A PLAN FOR PREVENTING AND COUNTERING TERRORIST AND VIOLENT EXTREMIST EXPLOITATION OF INFORMATION AND COMMUNICATIONS TECHNOLOGY IN AMERICA

AUDREY ALEXANDER
SEPTEMBER 2019

About the Program on Extremism
The Program on Extremism at George Washington University provides analysis on issues related to violent and non-violent extremism. The Program spearheads innovative and thoughtful academic inquiry, producing empirical work that strengthens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions that resonate with policymakers, civic leaders, and the general public.

About the Author
Audrey Alexander is a research associate and instructor at the Combating Terrorism Center at West Point. She started and finished most of this project while a senior research fellow at the Program on Extremism at George Washington University.

The views expressed in this paper are solely those of the author, and not necessarily those of the Program on Extremism or the George Washington University.

Acknowledgements
The author would like to thank Lorenzo Vidino and Seamus Hughes for their support of this brief and the broader Program on Extremism policy paper series. Additional thanks to the entire team at the Program on Extremism, along with the external reviewers, for their feedback, advice, and encouragement.

Executive Summary

Policymakers in the United States know that terrorists and violent extremists exploit information and communications technologies (ICTs), but the government still struggles to prevent and counter these threats. Although the U.S. does not face these challenges alone, the strategies and policies emphasized by some of its greatest allies are not viable or suitable frameworks for domestic policymakers. Since these threats persist, however, the U.S. government must develop a cohesive strategy to prevent and counter terrorist and violent extremist exploitation of ICTs. The approach should rest on the pillars of pragmatism, proportionality, and respect for the rule of law, and aim to disrupt terrorist and violent extremist networks in the digital sphere. To pursue this objective, the following brief calls for political leaders to create an interagency working group to formalize leadership and conduct a comprehensive assessment of terrorist and violent extremist abuse of ICTs. The evaluation must also weigh the costs and benefits associated with responses to these threats. Then, government officials should work to enhance the capability and coordination of government-led efforts, pursue partnerships with non-governmental entities, and facilitate productive engagements with the technology industry. In short, this approach would allow the government to use legislation, redress, and strategic outreach to empower more players to responsibly prevent and counter terrorist and violent extremist exploitation of ICTs.

Introduction*

On May 15, 2019, several world leaders and technology providers signed onto the Christchurch Call, a pledge to tackle terrorist and extremist violence online.[1] Arising two months after a terrorist live-streamed the shootings that killed 51 people within the Muslim community of Christchurch, New Zealand, the Call sought to unite various governments and online service providers "to *eliminate* terrorist and violent extremist content online."[2] State signatories of the non-binding pledge include Australia, Canada, the European Commission, France, Germany, Indonesia, India, Ireland, Italy, Japan, Jordan, the Netherlands, New Zealand, Norway, Senegal, Spain, Sweden and the United Kingdom.[3] The United States did not sign onto the Call, though U.S. representatives attended the summit to support the broader effort.

The White House explained the decision to abstain from the pledge with the following statement:

> "While the United States is not currently in a position to join the endorsement, we continue to support the overall goals reflected in the Call. We will continue to engage governments, industry, and civil society to counter terrorist content on the Internet" … "We continue to be proactive in our efforts to counter terrorist content online while also continuing to respect freedom of expression and freedom of the press" … "Further, we maintain that the best tool to defeat terrorist speech is productive speech, and thus we emphasize the importance of promoting credible, alternative narratives as the primary means by which we can defeat terrorist messaging."[4]

The U.S. government's history of abstention from agreements that brush up against the First Amendment made its decision not to formally endorse the Christchurch Call relatively unsurprising.[5] However, the choice elicited an array of responses.[6] Despite differences in opinion, many commentators concluded that the U.S. should still do something to confront the dangers posed by terrorist and violent extremist exploitation of information and communication technologies (ICTs). Given the high-stakes of policy decisions concerning this matter, namely security, speech, and privacy, action for the sake of action is perilous. Since the cost of measures to address terrorists and violent extremists in the digital sphere could potentially outweigh the benefits, key tradeoffs require thorough consideration. In order to support the decision-making process, the following policy brief proposes a roadmap to prevent and counter terrorist and violent extremist abuse of ICTs in America. This approach pushes the government to develop a plan to pragmatically and proportionally confront these threats as they persist and evolve. Even without formally signing onto the Christchurch pledge, the U.S. can create a plan to prevent and counter terrorist and violent extremist exploitation of ICTs and reassure allies by demonstrating commitment to this agenda.

Although domestic policymakers emphasize issues concerning social media and the Internet, and identify meaningful actions to address the problem, past and present national security and counter-terrorism strategies lack sufficient mandates to coordinate a policy agenda to prevent and counter terrorist and violent extremist exploitation of ICTs in America.[7] Over time, this resulted in cursory responses to long term, dynamic threats, and the government struggled to develop meaningful partnerships with civil society and the technology industry. In order to chart a more practical course of

* For the sake of scope and clarity, this policy brief discusses the future of efforts to prevent and counter terrorist and violent extremist exploitation of information and communication technologies (ICTs) in the United States. The brief uses the phrase "prevent and counter terrorist and violent extremist exploitation of ICTs" because it best represents the spectrum of proactive and reactive measures the government may leverage to mitigate different threats posed by ideologically-motivated violence in the U.S.

action, the U.S. must fully comprehend the issue and discern the U.S. government's role in directing and facilitating efforts to intervene in the exploitation of ICTs.

This brief posits that political leaders should make "marginalization strategy"[8] their guiding principle, and push for policies and laws that advance a strategic approach to prevent and counter terrorists and violent extremists in the digital sphere.[9] If policymakers rest on the pillars of pragmatism, proportionality, and the rule of law, they can identify new ways to tackle the threats posed by the exploitation of ICTs. In application, decisionmakers would pursue options that inflict the least harm to achieve beneficial outcomes. By striving to mitigate rather than eliminate terrorist and violent extremist activity online, U.S. political leaders can develop a more holistic approach that addresses the ecosystem of platforms and players that comprise nefarious social networks. Pursuing this objective requires the government to mandate efforts to identify measures to weaken the influence of violent extremists online, and task an entity capable of coordinating and facilitating efforts to prevent and counter violent extremist exploitation of ICTs. With this approach, the government can use legislation, redress, and strategic outreach to help coordinate and capacitate the range of actors against the exploitation of ICTs, empowering critical players such as civil society groups and private companies.

Background

Before delving into a discussion about how the U.S. government can configure an alternative approach to prevent and counter terrorist and violent extremist exploitation of ICTs, it is useful to review the nature of the problem, discuss contemporary trends, and examine past and present efforts to address the digital networks of terrorists and violent extremists in the U.S. and abroad.

As a starting place, while there is some utility in discussing the "online" and "offline" spheres as distinct spaces, the digital and physical arenas are inextricably linked. Challenges facing the security community writ large, such as establishing jurisdiction or defining what constitutes terrorism and violent extremism, can affect how policymakers and practitioners confront threats involving ICTs.[10] Although the terms "internet radicalization" and "online radicalization" arise in discourse and about cases involving ICTs, these labels do not sufficiently account for the underlying causes and precipitants of radicalization.[11] The security community broadly recognizes that technologies have some relationship with violent extremism and terrorism, but the nature of that relationship remains subject to debate and requires further investigation.[12] Put simply, "the extent to which extremists utilize social media, and whether it influences terrorist outcomes, is still poorly understood."[13] Even if a few trends are discernable, the lack of consensus regarding the precise effects of technology on terrorists and violent extremists suggests that there is not one monolithic relationship between individuals, organizations, tools, and ideas.[14]

Terrorist and violent extremist exploitation of ICTs is not a new phenomenon, and contemporary assessments of this problem are not unlike the observations some analysts articulated more than a decade ago.[15] Much research focuses on the use of technology by jihadists, but the exploitation of ICTs is not unique to these movements.[16] The far-right, for example, has a long legacy of using ICTs, especially in the U.S.[17] Regardless of ideology, technologies can improve the capabilities of terrorists and violent extremists by enhancing functions such as content production and dissemination, information gathering, fundraising, recruitment, and tactical planning.[18] Today, extremists in the U.S. and abroad use ICTs for a range of activities, and now integrate a more extensive array of tools including, but not limited to, social media, messengers, file-sharing sites, financial tools, web-archives, secure browsers, mobile security applications, virtual private networks (VPNs), and physical digital media, like thumb drives, hard drives, and smartphones.[19] In practice, much like non-extremist users, terrorists and violent extremists flow naturally across different platforms and tools rather than using one in isolation.[20] For

this reason, awareness of the mediums and methods that matter to these actors, and the ecosystem of communications they comprise, is critical to policymakers and practitioners tasked with preventing and countering these threats.

