No. 23-411

In the Supreme Court of the United States

VIVEK H. MURTHY, SURGEON GENERAL, ET AL.,
Petitioners,

v.

STATE OF MISSOURI, ET AL.,
Respondents.

On Writ of Certiorari to the United States Court of Appeals for the Fifth Circuit

BRIEF FOR UNITED STATES SENATOR MARK WARNER AS AMICUS CURIAE IN SUPPORT OF PETITIONERS

HASSAN A. ZAVAREEI
GLENN E. CHAPPELL
SPENCER S. HUGHES
Counsel of Record
GEMMA SEIDITA
SCHUYLER J. STANDLEY
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue
NW, Suite 1010
Washington, DC 20006
(202) 973-0900
shughes@tzlegal.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Legislatiave Materials

INTEREST OF AMICUS CURIAE[1]

Senator Mark Warner is Chairman of the United States Senate Select Committee on Intelligence (Intelligence Committee). With then-Chairman Richard Burr, he co-led a bipartisan committee investigation into foreign malign influence, ultimately releasing a five-volume bipartisan report in 2019 and 2020.

Senator Warner knows the threat that foreign malign influence campaigns pose to America, and he also knows social media platforms are the primary vector for modern, sophisticated influence campaigns. He considers it a national security imperative for government officials to engage with social media platforms about foreign malign influence targeting their users, particularly in the context of election influence and efforts to stoke social and racial tensions in the United States. Senator Warner understands foreign malign actors have repeatedly targeted the United States and its allies and will continue to do so. He believes government engagement with these platforms has successfully limited the damage of prior influence campaigns and that preserving effective channels for such engagement is essential to the Nation's security.

As Chairman of the Intelligence Committee, Senator Warner is keenly aware of the acute dangers posed by the Fifth Circuit's injunction. Russian influence operations have significantly escalated in

---

[1] No party or counsel for any party authored any part of this brief, and no person other than *amicus curiae* or his counsel made a monetary contribution intended to fund the preparation or submission of this brief.

recent years, with no sign of slowing down. Iran, China, Cuba, and Venezuela have targeted American elections through their own influence campaigns. Senator Warner believes any injunction here would prevent or chill communications between government officials and the social media platforms that unwittingly host foreign threats, thus imperiling our national security.

SUMMARY OF THE ARGUMENT

I. Foreign malign influence campaigns pose a severe threat to national security. The enormous growth of social media has given foreign actors a powerful tool for their campaigns, and many of them are seizing it. Election influence campaigns on social media roared into action before the 2016 election and have continued since, and other types of campaigns have followed.

Foreign malign influence campaigns seek to destabilize American society. Foreign actors such as Russia, Iran, China, and Cuba use social media to sow discord and heighten societal tensions in America. They accomplish this by operating social media accounts on popular platforms like Facebook, Instagram, Twitter, and YouTube impersonating American citizens, groups, and institutions.

These campaigns are serious. They are operated at the direction of foreign governments, and they utilize a blend of techniques designed to be deniable and avoid detection. Russia's campaigns have been honed by years of Russian investment and intelligence collection efforts. China's campaigns are growing in sophistication and scope.

Social media has become the most common vector of foreign malign influence campaigns targeting the

United States. The 2016 election cycle saw Russian influence campaign efforts explode across virtually every popular American social media platform and even obscure platforms. Russia employed "specialists" tasked with posting messages in English on social media at times of day corresponding with American time zones. For its efforts, Russia's 2016 campaign reached as many as 126 million Americans on Facebook alone, generating 76 million engagements on the platform as well as 187 million engagements on Instagram.

Russian operatives impersonated Americans on all sides of salient political and societal issues and communicated with presidential campaign members and journalists. They successfully impersonated the Tennessee Republican Party, dwarfing the legitimate party's Twitter follower count. When Russia expanded the scope of its social media focus to include marketing real-world events, it started with a "Confederate rally" before graduating into attempts to stoke real-world violence. One Russian operation involved promoting two simultaneous events to be held in front of the same Houston mosque—one called "Stop Islamization of Texas," and the other "Save Islamic Knowledge." The competing events escalated into confrontations and verbal attacks.

Foreign governments, including Russia, China, and Iran, are experienced in operating influence campaigns over social media, and there is no evidence they intend to stop. Foreign malign influence campaigns, including election influence campaigns in 2024, will only continue to grow in number, scope, and intensity.

II. The best way to combat foreign malign influence is cooperation between the public and private sectors. Threat sharing allows the government and social media companies to combine disparate data sets and share appropriate information. Through its legal authorities to collect foreign intelligence and counter foreign intelligence activity, the federal government frequently possesses sensitive information about foreign adversary operations targeting the United States, its allies, and U.S. national security interests. Social media companies want the government to share threats with them, and this information exchange has allowed them to identify and thwart multiple foreign malign influence campaigns on their platforms.

Threat sharing is a long-established counterintelligence practice. The government and social media companies established formal channels for threat sharing after the 2016 election to address national security matters and foreign threats, because social media platforms do not want to host foreign malign influence campaigns. On a bipartisan basis, the Intelligence Committee recognized in 2019 that information sharing "between the social media companies and law enforcement must improve, and in both directions." Social media platforms today are eager to cooperate with the government and one another to protect their users and combat foreign threats.

III. Any injunction here would prevent or limit the government's ability to communicate with social media companies and would leave the United States vulnerable to attack. Foreign malign influence campaigns have grown in number, scope, and

sophistication since 2016, and any progress gained through improved threat sharing processes may be entirely lost if the injunction is not lifted. Indeed, the injunction's chilling effect is still being felt even while stayed.

