Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions
Michael S. Smith II
Questions for the Record
Submitted November 7, 2017

QUESTIONS FROM SENATOR FEINSTEIN

Notification of Law Enforcement

1. Recently, British parliament's Home Affairs Select Committee released a report finding that social media platforms, such as Facebook, Twitter, and YouTube, failed to remove extremist material posted by banned jihadist and neo-Nazi groups, even when that material was reported. I am working on legislation to require technology companies to report known terrorist activity on their platforms to law enforcement. The provision is modeled after an existing law which requires technology companies to notify authorities about cases of child pornography.

    a. What are technology companies doing to prevent this type of activity from occurring on their platforms?

Answer by Michael S. Smith II:

I am unaware of the full scope of activities pursued by these and other American companies to attempt to prevent terrorists and other illicit actors from using their technologies to threaten the security of Americans and our closest allies. Indeed, most of these companies have not been transparent about the full scope of their efforts undertaken to address these and other issues which can have negative consequences for the safety and security of Americans and our allies.

Certainly, for some efforts to counter terrorists' and other extremists' online activities, secrecy helps to ensure success. Still, it is clear the various measures pursued to attempt to prevent the exploitations of these companies' technologies by terrorists engaged in efforts to incite violence within the United States and other countries over the Internet have failed to achieve an effect of deterring United States-designated foreign terrorist organizations—notably Islamic State—from persisting with efforts to convert American social media and file-sharing platforms into tools used to expand their capabilities to threaten Americans and our allies. As highlighted by this very question, it is also clear that, if left unchecked by policymakers, this set of problems can yield deleterious consequences for our nation's relations with our closest allies in Europe, which are facing the same terrorist threats emanating from spaces of the Internet managed by American companies, and whose representatives in government have publicly and privately in discussions with American officials expressed grievances concerning the myriad of deficiencies evinced by American companies' responses to the threat environment.

I also believe the counter-messaging, or "countering violent extremism," programs underway on certain platforms are unlikely to achieve desired results with respect to substantially reducing the likelihood of occurrence of terrorist attacks perpetrated in the United States and elsewhere in the West by individuals attracted to the ideology promoted by groups like Islamic State and al-Qa'ida over the Internet. Furthermore, I believe that, unless very carefully coordinated with law enforcement authorities, counter-messaging campaigns targeting social media account managers suspected of being sympathetic to terrorist groups can easily manifest in unintended outcomes. For instance, a project recently undertaken by the United States-based International Center for the Study of Violent Extremism that entailed confronting on Facebook suspected Islamic State sympathizers, whose postings indicate they reside in the West, using counter-messaging materials that might fail to persuade them to decide Islamic State is not worthy of support could have had the effect of increasing a sympathizer's hostility towards non-group members, possibly accelerating his or her willingness to perpetrate attacks called for by Islamic State in its online propaganda.[1] If such engagements are not coordinated with appropriate authorities, it is conceivable law enforcement personnel may not have the situational awareness required to enable interventions to disrupt the resort to violence that could be accelerated by this type of online confrontation.

Ultimately, I believe policymakers should require the United States Intelligence Community to prioritize disruption over simply monitoring illicit online networks, and over supporting efforts to "counter" messaging employed in terrorists' online recruitment and incitement programs. Additionally, I believe policymakers should develop legislation which compels American Internet companies to implement a variety of policies that can at once serve to disrupt and deter such activities that pose as severe sources of threats to America's national security.

The aforementioned companies' inabilities and/or unwillingness to develop and impose policies which could help to more effectively mitigate threats emanating from popular spaces of the Internet managed by them highlights there is a need for policymakers to develop legislation which can both help to guide and compel a wider effort to disrupt the persistent exploitations of these and other Internet companies' technologies by terrorist groups like Islamic State. Such legislation should also seek to encourage foreign social media and file-sharing sites to impose uniform sets of policies by denying United States-based advertisers and account users abilities to utilize their platforms should they refuse to impose policies deemed necessary to safeguard against threats posed by terrorists and other illicit actors of interest to national security managers.

b. In what ways do you think that technology companies can do more to prevent this type of activity from occurring on their platform?

Answer by Michael S. Smith II:

It is my assessment developing and implementing a variety of policies which serve to increase risks encountered by illicit actors should they seek to convert American companies' popular social media and file-sharing platforms into tools used to harm Americans and our allies is the most practical approach to deterring Islamic State, al-Qa'ida and other terrorist elements from persisting with their exploitations of these companies' technologies to recruit and incite violence—both in proximity of and far from their primary areas of operation, including within

[1] I served as a peer reviewer for a submission to a terrorism studies journal from this organization, in which this rogue "countering violent extremism" project was described.

the United States and other countries in the West.

One way Facebook, Twitter and Alphabet, the parent company of YouTube and Google Drive, could help disrupt and deter persistent exploitations of their technologies by terrorist groups like Islamic State, which encourages its members and supporters to employ various technologies to mask their physical locations when online, such as virtual private networks (VPNs), is to allow only account managers whose identities are known to them to access their accounts when simultaneously using technologies that can sometimes make it impossible for investigators to identify a user's physical location once suspicious or illegal activity is detected. Such policies will likely dually serve to deter other illicit actors from harnessing these companies' technologies to harm Americans and our allies.