Narrowing the focus, terrorists and violent extremists in America are not uniform in their uses of ICTs.[21] Individuals seem to select technologies that allow them to pursue their objectives. For example, while a broad-based social media platform may lend itself to broadcasting propaganda, an encrypted messenger may be preferable for communications about attack planning.[22] Although more research is necessary, data from the National Consortium from the Study of Terrorism and Responses to Terrorism show that an increasing number of radicalized extremists in the U.S. leverage "user-to-user" platforms to virtually connect with communities and share information and ideas.[23] In spite of the uptick in this form of online engagement, researchers note that "user-to-user communications do not appear to increase the likelihood that extremists will be successful in traveling to foreign conflict zones or committing acts of domestic terrorism."[24] On the contrary, analysis of the PIRUS dataset finds that "the extremists who were most active on social media had lower success rates regarding foreign fighter travel and terrorist plots than individuals who were not as active on social media."[25] This is partly because extremists' presence on such public platforms offers more opportunities for detection and disruption by law enforcement.[26] With a better comprehension of the digital environment leveraged by terrorists and violent extremists, it is easier to assess the U.S. government's efforts to address these threats and discuss possibilities for a reconfigured approach.

Terrorists and violent extremists are proactive and agile in their exploitation of ICTs, but the government is conventionally bureaucratic, risk-averse, and slow to develop cohesive responses to these problems. While necessity and opportunism govern the behavior of extremists and their virtual networks, a range of different legal boundaries define the scope of the U.S. government's actions at home and abroad. These factors, along with national security strategies, policy agendas, and the ebb and flow of resources, determine what measures the government can feasibly implement to meet requirements and achieve objectives. Over the years, political leaders in the U.S. offered little strategic guidance on how to prevent and counter terrorist and violent extremist exploitation of ICTs domestically, by messaging or other means.[27] The absence of a plan founded on strategy, policies, and laws is both the cause and symptom of insufficient mandates and authorities for leadership on the issue. Even though domestic responses to terrorist and violent extremist use of technology and communications are modest compared to the country's efforts abroad,[28] it is difficult to describe the government's actions to address the problem in a cohesive way.[29]

At the federal level, several bodies attempt to intervene in matters concerning the nexus of technology and violent extremism.[30] A truncated list of entities involved in domestic efforts includes the Department of Homeland Security, the Department of Justice, the Federal Bureau of Investigation, the National Counter Terrorism Center, the National Security Council, and Congress. With a lack of direction and no requirements for progress, parts of the government dabbled with a range of methods including counter-messaging, awareness briefings, partnerships, and legislation.[31] Where some initiatives showed promise then failed to materialize as intended,[32] other measures may have complicated concurrent efforts to prevent and counter terrorism and violent extremism.[33]

Over the last few years, the Countering Violent Extremism Task Force, housed at the Department of Homeland Security, directed some attention towards technology-related matters in an interagency framework. Although the Task Force put the issues concerning the internet and social media on its agenda, the body did not serve as a full-fledged coordination effort. Among other measures, the Task Force convened the "Digital Forum[s] on Terrorism Prevention" with private companies, academic

institutions, and organizations including Tech Against Terrorism. These forums brought together an array of stakeholders and flagged some evidence-driven recommendations for policymakers and practitioners.[34] In February 2018, the Task Force also worked with partners including the U.K. Home Office to launch an online training course entitled "Countering Terrorists Exploitation of Social Media and the Internet."[35] Though such steps promoted issue-specific information both inside and outside of the government, the plans to continue addressing the matter through the Task Force are unclear. At least in part, the Task Force's struggle to advance efforts regarding terrorist and violent extremism exploitation of technology is attributable to wavering priorities within the government and subsequent discontinuity in resources to the Task Force.[36] Without strategies, policies, and laws that allow government institutions to sustainably fund and facilitate efforts towards select objectives, any entity attempting to advance matters concerning technology and terrorism in the U.S. will likely face the same challenges as the Task Force.

Since many factors limit the government's ability to intervene in threats posed by terrorist and violent extremist exploitation of ICTs in the U.S., engagement with civil society and private industry represents a vital part of the government's toolkit. Research shows that scholars and practitioners in the field regard online counter-messaging as an inherently problematic approach for the government to pursue domestically, given concerns about protected rights and freedoms as well as a lack of evidence about the effectiveness of such initiatives.[37] Even so, some political leaders saw select public-private partnerships "as success stories and a less risky way for the government to be involved in [counter-speech] efforts."[38] Ultimately, as public-private partnerships faced challenges, the government's emphasis on the role of social media providers increased.

Like other Western countries, the U.S. government envisions some role for technology providers in the fight against violent extremist groups. Political calls for tech companies to address terrorist propaganda have continued over the last ten years.[39] The Obama administration began prioritizing dialogue with the tech industry in late 2015 and early 2016 after a spate of attacks in Europe and the U.S. suggested that existing measures to counter violent extremists were insufficient.[40] The administration reportedly held high-level talks with Apple, Facebook, Twitter, and Google.[41] In 2016, an initiative called the 'Madison Valleywood Project' encouraged the tech and entertainment industries to assist in the fight against terrorism. The project promoted counter-speech and emphasized the enforcement of companies' terms of service.[42] Ultimately, the project did not remain a recognized component of the government's agenda, and political leaders have not articulated how the U.S. government will engage with service providers to empower companies against the exploitation of their platforms.

While political leaders in other Western countries tend to be more aggressive in their demands for major social media providers to expedite the removal of promotional content online,[43] "the removal of extremist content from circulation is not universally viewed as acceptable" within the counter-extremism community in the United States, "especially when the government is driving the process."[44] Without agreement on how the U.S. government should engage technology providers on the topic of terrorist and violent extremist exploitation of ICTs, different facets of the government created confusion and pursued competing approaches.[45] To mitigate this problem and enhance efficiency in the future, government interactions with technology providers require more strategic coordination and continuity.[46]

Without reviewing all of U.S. allies' efforts to curb extremist messaging online, from the Christchurch Call to legislation regulating technology providers, it is helpful to discuss which elements of those approaches are not suited for the threat picture in America. The U.S. government cannot always leverage counter-messaging and content-removal techniques domestically, but the opportunities and challenges of these methods may highlight important considerations for policymakers and practitioners.

First, in some European models, the political and tactical reliance on content-removal and account suspensions on a few major social media platforms is reactive and struggles prevent or counter many mechanisms and methods terrorists and extremists use to advance their aims.[47] For example, even when problematic sites, accounts, and materials are removed, they often resurface and continue to flow across various platforms.[48] Although content removal offers many benefits and should remain part of the toolkit to prevent and counter terrorism and violent extremism, this method is not sufficient in isolation.[49] Similarly, the involvement of major social media companies on this issue is necessary, but not the solution to the problem.