No alternative injunction-compliant methods of communicating with social media companies are effective. Real-time private engagement between frontline government officials and social media companies is now effectively impossible, as any communication by the former must be laboriously scrutinized.

And while it is not clear that public threat announcements would pass muster under the injunction, it *is* clear they would imperil U.S. intelligence sources, give advance notice to foreign adversaries about how the U.S. identified their campaigns, and exacerbate the risk to innocent Americans who unwittingly interacted with foreign social media accounts that the government later publicly identified. Threat sharing and other defensive briefings are the best ways to advance our essential counterintelligence mission while protecting highly sensitive sources and methods of intelligence collection and analysis.

ARGUMENT

I. Foreign malign influence operations over social media pose a severe threat to national security.

Foreign governments and non-state actors continually seek to harm American society through subversive and covert attempts to change our attitudes or perceptions, known as malign influence operations. These foreign governments and actors

repeatedly engage in malign influence campaigns because of their proven effectiveness, deniability, and simplicity.

Today, the explosion of social media has given foreign actors a powerful, malleable tool to blast malign influence messages across the country with unprecedented speed and scale. They use this tool to tremendous effect on the world's largest platforms like Facebook, Instagram, Twitter (now X), YouTube, and more.

The Intelligence Committee and U.S. Intelligence Community have studied foreign malign influence operations across social media. The results are profoundly concerning. Russia, Iran, and other actors have tried—and succeeded—in bending American behaviors and perceptions to their will by posting messages on social media platforms. Their content has generated billions of views and engagements, aided by unwitting Americans who thought they were sharing and promoting content by their peers. And these messages have proven their potential for stoking real-world violence here in the United States.

A. Malign influence operations are well known and effective means of destabilizing democratic governments.

Foreign entities have conducted malign influence operations for decades or more across the globe, and they have proven effective. The Intelligence Community developed a lexicon to describe their different types. "Foreign malign influence" operations include subversive, covert activities by foreign governments, non-state actors, or their proxies to affect another nation's popular or political attitudes, perceptions, or behaviors. Nat'l Intel. Council,

Intelligence Community Assessment (ICA) 2022-27259-A: Foreign Threats to the 2022 US Elections (Dec. 23, 2022), at iii (2022 Election ICA). Foreign malign influence campaigns include efforts to sow division, undermine democratic practices and institutions, or steer policy toward the foreign actor's objectives. *Id.*

The Intelligence Community distinguishes this from more benign acts of foreign influence, including overt appeals allowing Americans to evaluate the message on the merits with the understanding the speaker is a foreign government or non-state actor. Through laws such as the Foreign Agent Registration Act, 22 U.S.C. §§ 611 *et seq.*, and the Lobbying Disclosure Act, 2 U.S.C. §§ 1601 *et seq.*, the federal government established clear avenues for foreign actors to engage in overt and declared foreign influence—with less risk of distorting the U.S. political process through covert means. Foreign malign influence subverts these established legal processes.

"Election influence" campaigns, a subset of foreign malign influence, include overt and covert efforts by foreign governments or their agents intended to affect an election. 2022 Election ICA at ii. But not all (or even most) foreign malign influence campaigns target elections. A foreign influence campaign can sow discord over social issues, like race or immigration, without seeking to affect the outcome of a particular election. Foreign malign influence instead more broadly seeks to "sow division . . . or steer policy and regulatory decisions in favor of a foreign actor's strategic objectives." *Id.* at iii.

Recent foreign malign influence operations that have targeted the U.S. share three salient characteristics. They exploit and heighten existing tensions and undermine faith in democratic institutions; they are run by highly trained intelligence operatives at the direction of the governments of our adversaries; and they are often exceedingly sophisticated, incorporating a blend of techniques.

Destabilizing American society is a key objective for foreign malign influence operations. In its 2016 election influence campaign, Russia's goals were to undermine Americans' public faith in the democratic process and affect the outcome of election contests. Nat'l Intel. Council, ICA 2017-01D: Assessing Russian Activities and Intentions in Recent US Elections (Jan. 6, 2017), at ii (2016 Election ICA). The Intelligence Committee found that Russia's 2016 election influence efforts were part of a "broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society." S. Rep. No. 116-290, 116th Cong., 2d Sess., *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, S. Select Comm. on Intel., Vol. 2 at 5 (Nov. 10, 2020) (Intel. Comm. Rep.). Russia's operations primarily came from the Internet Research Agency (IRA), a Saint Petersburg-based organization of "specialists" directed and financed by Yevgeniy Prigozhin, a Russian oligarch closely tied to Vladimir Putin. *Id.* The IRA targeted "socially divisive issues" such as race, immigration, and gun rights "in an attempt to pit Americans against one another and against their government." *Id.* at 6.

Similarly, Iran's 2020 election influence campaign primarily focused on "sowing discord" and "exacerbating" America's "societal tensions." Nat'l Intel. Council, ICA 2020-00078D: Foreign Threats to the 2020 US Federal Elections (Mar. 10, 2021), at 5 (2020 Election ICA). Iran targeted the response to the Covid-19 pandemic, economic recession, and civil unrest, and it continues to use influence operations in its attempts to "inflame domestic tensions" in the U.S. *Id.* at 6.

China, Russia, Cuba, and Iran each engaged in election influence campaigns targeting the 2022 elections. 2022 Election ICA at 1, 11. Their primary goals were to "heighten sociopolitical divisions" and "tensions." *Id.* at 1. China and Cuba also both sought to "support" or "undermine" specific candidates based on their policy positions. *Id.* Russia's election influence activity intended to "stoke anger, provoke outrage and protest, push Americans further away from one another, and foment distrust in government institutions." Intel. Comm. Rep., Vol. 2 at 6. And China has sought to "magnify US societal divisions," with messaging focused on divisive "social issues" like "abortion and gun control." 2022 Election ICA at 2.