Certainly, any American company which has determined, or even suspects members of terrorist groups and terrorist group sympathizers are using their technologies to threaten Americans and our allies should promptly alert federal authorities. Here, it is important to consider that reporting suspicious or illegal activities to authorities may serve to accomplish very little in the way of counterterrorism successes if the responsible parties have used VPNs whose managers are either unable or unwilling to share information which could be used to identify their locations. (Note: Many VPN access providers claim to have configured access to their technologies in manners which do not enable them to identify their users' physical addresses.)

As noted in my written testimony for the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing, if the popular website Wikipedia, which is managed by a nonprofit organization, can deny visitors editorial controls when using technologies such as VPNs to mask their physical locations, it stands to reason such technology innovators as the aforementioned companies can implement similar policies to deter a myriad of harmful activities on their popular platforms—ranging from extreme forms of cyber bullying of concern to First Lady Melania Trump to child predation, and from white collar crimes involving manipulation of investors' and traders' perceptions of stocks to terrorists' efforts to remotely groom supporters to perpetrate attacks in the United States.

To date, however, these companies have rejected calls for them to impose such policies. One example is provided in a commentary piece I published earlier in 2017 with *Foreign Affairs* (published by the Council on Foreign Relations), titled "Containing ISIS' Online Campaigns After Manchester: The Simple Tools We Can Use But Choose Not To."[2] Roughly a year prior, I proposed the same measures in a piece published by *The Christian Science Monitor*, titled "How to beat ISIS on Twitter."[3] Therein, I noted Islamic State member and British national Sally Jones—by this time designated a Specially Designated Global Terrorist by the United States Department of State[4]—was clearly not deterred by Twitter's increasingly-aggressive accounts suspension campaign, as she had recently used Twitter to harass me and a

[2] Link to material: https://www.foreignaffairs.com/articles/2017-05-27/containing-isis-online-campaigns-after-manchester?cid=soc-tw-rdr

[3] Link to material: https://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0527/Opinion-How-to-beat-ISIS-on-Twitter

[4] Link to designation details: https://www.federalregister.gov/documents/2015/09/30/2015-24894/in-the-matter-of-the-designation-of-sally-anne-frances-jones-also-known-as-sally-anne-jones-also

journalist who reports on Islamic State for *The New York Times*. Before doing so, to draw attention to her activities among federal officials, Jones followed the official Twitter accounts used by FBI and USCENTCOM.

Given these companies' resistance to such policy concepts, policymakers should examine ways regulatory bodies, such as the Federal Communications Commission, could require these and other American companies to implement policies which can help deter terrorists from converting their powerful technologies into tools used to threaten Americans and our allies.

Additionally, legislation which requires social media and file-sharing sites to provide intelligence agencies access to the full set of data and custom-tailored analytic tools they need access to in order to more rapidly identify and rigorously map terrorists' and other illicit actors' activities on American companies' social media and file-sharing sites should be contemplated.

In 2016, I was the lead source for *The Wall Street Journal*'s story on Twitter's decision to prevent Dataminr from executing a contract to provide more expansive support to various elements of the United States Intelligence Community, titled "Twitter Bars Intelligence Agencies From Using Analytics Service."[5] At the time, Dataminr had exclusive access to the full set of data generated on Twitter's platform—as it was being generated. Further, according to a representative of Dataminr, whom I met with prior to the publication of the aforementioned news story, Twitter owned five percent share of Dataminr and held board observer status. Years prior, CIA's venture capital arm, In-Q-Tel, provided funding for Dataminr to develop technologies which enabled real-time tracking of extremist postings on Twitter. According to the representative of Dataminr whom I met with, once Dataminr's obligations to the United States Intelligence Community expired pursuant to the terms of the agreement with In-Q-Tel, Twitter expressed concerns about the optics of the relationship between the company and American intelligence agencies negatively impacting Twitter's efforts to grow its business in various overseas markets.

This situation highlights why elements of the United States Intelligence Community require not only more direct, but also guaranteed access to both the data generated on social media sites and tools used to navigate it for the purposes of identifying prospective threats to national security. Indeed, policymakers should consider developing legislation that requires American companies managing social media and file-sharing platforms to provide, in the very least, counterterrorism practitioners in the United States Intelligence Community access to all data generated on their platforms in the manners their platform administrators may observe it in real time, as well as tools required to rapidly navigate this data to identify potential threats. This, in turn, can help to further deter terrorists from exploiting these companies' technologies. Because there is much evidence which suggests employees of these companies do not possess expertise with, for example, Salafiyya Jihadiyya sufficient to identify much of the material hosted and promoted on their sites to generate buy-in for this toxic ideology.

[5] Link to material: https://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682

Salafiyya Jihadiyya is the ideology which informs the agendas of Islamic State, al-Qa'ida and other Salafi-Jihadist elements, which, collectively, pose as one of the greatest sources of terrorist threats to global security. Once adopted, this ideology imbues adherents with a sense of urgency to "defend" their faith vis-à-vis support for terrorism campaigns waged against Americans and our allies.