Next, the broader aim of *eliminating* terrorist and violent extremist content online is attractive to many Western countries,[50] but in the U.S., this is not a pragmatic, proportional, or tangible goal. Vague standards and broad definitions of terrorist content in several laws and legislative proposals have drawn criticism for inviting risks of censorship by over-removal.[51] The First Amendment protects speech that is offensive, disagreeable, or concerning, but does not protect all speech,[52] including fighting words, incitements to imminent violence, defamation, obscenity, and true threats.[53] Just as these legal thresholds present challenges in practice, discerning what constitutes terrorist and violent extremist content online, and whether it is legal or illegal, is difficult.[54] Promotional, instructional, or threatening materials may clearly violate a company's terms of service or break the law in some cases, but actions involving terrorism or violent extremism and ICTs regularly defy black and white categorization.[55] The parties that determine the acceptability of content grapple with a range of dynamics, including scenarios in which activists, scholars, and news media share propaganda, and instances in which terrorists and extremists disseminate materials that do not violate a company's terms of service or break the law.[56]

Although certain companies are not willing to execute government requests, or prefer meeting behind closed doors, many lack the resources to police their platforms to the degree that governments envision.[57] When public officials want to flag content for removal, they can use either legal orders or administrative referrals to instigate the process.[58] Some companies can and do evaluate the legitimacy of government requests to an extent, which is challenging for even the best-resourced companies, but those without the means to asses orders may ignore requests altogether or comply as much as possible to avoid further scrutiny from officials.[59] Research discussing the effects of intermediary liability laws on the behavior of companies finds that "when platforms face legal risks for user speech, they routinely err on the side of caution and take it down."[60] While unintended, such regulatory configurations may result in over-removal.[61]

In light of this consequence, it is crucial to remember that legal orders and referrals by governments are not always legitimate. In April 2019, for example, as the European Parliament prepared to vote on legislation requiring sites to take down materials reported as terrorist content within one hour, the "Internet Archive Blog" (connected to archive.org) posted an article about how the French Internet Referral Unit falsely identified and reported "hundreds of URLs on archive.org as 'terrorist propaganda'" in one week.[62] The blogpost raises some critical considerations, including:

> "how can the proposed legislation realistically be said to honor freedom of speech if these are the types of reports that are currently coming from EU law enforcement and designated governmental reporting entities? It is not possible for us to process these reports using human review within a very limited timeframe like one hour. Are we to simply take what's reported as "terrorism" at face value and risk the automatic removal of things like THE primary collection page for all books on archive.org?"

Concerns that technology providers are strategically and tactically slow to address terrorist and extremist abuse of their platforms are not wholly unfounded; however, political leaders in America need to move forward and attune themselves to the technicalities and tradeoffs involved in preventing the exploitation of ICTs at this scale.[63] If policymakers do not have a basic understanding of the mediums that matter to terrorists and violent extremists, and lack perspective on how the issue compares to other technology-related threats in the U.S., they cannot exercise leadership, create standards, and promote good governance. Realistically, terrorist and violent extremist activities represent just one of many issues that demand attention from the technology industry and government officials.[64] For example, if a small company has finite resources to address public policy concerns and illegal activity, it may prioritize taking down child pornography over propaganda. The government's approach to prevent and counter exploitation of ICTs must pragmatically and proportionally weigh the severity of concurrent threats in the virtual landscape.

Policymakers and political leaders in the U.S. vested with protecting speech while preventing and countering terrorist and violent extremist exploitation of ICTs should develop an evidence-based strategy and implementation plan. Domestically, the government's actions on this front are insufficient because they lack the direction and coordination necessary to confront these issues in the short-, medium-, and long-term. The current approach, left unchanged, could affect the lives of Americans in less obvious ways by undermining security and free speech in the U.S., as regulations abroad have global effects. By creating a framework to prevent and counter the abuse of ICTs without bearing some of the same costs associated with more stringent approaches to regulating content online, the U.S. government can complement the work of its allies and other signatories of the Christchurch Call.

Foundational Considerations

As discussed, a range of competing factors shape the U.S. government's responses to terrorist and violent extremist exploitation of ICTs in America, but ad-hoc efforts do not amount to a synergistic plan. Since short-term fixes are not a sufficient response to perpetual and evolving threats, political leaders need to push for a strategic approach, based around policy and law, to prevent and counter terrorists and violent extremists in the digital sphere. Policymakers interested in charting this alternative course can use the "marginalization strategy"[65] as a guideline for a more comprehensive approach to preventing and countering extremist exploitation of ICTs.[66] Rather than casting the issue as a problem to solve, the marginalization paradigm requires political leaders to recognize the tenacity and adaptability of terrorist and violent extremist networks. It also requires policymakers to develop responses to issues in the short-, medium-, and long-term.

The principles of pragmatism, proportionality, and respect for the rule of law should serve as defining pillars of the U.S. government's policy for preventing and countering terrorist and violent extremist exploitation of ICTs. These ideals help ensure that the government makes appropriate considerations to protect speech, civil liberties, and privacy in addressing terrorists and violent extremists online. Following such principles, the U.S. government can focus less on responding to terrorist and violent extremist abuse of ICTs, and more proactively and responsibly facilitate efforts to weaken the influence of the virtual networks and undercut the tools involved in the process of radicalization, recruitment, and mobilization. In pursuit of these aims, political leaders in America can explore a mix of legislation, redress, and outreach to better empower the range of public and private partners to prevent and counter terrorist and violent extremist exploitation of ICTs in the U.S.

Recommendations

The following section discusses opportunities and considerations for political leaders in the U.S. who want to develop a strategic approach to prevent and counter terrorist and extremist exploitation of ICTs in America. Although various government bodies could potentially implement the recommendations below, this brief calls for the White House to kickstart the process by creating a strategy. Pursuing these objectives while promoting and protecting certain rights and values requires political leaders to weigh tradeoffs and adhere to the principles of pragmatism, proportionality, and respect for the rule of law. The points articulated below demonstrate how the government can configure a domestic approach to prevent and counter terrorist and violent extremist abuse of ICTs.

A. Create an interagency working group to formalize leadership on domestic efforts, and task this body with planning and coordinating efforts to prevent and counter terrorist and violent extremist exploitation of ICTs in America

- Any task force, working group, or office charged with these efforts must receive the authority and resources necessary to action-plan, convene stakeholders, and instigate change. In 2013, the White House established the "Working Group to Counter Online Radicalization to Violence."[67] The group was meant to develop plans for an internet safety approach to address violent extremism online and intended to coordinate the federal government's efforts to counter online radicalization to violence, but the plans never fully materialized.[68] Later, the Countering Violent Extremism Task Force devoted some attention to specific matters concerning technology, but these efforts also lost traction due to a lack of resources.[69] Critics might argue that a new iteration of these bodies will likely meet the same fate, the political landscape concerning terrorist and extremist use of the internet is increasingly tenuous, and demands for action are growing.[70] The working group should include representatives from the National Security Council, the Department of Justice, the Department of Homeland Security, the National Counterterrorism Center, and the Federal Bureau of Investigation, along with rotating positions for subject-matter experts and members of civil society organizations. Ideally, the working group would also engage other national security entities within the State Department and Department of Defense, to streamline efforts when possible and exchange best practices.

B. Conduct a comprehensive assessment of terrorist and violent extremist exploitation of ICTs in America and identify short-, medium-, and long-term responses to the problem. Once completed, the working group should use this assessment to inform an implementation plan for the strategy.

- After a robust assessment of terrorist and violent extremist exploitation of ICTs in America, the interagency working group should survey viable courses of action. In addition to reviewing potential policies, laws, and regulatory approaches, the survey should examine public-private partnerships, and techniques such as issuing best practices, counter-messaging, strategic communications, and methods of content moderation. In doing so, the working group must consider the potential for harm and rationally weigh the opportunity cost of various interventions to determine the suitability of such measures given the scope of the problem. As the working group evaluates options for legislation, redress, and other measures, it must elevate pragmatic and proportional responses to terrorists and violent extremists online that uphold the values important to democratic societies.[71] This brief raises a few examples that deserve policymakers' consideration.[72]

    - *Discuss intermediary liability and Section 230 of the Communications Decency Act (47 U.S.C. § 230)* - Government officials, legislators, and judges must help ensure that policies and laws evolve with the information environment through either judicial interpretation or legislation. Section 230, for example, is an essential part of the discussion about how to empower technology

providers against terrorist exploitation of their platforms.[73] The statute offers "protection for 'good Samaritan' blocking and screening of offensive material," stating that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[74] In short, the 1996 measure creates legal safeguards for network providers by ensuring that, with a few exceptions, platforms cannot be sued for content posted by a user, even if the company moderates some materials.[75] Lawmakers intended to create a safe space for companies to enforce their platforms by leveraging incentives and protections rather than legal mandates. This was a relatively "pragmatic calculation" given that stringent intermediary liability laws can invite risks to free expression as well as hinder business and technological development.[76] Today, some scholars argue that the good intentions of Section 230 in censoring "'offensive' materials are inconsistent with outlandishly broad interpretations that have served to immunize" the most ill-behaved platforms from liability.[77] In other words, the statute affords blanket protections to service providers, including those that have not necessarily earned them in good faith. In "The Internet Will Not Break," Danielle Keats Citron and Benjamin Wittes argue that Section 230 needs revising, explaining, "If courts do not construe the scope of federal immunity to avoid injustice… Congress should amend the law."[78] Citron and Wittes suggest that free speech and public safety are not mutually exclusive aims, explaining, "with modest adjustments to §230, either through judicial interpretation or legislation, [the U.S.] can have a robust culture of free speech online without shielding" deliberately dubious platforms from liability.[79] As some scholars discuss ways to use Section 230 to confront issues posed by terrorist and violent extremist exploitation of ICTs,[80] critics of such recommendations raise concerns about the importance of protecting intermediaries and promoting free speech.[81] The Center for Democracy and Technology, for example, along with other advocacy groups and legal scholars, recently released a guide for legislators engaging with Section 230 to increase awareness about "how the statue works and why changing it would raise significant risks to free expression online."[82] Ultimately, since perspectives on the right course of action for Section 230 differ, the interagency working group should seize this opportunity to foster a robust discussion weighing the costs and benefits of intermediary liability and identify alternative means to prevent and counter exploitation of ICTs.