Foreign malign influence campaigns are operated at the direction of adversary governments. The Intelligence Committee found that the Russian government "tasked and supported" the IRA's 2016 election influence campaign. Intel. Comm. Rep., Vol. 2 at 5. Russia's intelligence services, including the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), "exploited" social media platforms as another "vehicle" for Russian influence operations. *Id.* at 7-8.

The Chinese government is also directly involved in malign influence campaigns. Since 2020, senior Chinese leaders have issued "broad directives to intensify efforts" to influence American "policy and public opinion" in its favor. 2022 Election ICA at 2. Chinese intelligence services, diplomats, and "online influence actors" sought to "undermine or promote specific candidates" from both major U.S. political parties in the 2022 election. *Id.* at 3.

Iranian leaders evaluated options to distribute propaganda and employ actors to post on social media platforms in the lead up to the 2022 U.S. election, in addition to establishing front news agencies to interact with American media outlets. *Id.* at 6. In October 2022, Twitter exposed three Iran-based influence networks on its platform. *Id.*

These influence operations involve a blend of techniques, often informed by intelligence tradecraft, making it difficult for them to be identified. Although Russia's influence campaigns are approved at the highest levels of its government up to and including Vladimir Putin, they are "designed to be deniable" and rely on a multifaceted mix of actors and tactics. 2016 Election ICA at 2. Russian campaigns are informed by sophisticated intelligence collection efforts, honed by years of Russian investment in former Soviet states, and they feature data Russia has obtained from cyber operations, intrusions into American election boards, and overt propaganda. *Id.*

Similarly, the Intelligence Community has highlighted efforts of "cyber actors" associated with China, including the targeting of U.S. political party internet domains. 2022 Election ICA at 4. The Intelligence Community observed China's efforts to

gather information on American voters, political parties, candidates, and senior government officials. 2020 Election ICA at 8.

B. Social media is the most common vector of foreign malign influence targeting the United States.

Popular social media platforms like Facebook, Instagram, Twitter, YouTube, and TikTok are attractive targets for foreign malign influence campaigns due to their widespread use, accessibility, and the ease with which foreign actors can impersonate Americans on them. Leading up to November 2016, Americans generated nearly nine billion Facebook interactions and more than one billion tweets and retweets related to the election. Intel. Comm. Rep., Vol. 2 at 8-9. Political campaigns quickly realized social media's burgeoning value as a persuasive tool. The 2016 election cycle saw a 789% increase in digital advertising spending over 2012. *Id.* at 9. But this massive growth in social media use further energized foreign malign actors seeking to sow discord and discontent across America.

Foreign adversaries exploit the scale, targeting tools, and marketing tools of social media platforms to undermine U.S. security. Before the 2016 election, IRA operatives utilized "almost the entirety" of Facebook's suite of features—a set of tools intended for legitimate civic organizations, political candidates, and commercial brands to reach target audiences—"exactly as it was engineered to be used." *Id.* at 48. In 2020, the IRA manipulated Facebook's targeting tools to "deliver tailored content" to specific subsets of the U.S. population. 2020 Election ICA at 4. Its election influence campaigns pervaded essentially every

American social media platform, including Facebook, Instagram, Twitter, Google services (including YouTube, Gmail, and Google advertising platforms), Tumblr, Reddit, Medium, Pinterest, Meetup, Vine, Gab, LiveJournal, and LinkedIn. To broadcast its subversive messaging as widely as possible, and potentially to generate perceptions of consensus, the IRA even used browser extensions, music applications, and mobile games like Pokémon Go to communicate with American audiences. Intel. Comm. Rep., Vol. 2 at 62.

As the Intelligence Committee later learned and included in its bipartisan report, the IRA spent years preparing for its election influence campaigns. At least two years before the 2016 election, the IRA began to "track and study" groups on American social media sites "dedicated to U.S. politics and social issues." Indictment, *United States v. Internet Research Agency LLC*, No. 18-cr-00032 (D.D.C. Feb. 16, 2018) ¶ 29 (Mueller Indictment). It analyzed engagement metrics such as comments, likes, and responses to refine its future influence activities. *Id.* The IRA sent operatives to the U.S. in 2014 to obtain information and photographs for later use on social media. Special Counsel Robert S. Mueller, III, *Rep. on the Investigation into Russian Interference in the 2016 Presidential Election: Vol. I*, U.S. Dep't of Justice (Mar. 2019) at 14 (Mueller Rep.).

Russia displayed an intense commitment to social media as an influence campaign tool. The IRA employed teams of "specialists," divided into "day-shift and night-shift hours," that it instructed to post in English on social media sites in accordance with the appropriate U.S. time zone. Mueller Indictment ¶ 33.

These specialists posted messages from accounts pretending to be Americans, as well as from larger social media groups or public pages that claimed to be affiliated with U.S. political and grassroots organizations. Mueller Rep. at 22. Russia's efforts show its deep knowledge and understanding of social media, which it used to great effect in its 2016 election influence campaign.

As Russia and other adversaries realize, social media makes influence operations possible at a massive scale. An estimated 3.3 million Facebook users followed pages operated by the IRA. Intel. Comm. Rep., Vol. 2 at 45. Those pages produced 76.5 million engagements, including more than 30 million shares, 37 million likes, 3 million comments, and 5 million reactions. *Id.* According to Facebook, as many as 126 million Americans viewed content manufactured and disseminated by the IRA on Facebook pages between 2015 and 2017. *Id.*

The IRA's Facebook content ran the gamut of divisive issues in American society, with content supporting and opposing essentially all sides of every issue. Some of its most active Facebook pages included "Blacktivist," "South United," "LGBT United," and "Army of Jesus." *Id.* "Blacktivist"—which impersonated an American racial justice organization—garnered more than eleven million engagements. *Id.* at 46.