While YouTube's recent decision to remove all content featuring guidance provided by the American-born al-Qa'ida cleric Anwar al-Awlaki is to be commended, there remains an abundance of material from which groups like al-Qa'ida and Islamic State derive similar utility on this and other popular file-sharing platforms operated by American companies and Archive.org, a website managed by a United States-based nonprofit organization that has for years been an online clearinghouse for terrorist propaganda and a preferred point of initial online distribution for official Islamic State propaganda. As I noted in my prepared testimony for the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing, at the time of this hearing, one could also easily find materials featuring guidance by deceased Islamic State cleric Turki al-Bin'ali on YouTube.

As I also noted in my written testimony, many materials used by recruiters from Salafi-Jihadist groups to remotely cultivate support for their cause over the Internet do not contain messaging and imagery that violate most popular social media and file-sharing platforms' policies, such as, for example, threats of violence and scenes of terrorists committing violent crimes. Identifying this material requires rich subject matter expertise, as well as, in some cases, access to federal agencies' investigative resources that can be used to refine understandings of a disseminator's motives.

Indeed, as there is considerable overlap in the fundaments of Salafiyya Jihadiyya and the most prominent of the doctrines which inform how members of Islam's largest sect understand their faith (i.e., the Salafi doctrine that has for decades been aggressively promoted globally by the Kingdom of Saudi Arabia's Wahhabi school), rich subject matter expertise is often required to distinguish between "extremist" and mainstream guidance concerning how Sunni Muslims should demonstrate adherence to their professed faith through their actions.

For example, some ancient authoritative reference materials that have been converted into tools used to build support for Salafi-Jihadist groups like al-Qa'ida and Islamic State, such as the works of the 13th-14th Century Damascus-based theologian and Hanbali jurist Taqi al-Din Ahmad Ibn Taymiyyah, were channeled by the founder of the Wahhabi school as he developed a framework for legitimizing a decades-long, often violent revolutionary program that culminated in the establishment of the Kingdom of Saudi Arabia, whose very standard—upon which is emblazoned a sword—serves as a reminder that religiously-motivated militancy is featured prominently in Islamic history. To the casual observer, certain lectures focused on Ibn Taymiyyah's three anti-Mongol *fatawa* (religious edicts) that have inspired the intensely sectarian policies of Saudi Arabia and, more recently, Islamic State, and which have meanwhile inspired much of the support for jihad theaters like the one in Syria from mainstream religious authorities in the Middle East and other regions may simply appear as history lessons. However, in some cases, these materials are used to help stimulate thinking among individuals residing far from so-called "historically Muslim lands" about the question of whether tenets of their faith and early traditions of the faithful compel them to support terrorism campaigns waged against not only so-called “apostate” governments, as Salafi-Jihadist groups describe them, in the Middle East and other majority-Muslim regions, but also these governments’ allies in the West, along with the civilian populaces from which governments in the West derive power. Indeed, most of these materials contain messaging which is subtler than the calls for attacks targeting, for example, female American voters contained in the flyer Islamic State distributed using social media platforms like Twitter days prior to the 2016 presidential election in the United States.[6]

Similar utility is derived from special editions of works by Mohammed ibn Abd al-Wahhab, the founder of the Wahhabi school, that have been prepared and distributed online by Islamic State to help support the group’s arguments that contemporary Saudi religious and political leaders have deviated from al-Wahhab’s *manhaj* (methodology). Thus, according to Islamic State, and other terrorist groups, Saudi religious and political leaders are neither exemplars, nor stewards of the “pure” faith, and their policies are described by an array of Salafi-Jihadist elements as reflecting deviations from centuries-old Islamic legal constructs that have served to limit the influence of “unIslamic” elements, such as secularist Western nations, within Islamic societies. According to Islamic State and other Salafi-Jihadist groups, it is in consideration of such alleged deviations that, in accordance with the logic of Ibn Taymiyyah that was channeled by al-Wahhab, faithful Muslims should regard Saudi authorities’ rule over lands comprising Islam’s holiest sites as unacceptable. Moreover, according to Islamic State, adherents of the “pure” faith are compelled to wage jihad against Saudi Arabia’s clerical and political establishments to expunge “unIslamic” influence from the country’s system of governance by force.

Of course, the same works by al-Wahhab that are being leveraged by Islamic State to legitimize its calls for terrorist attacks in Saudi Arabia can be found for sale in legally-operated online Islamic bookstores. Meanwhile, these and other works comprising the corpus of ancient authoritative reference materials which are leveraged by “extremist” and mainstream clerics to guide the activities of their faithful followers are common foci of lectures broadcast globally online, with promoters of these materials often using American companies’ file-sharing sites to grow audiences for these religious educational materials here in the West.

Discerning the intended effects of such media on certain audiences is not an area of work in which most tech companies’ employees possess substantial experience. Nor, for that matter, do most tech companies’ employees have access to additional resources, such as information from ongoing terrorist recruitment-focused investigations, which may be needed to understand the motives of some individuals who promote mainstream Islamic educational materials while concomitantly proffering analyses of these materials for the purposes of helping to cultivate support for terrorist elements.

It is therefore advisable for the Executive Branch to direct the Office of Director of National

[6] See example of the promotion of Islamic State’s flyer titled “The Murtadd Vote” on Twitter in Michael S. Smith II, Social Media Jihad 2.0: Inside ISIS’ Global Recruitment and Incitement Campaign, New America, January 18, 2017, Beginning at 26:40. Briefing footage available at https://www.youtube.com/watch?v=vEOVd7oszSs

Intelligence to organize a section within the Open Source Enterprise (OSE)[7] tasked with advising American and foreign companies about the presences of all such materials on their platforms used to generate buy-in for Salafiyya Jihadiyya which can be identified by open source intelligence collection specialists and analysts who possess expertise with terrorist propaganda. This section should also work to identify materials used to persuade adoption of ideologies promoted by other terrorist and extremist elements of concern to national security managers.