- *Assess the utility of issuing guidance and best practices for relevant stakeholders* – Since any legislative approach to prevent and counter terrorist and violent extremist exploitation of ICTs would take time to develop, the interagency working group should examine alternatives to prescriptive standards, such as issuing guidance and best practices for public and private partners.[83] For example, the working group might develop such materials for technology companies, ideally with input from subject-matter experts, advocacy groups, and private industry representatives. Instead of pursuing amendments to CDA § 230 to prevent and counter terrorist and violent extremist exploitation of ICTs, an approach that lawmakers used to confront sex trafficking online, the government could recommend practices for good Samaritan blocking and screening of terrorist and violent extremist content. Given the resilience of terrorists and violent extremist networks online, and the tradeoffs associated with existing measures to disrupt them, the interagency working group might issue recommendations that advance a more pragmatic approach to the problem. Beyond the tactics of removing content or suspending accounts, the working group could encourage companies to pursue other productive methods to prevent and counter terrorist and violent extremist abuse of their platforms such as crafting or clarifying terms of service; articulating and refining definitions of "hate speech" and "extremist material;" participating in inter- and cross-sector collaboration;[84] inviting independent third-party assessments;[85] considering various models for access (such as password-protected content, age restrictions for select materials, or temporarily limited functionality for users that continually

violate terms of service); promoting counter-speech; utilizing moderation mechanisms that complement take-downs; flagging bots and spam; formalizing legal channels and procedures for law enforcement; recording and reporting government requests; providing opportunities for repeal; engaging civil society groups; and publishing transparency reports that sufficiently detail companies' efforts. Ideally, recommendations by the working group could empower companies of diverse sizes and capabilities to take proportional steps to prevent and counter terrorist and violent extremist abuse of their platforms. Although some critics might argue that this approach creates no real incentives or requirements for stakeholders to change their behaviors, the rationale for issuing guidance and best practices extends beyond instigating action from technology providers. For instance, recommendations for the technology industry by the government help advance the agenda to prevent and counter terrorist and violent extremist exploitation of ICTs, and promote transparency, accountability, and collaboration.

- *Consider the revival of The Office of Technology Assessment (OTA)* – In 1972, the OTA was established to equip lawmakers with objective and up-to-date analyses on matters concerning technological development.[86] While the Office of Science and Technology Policy provided expertise to the executive branch,[87] the OTA offered similar functionalities to Congress.[88] The OTA investigated an array of topics, identified knowledge gaps, and evaluated the opportunities and risks associated with various courses of action.[89] In 1995, the office was closed, but the statute that led to the creation of the OTA remains in effect.[90] Critics of the OTA suggested that it was too slow to produce research products, but ultimately, the office was closed as part of a broader push to reduce spending in the legislative branch.[91] Today, the Congressional Research Service provides resources for lawmakers on a range of policy issues, including responses to terrorists' use of the internet.[92] Additionally, in early 2019, the Government Accountability Office launched a new Science, Technology Assessment and Analytics team, which focuses on providing Congress "technology assessments and technical services."[93] Despite the utility of these resources, some policymakers and experts argue that the need for robust, objective, and accessible research persists, and call for Congress to meet this demand by reviving the OTA or creating a similar body.[94] Given the range of challenges and opportunities technologies invite, particularly in the context of terrorism and violent extremism, additional support on matters concerning technology might help Congress might make more informed decisions.

- Motivated by a comprehensive risk assessment of the threats posed by terrorist and violent extremist exploitation of ICTs and aware of the most pragmatic courses of action, the interagency working group should develop a multi-pronged approach to achieve the strategic objectives. While looking for ways to measure and evaluate progress, the working group's implementation plan would focus on enhancing the capability and coordination of government-led efforts to prevent and counter the exploitation of ICTs in America; identifying and enabling civil society partners that can complement efforts to marginalize the effects of terrorism and extremism online; and empowering ICT providers to cope with the abuse of their platforms while protecting free expression, civil liberties, and privacy.

C. Enhance the capability and coordination of government-led efforts to prevent and counter terrorism and extremist exploitation of ICTs in America

- With sufficient authority and resourcing, the interagency working group could more effectively streamline the government's efforts to prevent and counter terrorist and violent extremist exploitation of ICTs by creating a legislative policy agenda and training sessions for Congress, as well as facilitating awareness briefings for other facets of government at the federal, state, and local level.

- Lawmakers and their staffers, for example, need better technical fluency on cybersecurity and information and communications technology to promote good governance and more proactively prevent the proliferation of terrorism and violent extremism online.[95] Today, many elected leaders are not attuned to contemporary challenges concerning online safety, but they should be, as such matters affect their constituents in countless ways.[96] Scholars note that this knowledge-gap becomes problematic when voters leave complex cyber and technology-related issues up to "'the small number of people who make important policy in the smoky backrooms,'" despite the reality that "most people in today's smoky backrooms have never been in an internet chatroom."[97] This dynamic is especially relevant in the context of technology and violent extremism. A working group, however, could equip decision-makers with up-to-date information about how terrorists and violent extremists use contemporary and emerging technologies, as well as how technological developments offer emerging capabilities to governments and private companies. Beyond the scope of social media, independent training sessions for policymakers should review topics ranging from cybersecurity to machine learning. Ideally, training programs would be transparent about the shortcomings and dangers of advanced methods of monitoring the digital communications of terrorists and violent extremists. For instance, there is an ominous and essential lesson to learn from cases where governments abuse crime-prevention and counter-terrorism technologies to target journalists, human rights defenders, anti-corruption advocates, lawyers, and opposition politicians.[98] Leaders who understand these nuances and the technical considerations facing the U.S. will be more effective at preventing terrorist exploitation of ICTs.

- The federal government should increase the number of permanent staff members with the technical proficiency to bridge the gap between service providers and government officials tasked with preventing and countering terrorism and violent extremism.[99]

- The working group should create cohesion among federal, state, and local law enforcement authorities tasked with preventing and countering terrorists and violent extremists' use of ICTs. In an administrative capacity, a technology-centric government initiative could work to foster forums in which federal, state, and local law enforcement reflect on their experiences and learn from other practitioners to stay up-to-date on overarching trends concerning the use of communications technologies by terrorists and violent extremists.

D. Pursue partnerships with and empower non-governmental entities that can complement government initiatives to prevent and counter terrorist and violent extremist exploitation of ICTs in pragmatic and proportional ways.

- The working group, along with other facets of the government, can use strategic communications, public outreach, and awareness briefings to empower non-governmental entities, particularly in civil society, to prevent and counter the influence of terrorists and violent extremists online. Educating partners about the government's aims and means of achieving objectives, as well as sharing some assessments of risk, will help set the agenda and enhance complementarity.

- Entities tasked with preventing exploitation of technologies must overtly engage with a range of actors to convey the government's approach, share up-to-date information concerning the intersection of technology and extremism, and encourage stakeholders to design and implement initiatives that complement the government's efforts.[100] A critical aspect of communicating the threat is articulating contemporary counterterrorism challenges in responsible ways that manage expectations and

promote transparency. In this vein, the working group could instruct public affairs officers on how to use strategic communications to foster resilience among communities and reduce the harmful effects of terrorist and violent extremist abuse of ICTs. From day-to-day operations to the period following an attack, federal agencies and local government and law enforcement can communicate directly with audiences concerning the threats posed by terrorism and violent extremism, both online and offline. Public affairs officers should continue exploring ways to leverage communications technologies to inform the public about its efforts and responses to evolving situations.[101] Increased communications can help educate the public, contextualize threats, manage expectations, rebuild trust, and reduce the impact terrorism and violent extremism have on communities.