The IRA's engagement with Americans on Instagram "dramatically eclipsed" the interaction it achieved through Facebook. *Id.* at 48. The IRA used 133 Instagram accounts to publish more than 116,000 messages, nearly twice the number of its Facebook posts. *Id.* While the IRA's Instagram accounts

garnered 3.3 million followers (roughly the same as its Facebook pages), they generated 187 million engagements, about two and a half times as many as Facebook. *Id.*

On Instagram, IRA accounts posted content similar to that of its Facebook pages from accounts including "Blackstagram_" (racial justice issues), "american.veterans," "rainbow_nation_us" (LGBTQ issues), and "pray4police" (seeking to exploit Americans supportive of law enforcement). *Id.* at 49. Twelve IRA-operated Instagram accounts gained more than 100,000 followers each. *Id.* These foreign-operated accounts grew to such scale during a period where the government had not started sharing threat information with social media platforms.

The viral nature and cumulative follower base that social media offers allowed the IRA to avoid large marketing expenses. In total, the IRA spent about $100,000 on more than 3,500 Facebook advertisements. Mueller Rep. at 25. But its overall operating costs—about $1.25 million per month—dwarfed its advertising costs. Intel. Comm. Rep., Vol. 2 at 7. The IRA's assemblage of millions of followers, across pages and accounts on multiple platforms, allowed its influence campaign to spread with relatively small advertising expenditures and without the notice of American social media platforms.

Social media's nature also allows influence campaign messaging to spread rapidly. Posts on Facebook, Twitter, or Instagram can "go viral" in a matter of hours or even minutes. This allows Russia and other adversaries "to formulate and execute information operations with a velocity that far outpaces the responsivity of a formal decision-making

loop in NATO, the United States, or any western democracy." *Id.* at 17-18.

Foreign influence operators can easily impersonate Americans on social media platforms. Most accounts can be created using any name without any verification. When verification was required, IRA specialists used ill-gotten bank account numbers and fake driver's licenses to create PayPal and cryptocurrency accounts they used to pay for social media advertising. Mueller Indictment ¶¶ 91-93.

Russian-controlled accounts obtained positions of significant influence from which they fundamentally distorted our Nation's democratic discourse. One of the IRA's effective influence operations was the Twitter account @Jenn_Abrams, which amassed 80,000 followers. The account impersonated an American identity and tweeted about "everything from segregation to the futility of political correctness." Intel. Comm. Rep., Vol. 2 at 55. @Jenn_Abrams was cited by more than 40 American journalists before Twitter removed the account in late 2017. *Id.* One follower of the account was John Kelly, who served as Secretary of Homeland Security and White House Chief of Staff during the Trump administration. *Id.*

By early 2015, the IRA had created larger social media groups and pages that claimed false affiliation with U.S. political or grassroots organizations. Mueller Rep. at 22. Fake affinity groups for Muslim-Americans, Black social justice, and conservative politics each garnered over 200,000 Facebook followers. *Id.* at 25-26. The IRA also operated the @TEN_GOP Twitter account, which amassed over 150,000 followers—eleven times as many as the

legitimate Tennessee Republican Party account. Intel. Comm. Rep., Vol. 2 at 54. @TEN_GOP was successful in "deceptively injecting its inflammatory content" into American political discourse in 2016 and 2017. *Id.* Its content was widely cited in mainstream media and retweeted by celebrities, politicians, and political figures including Donald Trump, Jr. and Kellyanne Conway. *Id.*

The IRA's impersonation efforts on social media tricked unwitting Americans into believing the messages were coming from their neighbors and peers. Undetected by private-sector service providers, IRA specialists used Google and Yahoo email accounts impersonating Americans to send press releases to New York-area media outlets about election rallies in 2016. Mueller Indictment ¶¶ 61, 67. The IRA even fooled members of a presidential candidate's campaign team, communicating with unaware campaign officials on Twitter and Facebook. *Id.* ¶¶ 79-80. These impersonations take the place of authentic American voices and use this position of influence to sow mistrust that affects even legitimate American political and social organizations.

Crucially, undetected foreign malign influence activity that exploits American social media platforms does not exclusively impact the digital public sphere. The IRA experimented with instigating real-world events via social media in 2015, when it attempted to induce a mass gathering in New York City by promoting a Facebook event offering free food. Intel. Comm. Rep., Vol. 2 at 46. Quickly realizing the tactic's potential, the IRA invested more of its resources into event marketing.

Its first known event was a "Confederate rally" in Texas promoted on Instagram in 2015. Mueller Rep. at 29. The IRA's "Being Patriotic" Facebook page, which amassed over 216,000 followers, then promoted flashmobs supporting one presidential candidate. IRA-promoted events backing that candidate in the key state of Florida took place in Fort Lauderdale and Coral Springs. Intel. Comm. Rep., Vol. 2 at 47. IRA specialists communicated with unwitting campaign staff in preparation for these events, and the IRA paid participants to portray the candidate's opponent imprisoned in a cage on the back of a truck during them. *Id.* at 37. The IRA ultimately organized dozens of real-world rallies, and its specialists repeatedly sent funds to American volunteers or supporters to arrange for events that had been planned through social media. Mueller Indictment ¶¶ 29-30.