Here, I would be remiss in not stating it is imperative for all members of the Senate Committee on the Judiciary and your staffs to establish accounts for access to the massive cache of materials archived by OSE in its online database that highlight the nearly decade-old problem of terrorists exploiting American companies' social media and file-sharing platforms. Additionally, I believe all of this material, and translations thereof, that is archived by OSE should be made available to academics and think tank employees working to improve understandings of groups like Islamic State and al-Qa'ida while also helping policymakers and counterterrorism practitioners identify opportunities to more effectively reduce these terrorist groups' influence capacities. Indeed, all of these materials that have been collected and translated by OSE could be crucial tools for use in training more subject matter experts and terrorism analysts who can assist both government agencies and private sector entities with their efforts to degrade the influence capacities of terrorist groups like Islamic State. Here, it is also important for policymakers to consider that, by increasing access to these materials for trusted parties outside of government, the federal government could reduce expenditures on duplicative activities. Presently, various federal entities are funding an array of separate research efforts that entail collecting and translating online terrorist propaganda. This year, I provided data collection support to one such unclassified effort that is funded by grants awarded to academics by the Department of Defense's Minerva Research Initiative. Given that OSE is simultaneously collecting and translating these materials, some taxpayers might view funding for the Minerva Research Initiative-funded research project I was employed to support as wasteful spending. Further, as terrorist propaganda collected and processed by OSE translators is not copyright protected, and as its collection rarely requires use of classified technologies due to the fact this material is easily accessible on popular file-sharing websites, policymakers should take issue with the fact it is not being made readily available to experts and analysts working outside of government whose perspectives are frequently sought by policymakers and counterterrorism practitioners employed by our government. Meanwhile, this material has been made available to foreign governments, and classification of most of this material is so low that employees of state and local governments in the United States who do not possess security clearances required to review materials marked SECRET and above may establish OSE accounts.

As highlighted in your next question, Senator Feinstein, evidence used to support a large body of terrorism-related cases here in the United States demonstrates social media and file sharing-platforms have become crucial points of transfer into America's homeland of ideological indoctrination-oriented materials and other "soft" tools which have enabled terrorists located overseas in places like Yemen and Syria to groom sympathizers to perpetrate attacks here. As most employees of American Internet technology companies clearly do not possess expertise

[7] Originally named the Open Source Center (OSC).

sufficient to identify much of the activity on their platforms whose illicit characters can be more easily discernible among professionals in the United States Intelligence Community, one possible way to address this deficiency in a manner that could simultaneously help to more effectively disrupt and deter terrorists' exploitations of these companies' technologies is to organize units of federal agents to work alongside employees of companies like Twitter, Facebook and Alphabet who are tasked with monitoring activities on their respective platforms in real time to identify violations of their policies, including criminal activities.

Here, policymakers should consider that, in the post-9/11 era, the federal government has oriented previously unimaginable resources to safeguard against terrorists achieving reach into America's homeland through our nation's airports and seaports. These resources have included not only an ever-expanding array of detection technologies, but also agents of various federal entities which possess mandates to defend the nation against foreign and domestic threats. The absence of similar security postures for spaces of the Internet commonly used by terrorist elements to achieve influence within the United States is indeed remarkable.

Civil Injunction Authority Related to Terrorism

2. As you know, there is a relentless and growing ISIL recruitment effort through social media platforms. Recruitment is repeatedly identified in nearly all of the 100+ criminal indictments brought by federal authorities during the past two years relating to ISIL. Anwar al-Awlaki is frequently named as one of the inspirational sources in many of these indictments. I understand that civil injunction authority exists for the Attorney General to obtain orders against those who provide material support to a foreign terrorist organization, as well as to shut down websites from distributing software for spying on people.

    a. Do you believe that this type of civil injunction authority could help prevent terrorists and extremists from using tech platforms to commit crimes?

Answer by Michael S. Smith II:

I believe the threat of such actions may help to encourage the owners of social media and file-sharing platforms to do more to disrupt the persistent conversions of their technologies into tools used to support the global recruitment and incitement campaigns waged online by Islamic State and other terrorist groups. Further, I believe it is necessary for Congress and President Trump to do more to encourage and, should such encouragement fail to produce desired results, compel managers of spaces of the Internet where terrorist elements and other adversaries have been especially active to do more to disrupt and deter uses of their technologies and popular platforms to threaten Americans and our allies.

During a conference call with me in September 2017, the National Security Council staffer tasked with drafting the forthcoming National Security Strategy (NSS) indicated she intended to leverage a portion of input provided in my written testimony for the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing to draft a section of the NSS concerning the issue of terrorists' online recruitment and incitement activities. Further, this staffer indicated the Trump administration would likely be willing to use the forthcoming NSS to highlight what American companies that operate popular social media and file-sharing platforms could do to help to more effectively disrupt and deter exploitations of their technologies by terrorist groups like Islamic State. However, this staffer advised legislation which seeks to impose policies on these companies is likely to be viewed within the Executive Branch as being anathema to the Trump administration's larger agenda, as President Trump has often noted he intends to cut government regulations on private industries.