- The working group can continue to ask federal agencies and U.S. Attorneys, as well as local government and law enforcement, to integrate matters concerning terrorist and violent extremist exploitation of ICTs in public meetings addressing internet safety.[102] Although assessments of these community-level engagements are limited, such "measures were viewed as promising for increasing resilience against extremist messaging without prompting" the kind of backlash experienced by more targeted efforts to discuss violent extremism within specific communities.[103] Reframing public engagements to focus on these issues as a subset of online safety may also raise awareness and convene relevant stakeholders including non-governmental organizations, civil society, and companies.

- Similarly, government officials can work to integrate additional information about terrorist and extremist exploitation of ICTs into public safety initiatives online. Instead of developing an entirely new infrastructure to spread awareness about the issue, policymakers should push to disseminate more information about terrorists' and violent extremists' use of technology through existing internet safety campaigns led by the federal government such as OnGuard Online, Stop.Think.Connect, and Safe Online Surfing.[104] In addition to being cost-effective and relatively easy to implement, this approach might also face less stigma if it becomes part of the broader effort to promote internet safety rather than an explicit attempt to prevent terrorism and violent extremism in the U.S.

E. Facilitate productive engagements with technology providers to more effectively prevent and counter terrorist and violent extremist exploitation of ICTs in pragmatic and proportional ways

- At the recommendation of the interagency working group, political leaders in America should emphasize a broader range of tactics to reduce the influence of violent extremists online and create a safer internet. In the U.S., the rate at which the leading social media companies delete extremist content from their platforms is not a useful measurement of the technology sector's commitment to the aim of preventing and countering terrorist and violent extremist abuse of ICTs. Instead, the government should configure a broader and more pragmatic understanding of the myriad ways technology providers can prevent and counter extremist exploitation. Some examples of potentially positive actions discussed earlier might include steps like clear terms of service regarding the promotion of terrorism, age restrictions on select material, formal channels for law enforcement, transparency reports about moderation tactics and government requests, and training for civil society groups. While some of the major technology providers already take such actions, more can be done to address the ecosystem of platforms leveraged by terrorists and violent extremist. By fostering a more dynamic approach, the working group can make it easier for companies of various shapes and sizes to help disrupt the exploitation of ICTs and create a safer internet while promoting transparency and accountability.

- Beyond the major social media platforms, political leaders should advance policies that enable other types of technology providers to prevent and counter the exploitation of their technologies. As discussed, terrorists and violent extremists use a range of platforms and techniques to connect with their movements. Consequently, the government must convene a diverse array of companies and help the industry develop new mechanisms to disrupt terrorists' and violent extremists' digital networks. For example, relevant stakeholders might include messaging applications, file-sharing platforms, web archives, link-shorteners, email-services, financial technologies, web hosting services, mobile security tools, and virtual private networks (VPN). Policymakers and practitioners can help marginalize the ecosystem of platforms exploited by terrorists and violent extremists by encouraging more companies to participate in efforts and making it easier for them to engage in the process.

- A respectful and productive relationship with the private sector is vital to the government's efforts to prevent and counter terrorist and violent extremist abuse of ICTs. For this reason, the working group should help educate policymakers about industry-led self-regulation[105] and support partnerships that help facilitate the process.[106] Tech Against Terrorism, for example, a U.N.-mandated project with funding from various countries and technology providers, helps companies develop useful terms of service and share information to prevent terrorists' exploitation of providers' tools.[107] In November 2017, Tech Against Terrorism launched "The Knowledge Sharing Platform," an online tool offering practical resources to companies that participate in the initiative.[108] While governments cannot relegate their responsibility in mitigating the effects of terrorism and violent extremism, political leaders should support the participation of companies in pragmatic and transparent initiatives. Moreover, despite fewer calls from political leaders to address non-jihadist violent extremists online, some industry-led efforts in America are taking steps to keep far-right extremists off their platforms.[109] Private companies have also supported some innovative and experimental interventions and counter-messaging projects by civil society groups and non-governmental organizations.[110]

- In addition to issuing best practices, the working group could provide stakeholders with strategically-oriented situational awareness briefings and resources. In June 2018, DHS announced the launch of a "Countering Terrorists Exploitation of Social Media and the Internet" training module.[111] The course was designed to educate companies about these threats with examples of official and unofficial propaganda products, supplementary notes on various topics, and quizzes to test knowledge.[112] It discussed the efforts of the Islamic State and al-Qaida, and also highlighted trends concerning extremists motivated by white supremacy.[113] The 90-minute course concluded with information about public-private partnerships and encouraged continued collaboration.[114] Although it is hard to gauge how many companies used this resource, Tech Against Terrorism made the resource available on its Knowledge Sharing Platform. Moving forward, the U.S. should continue to promote this training as a resource for technology providers, and the working group might explore new ways to keep materials like that course up-to-date and accessible to parties interested in preventing and countering the abuse of their platforms.

- Government entities can continue to convene private companies, particularly social media providers, advertising agencies, academics, practitioners, and civil society groups, to foster collaboration and the exchange of good practices. For example, this environment may help the technology industry with information about how to promote transparency and accountability about content moderation.[115]

- Facilitating such engagements may also encourage experts to tailor analyses and recommendations that speak to the challenges raised by technology providers.[116] Sessions can also help direct civil society groups toward the information, resources, and connections they need to implement digitally savvy intervention campaigns to prevent and counter terrorism and violent extremism, thus complementing government-led efforts.

Conclusion

On May 8, 2019, about a week before the U.S. abstained from signing onto Christchurch Call citing First Amendment concerns, the House Homeland Security Committee hosted a hearing on domestic terrorism with witnesses from the FBI, DOJ, and DHS. At the hearing, "each of the witnesses emphasized the government's limited power to address online content from Americans, even when it is extreme or hateful," at least in part, because of the First Amendment.[117] In light of the domestic constraints facing American policymakers and practitioners, the witnesses noted that companies adhering to different standards and community guidelines represented vital partners for the government.[118] Illustrating the benefits of such relationships, the FBI's assistant director for counterterrorism, Michael McGarrity, stated, "We are seeing a tide change in social media companies being more proactive... When they see something that is noteworthy and alarming beyond the First Amendment, they will give us leads."[119] Modest steps like increased rates of voluntary reporting to law enforcement by companies are commendable, but a strategic plan would allow the government and its partners to make greater strides in efforts to prevent and counter terrorist and violent extremist exploitation of ICTs.

Today, the U.S. government, like many of its allies, is reckoning with the complexity and endurance of the challenges posed by terrorist and violent extremist abuse of ICTs. Although policymakers and practitioners broadly recognize this problem, existing efforts to address the exploitation of ICTs by terrorists and violent extremists consist of cursory responses to long-term, dynamic threats. As U.S. allies draft and implement policies designed to tackle terrorist and violent extremist materials online, including signing onto agreements like the Christchurch Call, demands for the U.S. government to prevent and counter the abuse of ICTs persist. Since some of the measures advanced by other countries are not suitable or viable models for policymakers in the U.S., the government must devise a unique approach that rests on the pillars of pragmatism, proportionality, and respect for the rule of law.

This brief argues that the government should craft a comprehensive strategy to prevent and counter the exploitation of ICTs. Political leaders must identify tangible aims, such as mitigating, rather than eliminating, terrorist and violent extremist exploitation of ICTs. The proposed framework calls for officials to create an interagency working group to formalize leadership, assess trends regarding the abuse of ICTs, and weigh the costs and benefits associated with responses to these threats. Next, policymakers should take steps to enhance the capability and coordination of the government and its partners in civil society and private industry. In sum, political leaders in the U.S. should use legislation, redress, and strategic outreach to unite a range of actors against the exploitation of ICTs and confront the ecosystem of communications leveraged by terrorists and violent extremists.