In 2016, the IRA particularly focused its efforts on agitating political events and protests across America in its attempt to stoke real-world violence. For example, IRA specialists used Facebook to promote a "Stop Islamization of Texas" event scheduled in front of a mosque in downtown Houston in May 2016. Intel. Comm. Rep., Vol. 2 at 47. The page the IRA used to advertise the event garnered 250,000 followers. *Id.* At the same time, the IRA used a second Facebook page with 325,000 followers called "United Muslims of America" to promote a "Save Islamic Knowledge" event, which it set for the same date and time in front of the same mosque. *Id.* Neither page referenced any opposing rally. *Id.* Both events were covered live by local news agencies, and local media reported they escalated into confrontations and verbal attacks. *Id.* The IRA's cost to advertise these competing events on

Facebook was just $200, and it performed its entire operation from Russia. *Id.*

Iran has made similar plans. In 2020, Iranian officials advocated for the use of covert social media accounts "to pit 'US extremist groups' against each other," likely for use in 2024. 2022 Election ICA at 5. This is consistent with prior Iranian efforts to "inflame extremist ideologies," "intimidate voters," and "stoke political violence" in 2020. *Id.*

Social media targeting tools allow foreign adversaries to covertly direct influence activity at narrow, specific groups of Americans—including in ways that suppress civic and political participation. In 2016, the IRA did this with precision. No group was targeted more than African Americans. Intel. Comm. Rep., Vol. 2 at 38. "By far," race was the "preferred" wedge issue for the IRA in its quest to divide the United States. *Id.* More than 66% of the IRA's Facebook advertising content included terms relating to race, and its locational targeting principally aimed messages at African Americans. *Id.* at 6. On ten YouTube channels operated by the IRA with names including "Black Matters," "BlackToLive," and "Cop Block US," 96% of its videos involved discussions of race and police brutality. *Id.* at 58.

As the 2016 election approached, IRA specialists encouraged U.S. minority groups not to vote in the presidential election or to vote for a third-party candidate. Mueller Indictment ¶ 46. The IRA-operated Instagram account "Woke Blacks" urged African Americans in October 2016 not to "resort to the lesser of two devils" because "we'd surely be better off without voting AT ALL." *Id.* ¶ 46(a). Five days before Election Day, the "Blacktivist" Instagram account

posted a message encouraging its followers to "Choose peace and vote for Jill Stein," the Green Party presidential nominee. *Id.* ¶ 46(b).

Iran also engaged in highly targeted influence efforts. Before the 2020 election, Iranian cyber actors sent threatening emails to voters in the Democratic Party in multiple states, demanding that they change their party affiliation and vote to re-elect President Trump. 2020 Election ICA at 6. American intelligence found that Iranian operatives specifically sought to intimidate American voters in advance of the 2020 election. 2022 Election ICA at 5. Senator Warner believes that these efforts by Iran were less successful than they might have been, in no small part due to the ability of government officials to share threat information with impacted platforms.

Another feature of social media is the ease with which one person or entity operating multiple accounts can post messages on all sides of any topic. The IRA used multiple false personas to drive wedges into hot-button issues, "taking and attacking all sides of the arguments," using different accounts operated by the very same computer. Intel. Comm. Rep., Vol. 2 at 53-54. On Twitter, two IRA accounts with the usernames @WokeLuisa and @BarbaraForTrump espoused opposing positions about professional football players kneeling in protest of police brutality and racism. *Id.* One of these tweets in March 2018 garnered 37,000 retweets, and @WokeLuisa's content appeared in more than two dozen mainstream news stories from outlets including BBC, USA Today, Time, and BET. *Id.* at 54-55.

Foreign-owned social media platforms are even more direct vectors for foreign malign influence.

Because TikTok and WeChat (two of the most popular platforms today) are Chinese owned, the U.S. government is limited in how directly it can engage with them. Specifically, the counterintelligence practice of using defensive and counterintelligence briefings—under which government officials share relevant threat information with U.S. social media platforms—involves the careful consideration of risk that any information shared could be passed to foreign actors.

Russia, Iran, China, and others are already familiar with social media's capabilities and potential, and their skills with popular platforms will only improve with time. Social media's role as the leading vector of foreign malign influence campaigns is likely to grow in the lead up to the 2024 election and beyond.

II. Engagement with social media platforms is the only effective way to limit the damage of foreign malign influence.

To proactively combat foreign malign influence on social media platforms, the public and private sectors must coordinate and cooperate. Threat sharing has always been a critical component of any counterintelligence strategy, dating well before the Cold War. It is particularly crucial in the case of foreign information operations carried out on social media. Social media companies and the government often have access to different, complementary information, and they are best able to address the dangers posed by foreign malign influence campaigns when they work together.

Since 2016, social media companies have become increasingly interested in working with the government to address foreign threats on their

platforms. They have been able to do so through reciprocal information sharing.

A. Threat sharing is a well-established counterintelligence practice.

In the counterintelligence context, the U.S. government has long relied on threat sharing—including defensive briefings—to alert unwitting U.S. persons and organizations to efforts by foreign adversaries and intelligence services to target, exploit, or infiltrate them. That information sharing is crucial in the information security context due to the increasing sophistication and organization of the attackers. Chris Johnson et al., *Guide to Cyber Threat Information Sharing*, NAT'L INST. OF STANDARDS & TECH. (Oct. 2016) at 2, dx.doi.org/10.6028/NIST.SP.800-150. Threat sharing not only allows organizations to leverage collective knowledge and capabilities to identify and increase awareness of certain threats, but it also permits those organizations to improve their systems and minimize susceptibility to threats going forward. *Id.* at 3-4.