I believe any resistance from the Executive Branch to legislation which seeks to both help and compel the aforementioned companies to more effectively manage terroristic and other threats to America's national security emanating from popular spaces of the Internet managed by them would serve as an indication President Trump does not understand the threat environment. This has already been suggested by President Trump's response to the terrorist attack in New York that occurred during the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing.

As I noted in my opening remarks for this hearing, so-called "chatter" focused on this attack that erupted during the hearing on spaces of the cyber domain where Islamic State is particularly active—specifically, Telegram Messenger channels I was able to observe during the hearing using my smartphone—indicated there may have been a linkage to the group. Indeed, soon thereafter, this became the eighth attack in the United States claimed by Islamic State since it declared its so-called "caliphate" in mid-2014. Further, as investigators quickly determined, materials found on the cell phone of the terrorist responsible for this attack indicate he consumed a large amount of Islamic State propaganda that was published online. Despite this, President Trump reiterated his view that immigration policy recalibrations—not policies which can help disrupt Islamic State's online recruitment and incitement program—are required to protect Americans against threats posed by Islamic State.

This suggests President Trump's advisors have not explained to our commander-in-chief that, as noted in my testimony, Islamic State has achieved a power of persuasion over the Internet which is far more impactful than any terrorist groups presently calling for their sympathizers to perpetrate attacks in the United States. The president's response also suggests his advisors may not yet recognize denying Islamic State capacity to govern territory in its original primary areas of operation has clearly not had the effect of significantly degrading the group's capacity to command violence in the United States and other countries in the West over the Internet.

Here, I believe policymakers providing oversight of the various entities comprising America's national security enterprise should consider false optimism concerning the impact of overseas counterterrorism campaigns has not been uncommon in senior echelons of America's national security enterprise and the Executive Branch. During a meeting in December 2014 with then Special Presidential Envoy to the Global Coalition to Counter ISIL General John Allen, USMC (Ret), I learned the Obama administrations' policies were guided by an assumption Islamic State would implode during 2015 due to increased military pressure applied against the group in its original primary areas of operation in Iraq and Syria. Years prior, in its National Strategy for Counterterrorism that was published just after al-Qa'ida's founding leader was killed, the Obama administration advised: "Since the beginning of 2011, the transformative change sweeping North Africa and the Middle East—along with the death of Usama bin Ladin—has further changed the nature of the terrorist threat, particularly as the relevance of al-Qa'ida and its ideology has been further diminished."[8]

Today, however, Islamic State claims to be stewarding the jihad charted by bin Ladin, in which attacks targeting Americans and Europeans were used as tools to endear al-Qa'ida to inhabitants of majority-Muslim regions whose worldviews are shaped by decades-, sometimes even centuries-old grievances concerning the influence of secularist Western governments in their homelands. To achieve such results, Islamic State has continued using tools like YouTube and Google Drive to promote propaganda engineered to help the group build and reinforce support here in the United States. Meanwhile, as noted in my written testimony and the Department of Justice's complaint against the terrorist responsible for the attack in New York that occurred during the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing, Islamic State has devolved directives for the execution of attacks in the United States in its online propaganda. Indeed, the type of attack executed in New York on October 31, 2017 conforms to directions provided in Islamic State propaganda referenced in my hearing testimony.

Without the imposition of policies which will more effectively deter terrorists from persisting with their uses of social media platforms to recruit and incite violence, it is almost certain Islamic State recruiters will continue using social media platforms like Twitter and Facebook to identify individuals who may be groomed over the Internet to perpetrate attacks targeting Americans and civilian populaces of other countries in the West, especially those of the United Kingdom, France, Germany, Canada, and Australia. During the coming years, without a more practical effort—guided by legislation informed by inputs from the most knowledgeable national security managers, counterterrorism practitioners and terrorism analysts—to reshape the online operating environment in which terrorists have found it so easy to maneuver while remotely mobilizing attacks from places like Syria and Yemen, it is very likely al-Qa'ida and other Salafi-Jihadist elements will also use American companies' technologies to expand their capabilities to further threaten Americans and our allies here in the West.

Again, I believe policymakers should do everything possible to encourage a more impactful set of responses from American firms to the persistent issue of terrorist elements exploiting their technologies to advance violent extremist agendas at the expense of United States' and allied nations' national security interests. Additionally, I believe more could and should be done by policymakers in Congress, as well as President Trump, to pursue such outcomes than developing policies which simply increase threats of civil injunctions against major American Internet companies like Facebook, Twitter and Alphabet. Nearly a decade after the American-born al-Qa'ida cleric Anwar al-Awlaki began using Facebook and YouTube to recruit and incite violence within the United States from Yemen, this set of problems has not been effectively addressed by these and other American companies. Therefore, policymakers should be skeptical of any commitments from these companies to do all they possibly can to safeguard against activities on their platforms that threaten the security of Americans and our allies.