References

[1]Romm, Tony, and Drew Harwell. 2019. "White House Declines to Back Christchurch Call to Stamp out Online Extremism amid Free Speech Concerns." *Washington Post*, May 15, 2019. https://www.washingtonpost.com/technology/2019/05/15/white-house-will-not-sign-christchurch-pact-stamp-out-online-extremism-amid-free-speech-concerns/?utm_term=.4c70f60e1be7; Roy, Eleanor Ainge. 2019. "Christchurch Call: Details Emerge of Ardern's Plan to Tackle Online Extremism." *The Guardian*, May 13, 2019. https://www.theguardian.com/world/2019/may/13/christchurch-call-details-emerge-of-arderns-plan-to-tackle-online-extremism; Koerner, Claudia. 2019. "The US Isn't Signing A Pledge To Fight Online Extremism After Christchurch." BuzzFeed News. https://www.buzzfeednews.com/article/claudiakoerner/christchurch-pledge-ardern-trump-usa-online-extremism.

[2]To read the original "Christchurch Call" document, visit: https://www.documentcloud.org/documents/6004545-Christchurch-Call.html

[3]"Supporters - Christchurch Call." 2019. Christchurch Call. 2019. https://www.christchurchcall.com/supporters.html.

[4]Romm, Tony, and Drew Harwell. 2019. "White House Declines to Back Christchurch Call to Stamp out Online Extremism amid Free Speech Concerns." *Washington Post*, May 15, 2019. https://www.washingtonpost.com/technology/2019/05/15/white-house-will-not-sign-christchurch-pact-stamp-out-online-extremism-amid-free-speech-concerns/?utm_term=.4c70f60e1be7; Koerner, Claudia. 2019. "The US Isn't Signing A Pledge To Fight Online Extremism After Christchurch." BuzzFeed News. https://www.buzzfeednews.com/article/claudiakoerner/christchurch-pledge-ardern-trump-usa-online-extremism.

[5] It is important to remember that the U.S. and some of its closest allies differ in views about speech. One journalist explains this dynamic, noting, "While the US is committed to free speech at all costs, the Europeans are more willing to curb speech when it expresses hate or causes harm." Ingram, Mathew. 2019. "White House Refuses to Join 'Christchurch Call' on Extremism." *Columbia Journalism Review*, May 16. https://www.cjr.org/the_media_today/white-house-christchurch-call.php; For more context, see also: Keller, Daphne. 2018. "Internet Platforms: Observations on Speech, Danger, and Money." National Security, Technology, and Law. Hoover Institution. https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money; Citron, Danielle Keats. 2017. "Policy Analysis: What to Do about the Emerging Threat of Censorship Creep on the Internet," CATO institute, November 28, 2017, https://www.cato.org/publications/policy-analysis/what-do-about-emerging-threat-censorship-creep-internet; "Douek, Evelyn. 2019. "Two Calls for Tech Regulation: The French Government Report and the Christchurch Call." Lawfare. May 18, 2019. https://www.lawfareblog.com/two-calls-tech-regulation-french-government-report-and-christchurch-call. For additional examples, see the following article, particularly the discussion of *Yahoo! V. La Ligue Contre Racism* - Levin, Brian. 2002. "Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America." *American Behavioral Scientist* 45 (6), 977-978, https://doi.org/10.1177/0002764202045006004.

[6] It is important to remember that the U.S. and some of its closest allies differ in views about speech. One journalist explains this dynamic, noting, "While the US is committed to free speech at all costs, the Europeans are more willing to curb speech when it expresses hate or causes harm." Ingram, Mathew. 2019. "White House Refuses to Join 'Christchurch Call' on Extremism." *Columbia Journalism Review*, May 16. https://www.cjr.org/the_media_today/white-house-christchurch-call.php; For more context, see also: Keller, Daphne. 2018. "Internet Platforms: Observations on Speech, Danger, and Money." National Security, Technology, and Law. Hoover Institution. https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money; Killion, Victoria. 2019. "Terrorism, Violent Extremism, and the Internet: Free Speech Considerations." Congressional Research Service. https://fas.org/sgp/crs/terror/R45713.pdf; Citron, Danielle Keats. 2017. "Policy Analysis: What to Do about the Emerging Threat of Censorship Creep on the Internet," CATO institute, November 28, 2017, https://www.cato.org/publications/policy-analysis/what-do-about-emerging-threat-censorship-creep-internet; "Douek, Evelyn. 2019. "Two Calls for Tech Regulation: The French Government Report and the Christchurch Call." Lawfare. May 18, 2019. https://www.lawfareblog.com/two-calls-tech-regulation-french-government-report-and-christchurch-call. For additional examples, see the following article, particularly the discussion of *Yahoo! V. La Ligue Contre Racism* - Levin, Brian. 2002. "Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America." *American Behavioral Scientist* 45 (6), 977-978, https://doi.org/10.1177/0002764202045006004.

[7]"National Strategy for Counterterrorism," 2011. The White House. https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf; "National Security Strategy." 2015. The White House. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf; "National Strategy for Counterterrorism of the United States of America." 2018. The White House. https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf; "National Security Strategy of the United States of America." 2017. The White House. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf;

[8]Braniff, William. 2017. "Recasting and Repositioning CVE as a Grand Strategic Response to Terrorism." National Consortium for the Study of Terrorism and Responses to Terrorism. November 14, 2017. http://www.start.umd.edu/news/recasting-and-repositioning-cve-grand-strategic-response-terrorism.

[9]Alexander, Audrey, and William Braniff. 2018. "Marginalizing Violent Extremism Online." Lawfare. January 21, 2018. https://www.lawfareblog.com/marginalizing-violent-extremism-online;

[10]Svantesson, Dan Jerker B. 2019. "Global Status Report 2019." Internet and Jurisdiction Policy Network. https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf; Fishman, Brian. 2019. "Crossroads: Counter-terrorism and the Internet*," National Security Law Review,* 2(2). https://tnsr.org/2019/04/crossroads-counter-terrorism-and-the-internet/; Guittard, Alexander and Ryan Greer. 2019. "Terror by any other name," *The Hill*, April 9, 2019. https://thehill.com/opinion/national-security/437978-terror-by-any-other-name; Blazakis, Jason. 2018. "American Terrorists: Why Current Laws Are Inadequate for Violent Extremists at Home." *Lawfare*. December 2, 2018. https://www.lawfareblog.com/american-terrorists-why-current-laws-are-inadequate-violent-extremists-home; Watkins, Ali, and Josh Meyer. 2017. "Domestic Hate Groups Elude Feds." POLITICO. August 15, 2017. https://www.politico.com/story/2017/08/15/us-hate-groups-legal-protections-241653

[11]This awareness briefing offers one example of how elusive terminology can arise in practical recommendations - "Awareness Brief: Online Radicalization to Violent Extremism." 2014. Community Oriented Policing Services, U.S. Department of Justice. https://ric-zai-inc.com/Publications/cops-w0739-pub.pdf. For more information about knowledge gaps and enduring questions concerning the intersections of ICTs and terrorism and violent extremism, see: Conway, Maura, 2017. "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research." *Studies in Conflict & Terrorism*, 40(1).

https://www.tandfonline.com/doi/full/10.1080/1057610X.2016.1157408; Benson, David. 2014. “Why the Internet is not increasing Terrorism,” *Security Studies,* 23(2), https://doi.org/10.1080/09636412.2014.905353. Meleagrou-Hitchens, Alexander, Audrey Alexander, Nick Kaderbhai. 2017. “Literature Review: The impact of digital communications technology on radicalization and recruitment,” *International Affairs*, 93(5), September 2017, https://doi.org/10.1093/ia/iix103;

[12]Von Behr, Ines, Anaïs Reding, Charlie Edwards, and Luke Gribbon. 2013. “Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism.” RAND Europe.
https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf; Alava, Seraphin, Divina Frau-Meigs, and Ghayda Hassan. 2017. “Youth and Violent Extremism on Social Media: Mapping the Research.” UNESCO.
https://unesdoc.unesco.org/ark:/48223/pf0000260382; Gill, Paul, Emily Corner, Amy Thornton, and Maura Conway. 2015 “What Are the Roles of the Internet in Terrorism?: Measuring the Online Behaviors of Convicted UK Terrorists.” VoxPol. http://voxpol.eu/wp-content/uploads/2015/11/DCUJ3518_VOX_Lone_Actors_report_02.11.15_WEB.pdf; Conway, Maura, 2017. "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research." *Studies in Conflict & Terrorism*, 40(1).
https://www.tandfonline.com/doi/full/10.1080/1057610X.2016.1157408; Koehler, Daniel. 2014. “The Radical Online: Individual Radicalization Processes and the Role of the Internet.” *Journal for Deradicalization* 2014/15 (1). http://journals.sfu.ca/jd/index.php/jd/article/viewFile/8/8; Meleagrou-Hitchens, Alexander, Audrey Alexander, Nick Kaderbhai. 2017. “Literature Review: The impact of digital communications technology on radicalization and recruitment,” *International Affairs*, 93(5), September 2017, https://doi.org/10.1093/ia/iix103;

[13]Jensen, Michael, and Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, Elizabeth Yates. 2018. "The Use of Social Media by United States Extremists." START, College Park,
Maryland. https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf; Conway, Maura, 2017. "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research." *Studies in Conflict & Terrorism*, 40(1). https://www.tandfonline.com/doi/full/10.1080/1057610X.2016.1157408.