Following the 2016 election, the Intelligence Committee issued a bipartisan report with numerous recommendations regarding threat sharing, emphasizing that "[t]he Federal government, civil society, and the private sector, including social media and technology companies, each have an important role to play in deterring and defending against foreign influence operations that target the United States." Intel. Comm. Rep., Vol. 2 at 78. The Committee also recommended that companies facilitate increased information sharing between the public and private sectors, and across social media platforms, to address

"malicious activity and platform vulnerabilities that are exploited to spread misinformation." *Id.*

Similarly, the Committee recommended that Congress "consider ways to facilitate productive coordination and cooperation" between social media companies and the government to "curtail[] foreign influence operations that target Americans," because it found "[i]nformation sharing between the social media companies and law enforcement must improve, and in both directions." *Id.* at 80.

Prior to the 2016 election, threat monitoring and coordination between social media companies and the government was largely done on an *ad hoc* basis, relegated to coordination through contractors, rather than through any formalized or regularized channels. The Intelligence Committee found this to be "troubling." *Id.* at 72-73. This dynamic reflects the belated recognition by both the Intelligence Community and social media companies that foreign malign influence actors would—and could—use social media in sophisticated, extensive ways to undermine U.S. national security. Senator Warner has described the 2016 election as a "wakeup call" to both government officials and private sector leaders on the efficacy of social media as a vector of foreign malign influence. Fortunately, threat sharing has since increased significantly, improving the abilities of both government agencies and social media companies to combat foreign influence operations. *Id.* at 72.

For example, following the 2016 election, Twitter and Facebook voluntarily established relationships with law enforcement agencies including the FBI's Foreign Influence Task Force and Counterintelligence Division, the Department of Homeland Security's

(DHS) Election Security Task Force, the Department of Justice's National Security Division, and Secretaries of State, with whom these companies share threat information to detect and stop foreign malign influence. *Id.* at 72. In fact, companies including Facebook, Twitter, and Google met with government officials from DHS, the FBI, and the Office of the Director of National Intelligence in advance of the 2018 and 2020 elections to partake in threat sharing and strategically collaborate. *See* Sheera Frenkel et al., *Top Tech Cos. Met with Intel. Officials to Discuss Midterms*, N.Y. TIMES (June 25, 2018), www.nytimes.com/2018/06/25/technology/tech-meeting-midterm-elections.html. During the 2020 elections, "proactive information sharing with social media companies facilitated the expeditious review, and in many cases removal, of social media accounts covertly operated by Russia and Iran." 2020 Election ICA at 1.

B. Social media platforms do not want to serve as vectors of foreign malign influence.

Social media platforms share the Intelligence Committee's concern regarding foreign malign influence. They categorically do not want to be a vector or facilitate these campaigns. To that end, they proactively share intelligence information with the government and request that government agencies and officials share knowledge with them, too.

Even before the 2016 election, Facebook in several instances "detected and mitigated threats from actors with ties to Russia" and proactively reported them to U.S. law enforcement officials and agencies. Intel. Comm. Rep., Vol. 2 at 73. Likewise, since the 2016

election, Facebook has also coordinated with the FBI's Counterintelligence Division and Foreign Influence Task Force, DHS, and multiple Secretaries of State to stop foreign information operations. *Id.* at 72.

Indeed, during his time as Chairman and Vice Chairman of the Intelligence Committee, Senator Warner garnered firsthand experience with senior executives at multiple social media companies requesting his help (and help from the Intelligence Community generally) to push the government to share foreign malign threat information. Throughout 2017, as increased evidence of Russia's efforts to influence the 2016 election mounted, senior-most executives at Facebook, Google and Twitter requested Senator Warner push intelligence agencies to share threat information with security teams assembled by the companies. In a 2017 meeting before the Intelligence Committee, Sean Edgett (then General Counsel of Twitter) emphasized that cooperation was essential to addressing foreign malign influence, informing the Committee that "the best approach is to combine information and ideas to increase our collective knowledge." *Social Media Influence in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intel.*, 115th Cong. 23 (2017).

Likewise, Sheryl Sandberg and Jack Dorsey (then senior executives of Facebook and Twitter, respectively) both highlighted that the government and social media companies have access to different types of information and sharing that information will allow them to collaborate faster and strengthen collective defenses to foreign threats. *Foreign Influence Operations' Use of Social Media Platforms: Hearing Before the S. Select Comm. on Intel.*, 115th

Cong. 2 (2018). Both Sandberg and Dorsey expressed an interest in meeting routinely with governmental divisions and exchanging more information to strengthen threat responses and spoke of their successful, voluntary engagements with both the FBI's Foreign Influence Task Force and DHS. *Id.*

Before the 2018 midterms, Facebook hosted a meeting with Under Secretary of DHS for National Protection and Programs Christopher Krebs, a representative of the FBI's Foreign Influence Task Force, and several large technology companies including Twitter and Google to facilitate information sharing concerning threats these companies should anticipate. *See* Frenkel, *Top Tech Cos. Met with Intel. Officials to Discuss Midterms*, *supra* p. 23. Facebook held a similar meeting in advance of the 2020 election where representatives from Facebook, Twitter, and Google noted the importance of coordinating with the government to prevent threats to the integrity of U.S. elections. *See* Mike Isaac et al., *Big Tech Cos. Meeting with U.S. Officials on 2020 Election Sec.*, N.Y. TIMES (Sept. 4, 2019), www.nytimes.com/2019/09/04/technology/2020-election-facebook-google.html. As then-Vice Chairman of the Intelligence Committee in advance of these elections, Senator Warner recalls conversations with government officials and industry executives on the importance and voluntary nature of these engagements.