[8] Link to material: https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf

Senate Judiciary Committee
Subcommittee on Crime and Terrorism
"Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions"
Questions for the Record
October 31, 2017
Senator Amy Klobuchar

Question for Michael Smith, Terrorism Analyst
As you correctly noted in the hearing, ISIS has claimed credit for a number of terrorist attacks in the United States—including one that left 10 injured at a shopping mall in St. Cloud, Minnesota last year.

- What have we learned from these types of tragic incidents so that we can track similar behavior and prevent other attacks like this in the future?

Regrettably, time provided to reply to this and other questions presented to me by members of the Senate Committee on the Judiciary is not sufficient for me to cover the very long list of lessons learned pursuant to terrorist attacks like the aforementioned attack in Minnesota. Meanwhile, with this reply to your question, I will attempt to cover several matters which I believe should be of interest to members of the Committee and other policymakers.

Firstly, we have learned the Global Jihad movement, in which al-Qa'ida and Islamic State have competed for dominance since 2014, is a far more durable source of threats to global security than was recognized by senior national security officials in the Obama administration, which presented the public the following assessment in the 2011 National Strategy for Counterterrorism: "Since the beginning of 2011, the transformative change sweeping North Africa and the Middle East—along with the death of Usama bin Ladin—has further changed the nature of the terrorist threat, particularly as the relevance of al-Qa'ida and its ideology has been further diminished."[1] As noted in my responses to Senator Feinstein's questions and in my written testimony for the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing: Today, however, Islamic State claims to be stewarding the jihad charted by bin Ladin, in which attacks targeting Americans and Europeans were used as tools to endear al-Qa'ida to inhabitants of majority-Muslim regions whose worldviews are shaped by decades-, sometimes even centuries-old grievances concerning the influence of secularist Western governments in their homelands.

To achieve leadership status in the Global Jihad movement, Islamic State has used American companies' popular social media and file-sharing platforms to promote propaganda engineered to help the group build and reinforce support here in the United States. Meanwhile, as noted in my written testimony and the Department of Justice's complaint against the terrorist responsible for the attack in New York that occurred during the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing, Islamic State has devolved directives for the execution of attacks in the United States in its online propaganda. Indeed, the

[1] Link to material: https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf

type of attack executed in New York on October 31, 2017 conforms to directions provided in Islamic State propaganda referenced in my hearing testimony. Since September 2014, when Islamic State began petitioning for supporters to perpetrate attacks in the West, so too have numerous other failed and successful attack plots in the United States. Among which are attacks not claimed by Islamic State, despite their perpetrators having explicitly stated their actions were meant to demonstrate their willingness to fulfill directives issued in Islamic State propaganda.

There are ample indications Islamic State has achieved a power of persuasion sufficient to remotely accelerate the radicalization process over the Internet. Furthermore, the attack in New York on October 31, 2017 indicates that denying Islamic State capacity to govern civilian populaces in its original primary areas of operation may not serve to substantially diminish its leader's and his proxies' capabilities to command violence within the United States.

These and other factors indicate it is necessary for policymakers to recalibrate priorities of intelligence and law enforcement agencies in order to emphasize disruption of terrorists' online activities over monitoring these activities, as well as over engagement in online counter-messaging programs.

In addition, the power of persuasion achieved by Islamic State through its online recruitment and incitement program suggests there is a need to adjust policies governing how FBI and other agencies evaluate prospective threats to public safety posed by American citizens who are suspected sympathizers of Islamic State and other Salafi-Jihadist groups like al-Qa'ida. In the very least, policymakers should help to ensure the Department of Justice can increase timelines for FBI's investigations aiming to determine whether Americans are sympathetic to Islamic State and other terrorist elements. As members of this committee are aware, various protocols continue to constrict FBI's abilities to both identify and disrupt otherwise possibly foreseeable criminal activities perpetrated by Americans susceptible to the influence of foreign terrorist organizations.

I believe it is especially important for members of this Committee to consider that the successes Islamic State has achieved with its aggressive online recruitment and incitement program can serve to stimulate interests among other terrorist groups in waging similarly aggressive online campaigns aiming to persuade individuals located within the United States to perpetrate attacks here. Meanwhile, as I noted in my opening remarks for the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing, the ease with which Islamic State has exploited American companies' social media and file-sharing platforms to recruit and incite violence within the United States very likely influenced Russian intelligence officials' calculations when assessing the feasibility of plans to harness these companies' technologies to undertake their influence operation targeting American voters. Given the enthusiasm Islamic State has cultivated for its agenda through its online influence campaign, policymakers should consider that it would be very easy for agents of hostile governments, such as the governments of Russia and Iran, as well as members of competing terrorist groups like al-Qa'ida, to capitalize on such enthusiasm by posing as Islamic State recruiters and grooming Islamic State sympathizers to function as patsies in their wider efforts to undermine our national security.

In effect, among the most important lessons learned from attacks like the one Islamic State has claimed responsibility for in Minnesota is that an absence of laws that compel companies like

Facebook, Twitter and Alphabet, the parent company of YouTube and Google Drive, to implement policies that will make their technologies less attractive tools for terrorists, other illicit actors, and agents of hostile governments has rendered Americans more vulnerable to threats posed by these elements. In addition, the persistent exploitations of these and other American companies' technologies by Islamic State and other terrorist groups has highlighted the need for laws which help to guide a reshaping of the online operating environment in which terrorists and other adversaries have found it so easy to maneuver while threating the safety and security of Americans and our allies. As I noted in my responses to Senator Feinstein's questions, policymakers should be skeptical of any commitments from these companies to do all they possibly can to safeguard against activities on their platforms that threaten the security of Americans and our allies.

