] Press Release, U.S. Dep't of Just., Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research (Jul. 19, 2021), https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

[9] Press Release, U.S. Dep't of Just., North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

Cyber criminals, including nation state actors, frequently use social media platforms to commit crimes. Many of these platforms provide direct-messaging capabilities to users, which cyber criminals can use to conduct spear phishing attacks. Spear phishers target select groups of people with something in common. For example, the targets might work at the same company, bank at the same financial institution, attend the same college, or order merchandise from the same website. Using inside information that may have been obtained through hacking or by combing through websites, blogs, or social media platforms, cyber criminals send messages or post advertisements through the social media platform to targeted victims. They might offer urgent and legitimate-sounding explanations for why they need the victims' personal data or offer enticing goods or services in a method referred to as "malvertizing." Victims are asked to click on a link inside the message or advertisement that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, and similar information or are deceived into downloading malware. Once criminals have the victims' personal data, they can access their bank account, use their credit cards, create a whole new identity using their information, or otherwise leverage such data for further intrusion activity.

To combat cyber-crime, the FBI may in some circumstances notify social media platforms of spear phishing, malvertizing, or other fraud-enabling activities on their platforms. These notifications may be about general trends that the FBI is seeing or about particular incidents. The FBI's practice is not to pressure or coerce companies to take any actions, and companies do not necessarily disclose to the FBI whether they took any action on such fraud.

In addition, the FBI has on occasion been contacted by companies when cyber criminals appear to have taken over the company's social media account or created a fraudulent account in the company's name. Where a company is unsuccessful in reaching the social media platform hosting the relevant accounts, the FBI can relay the company's report to the social media platform directly.

When it comes to prosecuting crimes that arise from these activities, attorneys from various parts of the Department may become involved, including the Department's Criminal Division, NSD, and various offices of United States Attorneys around the country.

Other Crimes and Security Threats on Social Media Platforms

In addition to the examples described above, there may be other situations where it would be in the public interest to notify a social media platform of criminal conduct or security threats on its platform.

For example, if properly classified national security information is posted on a social media account and foreign adversaries become aware of it, that posting would reasonably be expected to cause damage to national security. In such a situation, the FBI may ask the social media platform to remove the classified information.

In other examples, individuals have posted explicit threats against federal officials on social media, or else posted personal information of law enforcement personnel and federal judges to encourage violence against those individuals. In some circumstances, the FBI has asked platforms to take down such postings.

Given the broad scope of the FBI's law enforcement and national security missions, the wide range of activity taking place on social media, and the constantly emerging threats from criminals, foreign adversaries, and other hostile actors, it is not possible to predict all the situations that might prompt us to notify social media platforms of criminal activity or security threats on their platforms.

Conclusion

We want to reiterate that the Department, including the FBI, does not investigate or take enforcement actions on the basis of protected viewpoints or content. Social media companies have independence and the ultimate authority to make decisions regarding their terms of service and their application to particular content and accounts.

To provide additional detail about the FITF's work, we are producing along with this letter the transcript (Bates-numbered DOJ-HJC-SM-0000001 to DOJ-HJC-SM-0000386) from a civil deposition provided last November by an FBI employee who has assisted in FITF matters. We respectfully request that the Committee consult with the Department before using information in the enclosed document in any way publicly. We also request the opportunity to review and apply redactions to any such disclosure to protect information, such as personally identifiable information, that the Department has a longstanding practice of not making public.

We are continuing our good faith search for documents responsive to the requests in your letters of April 18, 2023, to the Department and to the FBI. Should we identify additional responsive documents, we will provide them to you in a subsequent response.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

CARLOS URIARTE

Digitally signed by CARLOS URIARTE
Date: 2023.06.21 19:01:14 -04'00'

Carlos Felipe Uriarte
Assistant Attorney General

Enclosure

cc: The Honorable Jerrold L. Nadler, Ranking Member