U.S. social media companies do not wish to be conduits of foreign malign influence. They have gone out of their way, repeatedly, to seek and share information about threats and methods to protect their platforms and users from foreign malign

influence. Social media companies continue to request the government's assistance in combatting foreign threats, and the government remains prepared to assist if it is not prevented from doing so. At no time have industry executives or other corporate representatives of social media platforms indicated to Senator Warner that they felt compelled or coerced to engage with government officials.

C. Government engagement with social media platforms has limited the damage of foreign malign influence.

Coordination between the federal government and social media companies has already curtailed the harmful impacts of foreign malign influence. For example, following the 2016 election, Facebook worked closely with government partners from the FBI and the Cybersecurity and Infrastructure Security Agency to address foreign malign information campaigns leading up to the 2018 and 2020 elections. That cooperation enabled Facebook to locate and remove "foreign operations backed by Russia, China, and Iran that used fake accounts to deceive users and undermine trust in the United States." Facebook, *A Look at Facebook and US 2020 Elections* 6 (2020), about.fb.com/wp-content/uploads/2020/12/US-2020-Elections-Report.pdf. Until the recent injunction, Senator Warner understands these interactions continued, resulting in the identification of foreign malign influence activity previously undetected by the social media platforms.

Facebook itself recognized the importance of collaboration with the government, acknowledging that while foreign malign influence certainly poses a

threat, it "can be countered by determined defenders who coordinate regularly." *Id.* at 7. In fact, the head of security policy for Meta (Facebook and Instagram's parent company) noted that while it has resources to detect coordinated attacks on its networks, "the government is often more adept at tracking campaigns that are organized off social media." Naomi Nix et al., *U.S. Stops Helping Big Tech Spot Foreign Meddling Amid GOP Legal Threats*, WASH. POST (Nov. 30, 2023), www.washingtonpost.com/technology/2023/11/30/biden-foreign-disinformation-social-media-election-interference. After receiving tips from law enforcement about off-platform activity, Meta "dismantled three covert influence operations based in Russia, Mexico and Iran" in advance of the 2020 election. *Id.*

Tumblr also restrained foreign malign influence on its platform through cooperation with the government. In 2017, Tumblr announced it had uncovered 84 accounts associated with the IRA that interacted with 11.7 million U.S. users and nearly 30 million users globally. Intel. Comm. Rep., Vol. 2 at 60. Then, in Fall 2018, law enforcement notified Tumblr about possible IRA influence and operational activity regarding the 2018 midterm elections. Using that information, "Tumblr identified 112 accounts tied to what was identified as an influence operation, indicating that Russia-based influence operatives continue to exploit the Tumblr platform targeting the United States." *Id.* at 61.

Multiple actors within the Intelligence Community have recognized the positive impact threat sharing has had in preventing foreign malign influence operations. Proactive threat sharing has

"facilitated the expeditious review" and "removal" of Russian and Iranian social media accounts. 2020 Election ICA at 1. Because threat sharing has been made a "particular point of emphasis," the government and social media companies have "improved" their ability to "identify and combat" imposter accounts. Intel. Comm. Rep., Vol. 2 at 72. Threat sharing has proven to be an effective way to keep Americans safe.

III. Even a narrowly drawn injunction risks crippling the United States' ability to counter foreign malign influence.

Any injunction here, no matter how narrow, poses a great security risk to the United States by restricting the ability of the government and social media companies to counter foreign malign influence together. Since the 2016 election, foreign influence campaigns have only increased in number, scope, and sophistication. They will continue to do so. In recent years, social media companies worked with one another and the government to seek and share information about specific threats which improved their own security and that of their peers. These interactions are necessary to ensure that foreign malign influence activity does not reach or exceed the scale or scope of the IRA's efforts in 2016.

This progress will be halted if the injunction is upheld in any form by hindering—if not destroying—the most effective method of countering foreign malign influence, forcing intelligence officials instead to resort to less effective alternatives that dramatically increase the risk of compromising highly sensitive intelligence sources and methods.

A. Social media-enabled foreign malign influence operations have grown since 2016 and will continue to grow.

While foreign entities seeking to undermine the American-led liberal democratic order is nothing new, Russia's foreign influence operations aimed at the 2016 elections were a "significant escalation in directness, level of activity, and scope of effort compared to previous operations." 2016 Election ICA at ii. The Intelligence Community concluded that such operations are a "new normal" and that Russia will apply lessons learned from the 2016 influence campaign to its future efforts. *Id.* at 5.

Indeed, subsequent Intelligence Community assessments have identified a growing number of adversaries engaged in foreign influence operations, a growth in the scale and scope of those operations, and an expansion of the techniques and tactics employed. In addition to Russia, China, and Iran (who have historically been involved in foreign malign influence operations), foreign actors such as Cuba, Venezuela, and Hizballah also attempted to launch campaigns to influence the 2020 presidential election. 2020 Election ICA at 8. This increased involvement of foreign actors can be attributed to a "shifting geopolitical risk calculus, perceptions that election influence activity has been normalized, the low cost but potentially high reward of such activities, and a greater emphasis on election security in [intelligence] collection and analysis." 2022 Election ICA at 5. As Chairman of the Intelligence Committee, Senator Warner has seen firsthand how foreign governments increasingly embrace online influence capabilities as an instrument of covert military and intelligence aims.

The "scale and scope" of foreign activity targeting the 2022 midterm elections "exceeded" what the Intelligence Community detected during the 2018 midterm. *Id.* Because foreign malign influence has become "normalized" and is increasing, *id.* at 1, it is imperative for social media companies and the government to work collaboratively to combat it.