Michael Smith – Extremist Content and Russian Disinformation Online
Questions for the Record
Submitted November 7, 2017

QUESTIONS FROM SENATOR COONS

1. Foreign entities will continue to try to use social media to interfere with U.S. elections. What actions would you recommend that the Executive Branch take to combat Russian interference?

Answer by Michael S. Smith II:

I would recommend the Executive Branch call upon Congress to develop legislation which serves to address not only the scope of vulnerabilities referred to with this question, but also threats posed by terrorists and other illicit actors which have converted American companies' social media and file-sharing platforms into tools used to threaten the safety and security of Americans and our closest allies. For information concerning topics which I believe policymakers should contemplate while developing such legislation, please reference my written answers to Senator Feinstein's questions.

Not contemplated in those answers is the issue of bots being used by America's adversaries to wage influence campaigns on social media platforms. The impact of bot use by agents of Russia's online influence operation targeting American voters suggests it may be necessary to develop legislation that serves to require social media companies to develop new features of their infrastructure which could help deny access to their platforms for bots used by illicit actors and agents of hostile foreign governments.

As noted in my replies to Senator Feinstein's questions, I believe any resistance from the White House to legislation which seeks to both help and compel American companies to more effectively mitigate threats to America's national security emanating from popular spaces of the Internet managed by Facebook, Twitter, Alphabet and other companies would serve as an indication President Trump does not understand the threat environment. This has already been suggested by President Trump's response to the terrorist attack in New York that occurred during the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism's October 31, 2017 hearing. Specifically, President Trump reiterated his view that immigration policy recalibrations—not policies which can help disrupt Islamic State's online recruitment and incitement program—are required to protect Americans against threats posed by Islamic State. Here, I believe it is important for policymakers to consider that, if tons of banned narcotics and thousands of people can be smuggled into the United States each year, it is very likely a well-resourced terrorist group like Islamic State could move dozens of trained terrorists into the United States via routes not subject to federal inspection. Also important to consider is that Islamic State has not needed to resort to such measures for the purposes of meeting expectations set in its propaganda that it will kill Americans in our homeland. Indeed, Islamic State has repeatedly demonstrated it is not necessary to move trained terrorists into America's homeland from such countries as Syria in order to mobilize attacks against American civilians. Clearly, such results can be produced remotely vis-à-vis the group's exploitation of American companies' social media and file-sharing platforms to build support here while orienting supporters' interests towards executing attacks like the deadly attack that occurred in New York on October 31, 2017. In addition, I believe President Trump's various comments concerning Russia's recent online influence operation targeting American voters indicate the president's national security advisors have failed to effectively inform our commander-in-chief's understandings of both the domestic and global implications of that situation, along with the potentially deleterious consequences his comments about these matters could have for our nation's relationships with America's most reliable allies.

Pursuant to a conference call I held in September 2017 with the National Security Council staffer tasked with drafting the forthcoming National Security Strategy, which is referenced in both my written testimony and written answers to Senator Feinstein's questions, I believe President Trump does not grasp the following issue: Past actions of American companies whose social media and file-sharing platforms have been exploited by terrorists and, more recently, Russian agents to wage influence campaigns for the purposes of undermining the national security of the United States and allied nations provide ample indicators these companies are unlikely to do all they can to address these problems unless new laws are introduced to compel them to more effectively disrupt and deter such uses of their technologies.

Ultimately, if one wishes to develop a sense of how some American social media companies' policies do not reflect sufficient attention to the wide-ranging concerns of American national security managers, one might consider that Twitter has provided the account managed by Edward Snowden Twitter's cache "verified" status, and his Twitter account has amassed a following of more than 3.5 million accounts. Arguably, that Mr. Snowden is allowed to operate a Twitter account in the first place suggests Twitter is disinterested in the concerns of many American national security managers, and especially those who may view Mr. Snowden's apparent popularity—the perceptibility of which is enhanced by his massive following on Twitter—as an issue which may serve to encourage young Americans with access to our nation's top secrets to emulate Mr. Snowden's behaviors that have enabled him to attain pseudo-celebrity status.

2. Is legislation necessary to confront the ongoing threat of Russian propaganda and ISIS propaganda on social media platforms?

Answer by Michael S. Smith II:

I believe policymakers should develop legislation which compels American Internet companies to implement a variety of policies that can at once serve to disrupt and deter terrorists' activities on social media and file-sharing platforms that pose as serious threats to not only America's national security, but also global security. This legislation should be developed to safeguard Americans and our allies against a range of other activities in the cyber domain, including the type of online influence operation managed by Russia during the last election cycle. As noted in my written replies to Senator Feinstein's questions, I believe such legislation should also seek to encourage foreign social media and file-sharing sites to impose uniform sets of policies by denying United States-based advertisers and account users abilities to utilize their platforms should they refuse to impose policies deemed necessary to safeguard against threats posed by terrorists and other illicit actors of interest to national security managers.

3. Social media companies have announced reforms intended to identify fake accounts and pages and increase scrutiny of ad purchases. Do you believe those proposals are sufficient?