[14] There are divergent perspectives regarding whether or not the internet expedites the process of radicalization. Whereas one study of select cases in the U.K. explains that “evidence does not necessarily support the suggestion that the internet accelerates radicalization,” a study of cases in the U.S. finds evidence suggesting “that [social media] has contributed to the acceleration of radicalization of U.S. extremists.” Von Behr, Ines, Anaïs Reding, Charlie Edwards, and Luke Gribbon. 2013. “Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism.” RAND Europe. https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf; Jensen, Michael, and Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, Elizabeth Yates. 2018. "The Use of Social Media by United States Extremists." START, College Park,
Maryland. https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf. Differences like this often arise in academic literature on the subject, and demonstrate why it is important to educate policymakers and practitioners about such nuances.

[15]Weimann, Gabriel. 2004. “Www.Terror.Net: How Modern Terrorism Uses the Internet.” Special Report. United States Institute for Peace. https://www.usip.org/sites/default/files/sr116.pdf; - Levin, Brian. 2002. “Cyberhate: A Legal and Historical Analysis of Extremists’ Use of Computer Networks in America.” *American Behavioral Scientist* 45(6), 977-978, https://doi.org/10.1177/0002764202045006004.

[16]For example, one paper notes “domestic terrorists – much like their violent jihadist analogues – are often internet savvy and use the medium as a resource for their operations,” Bjelopera, Jerome. 2017. “Domestic Terrorism: An Overview,” Congressional Research Service. https://fas.org/sgp/crs/terror/R44921.pdf; See also, Levin, Brian. 2002. “Cyberhate: A Legal and Historical Analysis of Extremists’ Use of Computer Networks in America.” *American Behavioral Scientist* 45(6). https://doi.org/10.1177/0002764202045006004;

[17]For example, scholars note that as early as 1983, neo-Nazis in the U.S. first realized the potential of the web, see: Michael, George. 2013, "The new media and the rise of exhortatory terrorism," *Strategic Studies Quarterly*, 40 (4),
https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-07_Issue-1/Michael.pdf; Schafer, Joseph, 2002, “Spinning the Web of Hate: Web-Based Hate Propaganda by Extremist Organizations,” *Journal of Criminal Justice and Popular Culture*, 9(2),
https://www.albany.edu/scj/jcjpc/vol9is2/schafer.html; *Poisoning the web: hatred online*, Anti-Defamation League, 1999; Meleagrou-Hitchens, Alexander, Audrey Alexander, Nick Kaderbhai. 2017. “Literature Review: The impact of digital communications technology on radicalization and recruitment,” *International Affairs*, 93(5), September 2017, https://doi.org/10.1093/ia/iix103

[18]Weimann, Gabriel. 2004. “Www.Terror.Net: How Modern Terrorism Uses the Internet.” Special Report. United States Institute for Peace. https://www.usip.org/sites/default/files/sr116.pdf.

[19]Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. 2017. “Terrorist Use of the Internet by the Numbers Quantifying Behaviors, Patterns, and Processes.” *Criminology and Public Policy* 16(1). https://onlinelibrary.wiley.com/doi/pdf/10.1111/1745-9133.12249; Jones, Seth. 2018. “The Rise of Far-Right Extremism in the United States.” *Center for Strategic and International Studies* (blog). November 7, 2018. https://www.csis.org/analysis/rise-far-right-extremism-united-states; Amble, John Curtis. 2012. “Combating Terrorism in the New Media Environment.” Studies in Conflict and Terrorism 35 (5): 339; Zelin, Aaron, 2003, *The State of Global Jihad Online,* New America Foundation, https://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20130201-NewAmericaFoundation.pdf; Alkhouri, Laith, and Alex Kassirer. 2016. “Tech for Jihad: Dissecting Jihadists’ Digital Toolbox.” Flashpoint. https:// www.flashpoint-intel.com/wp-content/uploads/2016/08/ TechForJihad.pdf. Binder, Laurence, and Raphael Gluck. 2017. “Wilayat Internet: ISIS’ Resilience across the Internet and Social Media.” *Bellingcat* (blog). September 1, 2017. https://www.bellingcat.com/news/mena/2017/09/01/wilayat-internet-isis-resilience-across-internet-social-media/; Fishman, Brian. 2019. “Crossroads: Counter-terrorism and the Internet*,” National Security Law Review,* 2(2). https://tnsr.org/2019/04/crossroads-counter-terrorism-and-the-internet/; Brantly, Aaron. 2017. “Innovation and Adaptation in Jihadist Digital Security.” *Survival* 59 (1). http://dx.doi.org/10.1080/00396338.2017.1282678; Clifford, Bennett. 2018. “‘Trucks, Knives, Bombs, Whatever:’ Exploring Pro-Islamic State Instructional Material on Telegram.” *CTC Sentinel* 11(5). https://ctc.usma.edu/trucks-knives-bombs-whatever-exploring-pro-islamic-state-instructional-material-telegram1; “ISIS use of smaller platforms and the D-Web to share Terrorist Content,” Tech Against Terrorism (blog), April 29, 2019, https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/

[20]To better comprehend the dynamic nature of extremist communications, it is helpful to consider day-to day uses of ICTs among non-extremist users. On a smartphone alone, one professional person might have their work email and a private email address, along with multiple social media applications that serve different purposes. The individual might communicate with friends and family over text message but discuss work-related and sensitive matters on a messenger with encryption features. Depending on the nature of their work, or personal interests, the person might

download additional applications that allow them to share and edit files, produce videos, or translate a language. By flowing across different platforms, and engaging with various networks and tools, individuals become part of a complex ecosystem of communications. Terrorist and violent extremists do the same thing. To offer an example, a violent extremist might use a messenger with encryption features on their phone to send a like-minded sympathizer a link to a file-sharing site with instructions about how to create multiple social media accounts to disseminate propaganda. The sympathizer could access the same messaging app on their computer using a web-platform, then click the link, save the contents from the file-sharing site, and upload the instructions about how to create multiple social media accounts along with other instructional materials.

[21]At the tactical level, one might consider the various ways in which like-minded Islamic State sympathizers with links to the U.S. leveraged technology. Here are some preliminary examples**:** **Keonna Thomas** used Twitter and Skype to build and maintain relationships with people in jihadist-controlled territory and she also read digital guidebooks as part of her research on travel routes to Turkey, where she could cross the border into Syria. "Criminal Complaint and Affidavit." 2015, *USA v. Keonna Thomas,* U.S. District Court for the Eastern District of Pennsylvania; **Terrence McNeil** expressed his support for ISIS on several social media platforms, including Twitter, Facebook, and Tumblr, and he solicited violence by reblogging a file with leaked addresses of personnel in the U.S. military, "Affidavit." 2016. *USA v. Terrence Joseph McNeil*, U.S. District Court for the Northern District of Ohio; **Eric Jamal Hendricks** aspired to create and Islamic State-cell in America and used at least four social media applications, three of which offered encryption features, the file sharing site justpaste.it, and an anonymizing software application, "Affidavit." 2016. *USA v. Erick Jamal Hendricks,* U.S. District Court for the Northern District of Ohio; In preparation for traveling to Islamic State-controlled territory, **Mohamad Khweis** used email accounts, Facebook, Twitter, Kik, Surespot, Telegram, VPN Master, VPN Defender, VPN InTouch, and Tor browser, "Trial Transcript." 2017. *USA v. Mohamad Jamal Khweis*, United States District Court for the Eastern District of Virginia; After defrauding several financial institutions and garnering illicit funds, **Zoobia Shahnaz** purchased over $60,000 in Bitcoin and other cryptocurrencies, then siphoned the funds through a bank account and various wider transfers to avoid detection by law enforcement, Letter to Judge Tomlinson." 2017. *USA v. Zoobia Shahnaz*, U.S. District Court in the Eastern District of New York; To learn more about broader trends concerning terrorist and violent extremist exploitation of ICTs in the U.S., see: Jensen, Michael, and Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, Elizabeth Yates. 2018. "The Use of Social Media by United States Extremists." START, College Park, Maryland. https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf.