Foreign actors have also learned to use an expanded set of techniques and tactics in their influence operations. For example, during the 2022 election cycle, adversaries made payments to social media "influencers" and enlisted public relations firms to engage in information manipulation tactics. *Id.* at 5. Russian influencers "amplified narratives about purported voting abnormalities and fraud, particularly in Arizona" and "highlighted a conspiracy theory claiming that Ukraine had invested US aid money in the FTX cryptocurrency exchange to benefit Democratic campaigns." *Id.* at 10.

Foreign adversaries are also targeting "alternative" online mediums to target audiences they perceive as "receptive to their messaging." *Id.* at 5. One method is to use a "Russian influence-for-hire group" that created personas on the conservative-oriented social media networks Gab and Gettr to reach new audiences. *See id.* at 9. Indeed, the growth of alternative platforms catering to narrower audiences offers even greater opportunities for foreign adversaries to target discrete communities and sow social and racial discord.

Generative artificial intelligence (AI) tools are yet another technological advance that present new opportunities for foreign malign actors. In 2016, using less sophisticated tools, the IRA fabricated a video

falsely depicting a political candidate engaged in a sex act, which was viewed more than 250,000 times. Intel. Comm. Rep., Vol. 2 at 59. Today's generative AI improves disinformation capabilities and makes them even less detectable. Further, the blazing speed that a fake video can travel across social media means rapid information sharing is even more crucial to combat it. Rather than putting government officials in a position of evaluating the veracity of particular content, successful threat sharing engagements empower platforms to make their own content moderation decisions with knowledge of foreign adversarial behaviors and malicious activity.

Cooperation and coordination between the public and private sectors to address these concerns is paramount in light of the increasing scope, frequency, and danger posed by foreign malign influence.

B. The injunction at issue here, even when stayed, dramatically reduces the government's ability to engage with social media companies.

The injunction at issue here has already diminished and will continue to deplete the government's ability to engage with social media companies about matters of national security. Indeed, this lawsuit has had a demonstrated chilling effect on threat sharing. This injunction has "led to broad uncertainty" among government officials about what "communications with tech companies" are "appropriate." Nix, *U.S. Stops Helping Big Tech Spot Foreign Meddling Amid GOP Legal Threats*, *supra* p. 27. When government agents must "second-guess every time they need to send an email or pick up the phone," a former State Department official explained,

their response capabilities will be "less functional." *Id.* The chilling effect of the injunction is so great that, as the agency has informed Senator Warner, the FBI has not shared *any* threat intelligence with social media companies since it was issued on July 4, 2023.

These problems extend beyond the context of federal elections. For instance, policymakers have raised concerns about foreign malign influence activity directed at Americans in relation to the conflict between Israel and Gaza.

Taking lessons from the 2016 election to heart, social media companies and the government coordinated and collaborated in responding to foreign interference campaigns before and during the 2018, 2020 and 2022 elections. Any injunction of any scope here would threaten their ability to combat election influence campaigns leading up to the presidential election in 2024 or any other foreign malign influence campaigns that continue to attack America.

Even while stayed, this injunction has already reduced the Intelligence Community's threat sharing capacity. Ben Nimmo, Meta's chief of global threat intelligence, said government officials "stopped communicating foreign election interference threats" to Meta in July—the same month the preliminary injunction was issued below in the district court. *Id.* FBI Director Christopher Wray told Congress that, "out of an abundance of caution," the FBI's interactions with social media companies "changed fundamentally" after the injunction was imposed. *Id.* Even the more limited, now-stayed injunction still curtails progress made since 2016 to respond to foreign malign influence campaigns. As Stanford Law School professor Evelyn Douek explained, the

injunction's chilling effect "creates [an] instinct" to "just not do anything" to avoid being seen as doing "something problematic." *Id.* And while American threat sharing efforts are hampered, our foreign adversaries' capabilities are only improving.

There is no effective alternative to real-time communication between frontline government officials and social media companies. Defensive and counterintelligence briefings involve delicate evaluations of the benefit of sharing information to counter foreign influence activity against the risk that such sharing might alert foreign actors of U.S. intelligence collection.

By contrast, public exposure of threats (assuming an injunction would allow it) dramatically imperils the protection of U.S. intelligence sources and methods and risks decreasing our capacity for gathering further intelligence. The effectiveness of identifying threats is limited if Russia, Iran, or other actors were privy to the clues that ultimately tipped off the government or social media companies. And public exposure of threats risks implicating innocent Americans who may have inadvertently interacted with foreign-controlled accounts that the government later publicly identifies. Instead, defensive briefings and threat sharing provide the most targeted, effective, and privacy-preserving method of advancing a valid counterintelligence mission, with the least risk of harm to U.S. intelligence assets.

There is no substitute for real-time threat sharing between the government and social media companies when it comes to combating foreign malign information campaigns. The government and social media companies have access to different types of

information and benefit from exchanging such information where appropriate. It is essential to our national security that the government can communicate freely with social media companies about threats that foreign malign influence campaigns pose to their platforms and users.

CONCLUSION

To preserve America's ability to respond quickly and effectively to foreign malign influence campaigns that target our national security and elections, this Court should reverse the judgment of the Fifth Circuit in relevant part and direct that the preliminary injunction be vacated in its entirety.

Respectfully submitted,

HASSAN A. ZAVAREEI
GLENN E. CHAPPELL
SPENCER S. HUGHES
Counsel of Record
GEMMA SEIDITA
SCHUYLER J. STANDLEY
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue
NW, Suite 1010
Washington, DC 20006
(202) 973-0900
shughes@tzlegal.com

Counsel for Amicus Curiae

December 26, 2023