Answer by Michael S. Smith II:

No. Furthermore, I do not believe the companies of concern will do all they possibly can to address these and other issues of concern to America's national security managers unless policymakers develop legislation which both guides and compels a more effective approach to mitigating threats to our national security emanating from spaces of the Internet managed by them.

4. In your view, are social media companies overly reliant on algorithms and computer intelligence to detect and prevent content from foreign adversaries?

Answer by Michael S. Smith II:

The companies whose technologies have been so aggressively exploited by United States-designated foreign terrorist organizations, foreign adversaries and other illicit actors to harm Americans and our allies have not been transparent about the full scope of their effort to address such issues. Therefore, I am unable to answer this question. Meanwhile, as noted in my written replies to Senator Feinstein's questions, it is clear that none of the measures taken to attempt to prevent the exploitations of these companies' technologies by terrorists engaged in efforts to incite violence within the United States over the Internet have effectively deterred United States-designated foreign terrorist organizations—notably Islamic State—from persisting with their efforts to convert American social media and file-sharing platforms into tools used to expand their capabilities to threaten Americans and our allies. As noted in my responses to Senator Feinstein's questions, I do not believe most employees of companies managing popular social media and file-sharing platforms possess expertise with an array of ideologies and activities of concern to national security managers sufficient to enable these companies to identify much of the activities on their platforms which pose as sources of threats to Americans and our allies. In my answers to Senator Feinstein's question, I have also stated the following: As most employees of American Internet technology companies clearly do not possess expertise sufficient to identify much of the activity on their platforms whose illicit characters can be more easily discernible among professionals in the United States Intelligence Community, one possible way to address this deficiency in a manner that could simultaneously help to more effectively disrupt and deter terrorists' exploitations of these companies' technologies is to organize units of federal agents to work alongside employees of companies like Twitter, Facebook and Alphabet who are tasked with monitoring activities on their respective platforms in real time to identify violations of their policies, including criminal activities.

5. How do we prevent propaganda from masquerading as real news, while ensuring that we do not infringe upon the First Amendment?

Answer by Michael S. Smith II:

The first step in any such efforts must entail developing an operational definition for the term “fake news” for policymakers to use in your efforts to address this phenomenon.

The following definition I developed for undergraduate students enrolled in a class offered by Georgia State University’s Communication Department that I am presently teaching may be useful:

Fake News: A term used to refer to disinformation presented in manners that mimic deliveries of information by credible sources, such as major news organizations, and which is intended to persuade consumers to engage in activities the disseminator deems helpful to the advancement of an agenda typically characterized by political, economic and social interests, or any combination thereof.

Next, I believe policymakers should consider developing legislation which can more effectively address the witting online dissemination of “fake news” for such purposes as those discernible from the influence operation waged by Russia during the recent election cycle, as well as the influence operations waged online by terrorist organizations like Islamic State. Indeed, Islamic State’s claims it has restored a “caliphate” and established 16 “provinces” beyond Iraq and Syria are glaring instances of “fake news” being used to persuade certain segments of the group’s worldwide audience in the cyber domain to perceive Islamic State as being worthy of support, including in the form of terrorist attacks perpetrated in the United States. Without policymakers developing a legal framework to more effectively disrupt and deter such activities, it is likely terrorists and other adversaries will persist with their exploitations of popular social media and file-sharing platforms to wage influence operations at the expense of United States’ and allied nations’ national security interests.

Meanwhile, such legislation should contemplate instances of unwitting support for “fake news” campaigns. As unwitting support for “fake news” campaigns highlights media literacy factors importantly in Americans’ abilities to discern what is/not “fake news” developed, for example, to undermine the integrity of our electoral system, I believe any legislation developed to address this phenomenon should provide more resources for media literacy programs in middle schools, high schools, and at our nation’s colleges and universities.

6. During the hearing, when asked whether the United States is prepared to handle threats posed by foreign adversaries’ interference using social media and violent extremism online, you stated, “I believe that [dealing with these threats] could be accomplished in very short order. . . . We have the capability.”
   a. In terms of foreign adversaries’ interference using social media, what are our most exploitable weaknesses? What steps can private companies take to fix them? What can Congress do to address them?
   b. In terms of violent extremism online, what are our most exploitable weaknesses? What steps can private companies take to fix them? What can Congress do to address them?

Answer by Michael S. Smith II:

Please see my written replies to Senator Feinstein’s questions. Please also review my written testimony for additional input on how social media and file-sharing platforms have been converted into tools used to threaten the safety and security of Americans and our closest allies.

7. In January, Senator Gardner and I introduced a bipartisan resolution to establish a Select Committee on Cybersecurity (S.Res. 23), which Senators McCain and Blumenthal have cosponsored. Do you support this bill to create a Select Committee on Cybersecurity? If not, how can it be improved?

Answer by Michael S. Smith II:

Yes, I support the establishment of a Select Committee on Cybersecurity. Meanwhile, I welcome opportunities to work with you and your colleagues to examine ways this bill could be improved. That it is necessary to contemplate creation of such a committee highlights the persistent issue of deficient strategic analysis against terrorists and other adversaries in policymaking spheres. I am confident this bill can benefit from additional input offered by knowledgeable and talented national security professionals and tech industry experts who are already working to address certain issues which are likely to be of paramount concern for members of this proposed new committee.