[22]Brantly, Aaron. 2017. "Innovation and Adaptation in Jihadist Digital Security." *Survival* 59 (1), https://www.tandfonline.com/doi/abs/10.1080/00396338.2017.1282678; Jensen, Michael, and Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, Elizabeth Yates. 2018. "The Use of Social Media by United States Extremists." START, College Park, Maryland. https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf

[23] Please note that this PIRUS dataset defines social media as "any form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content, such as videos and images. This form of online communication is distinct from other types of internet usage in that it emphasizes online user-to-user communication rather than passively viewing content hosted by an online domain. Additionally, [the PIRUS dataset's] definition of social media does not include file-sharing sites (e.g., Torrent networks, Dropbox, P2P networks, etc.)" Jensen, Michael, and Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, Elizabeth Yates. 2018. "The Use of Social Media by United States Extremists." START, College Park, Maryland. https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf

[24]Ibid.

[25]Ibid.

[26] Muller, John and Mark Steward. 2015. "Terrorism, counterterrorism, and the Internet: The American Cases," Dynamics of Asymmetric Conflict, 8(2), https://doi.org/10.1080/17467586.2015.1065077; Jensen, Michael, and Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, Elizabeth Yates. 2018. "The Use of Social Media by United States Extremists." START, College Park, Maryland. https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf

[27]"National Strategy for Counterterrorism," 2011. The White House. https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf; "National Security Strategy." 2015. The White House. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf; "National Strategy for Counterterrorism of the United States of America." 2018. The White House. https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf; "National Security Strategy of the United States of America." 2017. The White House. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf;

[28]For additional materials about the U.S. government's efforts to address the intersections of terrorism, violent extremism, and information and communication technology in the U.S. and abroad, see: Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html; Watts, Clint. 2018. *Messing with the Enemy*. P.191; For efforts concerning social media providers, see: Harris, Gardiner, and Cecilia Kang. 2017. "Obama Shifts Online Strategy on ISIS." *The New York Times*, December 21, 2017. https://www.nytimes.com/2016/01/09/world/middleeast/white-house-officials-to-meet-with-tech-leaders-on-thwarting-terrorists.html; For a look at steps by the Department of Homeland Security, see: "Executive Summary: Digital Forum on Terrorism Prevention." 2017. Department of Homeland Security. December 1, 2017. https://www.dhs.gov/publication/executive-summary-digital-forum-terrorism-prevention; "DHS Announces the Launch of the 'Countering Terrorists Exploitation of Social Media and the Internet' Training." 2018. Department of Homeland Security. June 11, 2018. https://www.dhs.gov/blog/2018/06/11/dhs-announces-launch-countering-terrorists-exploitation-social-media-and-internet. For commentary on measures by the Department of Defense see: Nakashima, Ellen, and Missy Ryan. 2016. "U.S. Military Has Launched a New Digital War against the Islamic State," July 15, 2016. https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?utm_term=.923919b14ce5; Martelle, Michael. 2018. "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL." National Security Archive: Cyber Vault. (blog). August 13, 2018. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil; Department of Defense Press Release. 2017. "Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges." https://dod.defense.gov/News/Article/Article/1356172/project-maven-industry-day-pursues-artificial-intelligence-for-dod-challenges/. For reference on measures by the State Department, see: "Panel Casts Doubt on U.S. Propaganda Efforts against ISIS." *Washington Post*, December 2, 2015. https://www.washingtonpost.com/world/national-security/panel-casts-doubt-on-us-propaganda-efforts-against-isis/2015/12/02/ab7f9a14-9851-11e5-94f0-9eeaff906ef3_story.html?utm_term=.021256fdeb04; Levitt, Matthew. 2016. "A Counterterrorism

Restructuring That Can't Work Without Funding." *Washington Institute*. January 16, 2016. https://www.washingtoninstitute.org/policy-analysis/view/a-counterterrorism-restructuring-that-cant-work-without-funding; "The Global Engagement Center's Technology Demonstration Series." U.S. Department of State. 2018. https://www.state.gov/r/gec/tech/index.htm.

[29]Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html

[30]Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html; Hughes, Seamus. 2018. "Whose Responsibility is it to Confront Terrorism Online?" *Lawfare Blog.* April 27, 2018.https://www.lawfareblog.com/whose-responsibility-it-confront-terrorism-online; Wiktorowicz, Quintan. 2013. "Working to Counter Online Radicalization to Violence in the United States." Whitehouse.Gov. February 5, 2013. https://obamawhitehouse.archives.gov/blog/2013/02/05/working-counter-online-radicalization-violence-united-states; "Remarks by Assistant Attorney General John Carlin Opening of Madison Valleywood Project." 2016. Department of Justice. https://epic.org/foia/MadisonValleywood_2.pdf; Haughom, Jaclyn. 2016. "Combating Terrorism in the Digital Age: First Amendment Implications," Freedom Forum Institute, https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/combatting-terrorism-in-a-digital-age-first-amendment-implications/.

[31]Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html; "Don't Be a Puppet." Federal Bureau of Investigation. https://www.fbi.gov/cve508; "DHS Announces the Launch of the 'Countering Terrorists Exploitation of Social Media and the Internet' Training." 2018. Department of Homeland Security. June 11, 2018. https://www.dhs.gov/blog/2018/06/11/dhs-announces-launch-countering-terrorists-exploitation-social-media-and-internet; "Legislative Proposals on Terrorist Use of Social Media Raise Policy and Legal Questions." 2015. Council on Foreign Relations. July 16, 2015. https://www.cfr.org/blog/legislative-proposals-terrorist-use-social-media-raise-policy-and-legal-questions; "How DHS Partnerships Help Counter Violent Extremism." 2016. Study in the States. https://studyinthestates.dhs.gov/2016/07/how-dhs-partnerships-help-counter-violent-extremism.

[32]Wiktorowicz, Quintan. 2013. "Working to Counter Online Radicalization to Violence in the United States." Whitehouse.Gov. February 5, 2013. https://obamawhitehouse.archives.gov/blog/2013/02/05/working-counter-online-radicalization-violence-united-states; "Remarks by Assistant Attorney General John Carlin Opening of Madison Valleywood Project." 2016. Department of Justice. https://epic.org/foia/MadisonValleywood_2.pdf.

[33]See Chapter 10 of Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html;

[34]"Executive Summary: Digital Forum on Terrorism Prevention." 2017. Department of Homeland Security. December 1, 2017. https://www.dhs.gov/publication/executive-summary-digital-forum-terrorism-prevention.

[35]"DHS Announces the Launch of the 'Countering Terrorists Exploitation of Social Media and the Internet' Training." 2018. Department of Homeland Security. June 11, 2018. https://www.dhs.gov/blog/2018/06/11/dhs-announces-launch-countering-terrorists-exploitation-social-media-and-internet.

[36]While funding for this interagency CVE Task Force remains unclear, similarly-oriented entities like the Department of Homeland Security's Office of Community Partnerships have been rebranded and defunded by the current administration. See: Greer, Ryan, and George Selim. 2018. "Reframing Prevention: If Government Won't Lead, Civil Society Must Step Up to Curb Extremism." *Just Security* (blog). December 10, 2018. https://www.justsecurity.org/61755/reframing-prevention-government-lead-civil-society-step-curb-extremism/. See also, Beinart, Peter. 2018. "Trump Shut Programs to Counter Violent Extremism." *The Atlantic*, October 29, 2018. https://www.theatlantic.com/ideas/archive/2018/10/trump-shut-countering-violent-extremism-program/574237/.

[37]For more information about online counter-messaging as it pertains to the government, the private-sector, and non-governmental organizations, see: Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html

[38]To offer an example, the Peer2Peer (P2P) program was a public-private partnership between EdVenture Partners and DHS that ran until 2016, when its federal funding for domestic efforts ended. Supporters of the initiative credit P2P for educating students about, and mobilizing young people against, violent extremism, but critics of the program question the efficacy of the counter-messaging campaigns created by students. Today, the State Department works with EdVenture Partners and Facebook to facilitate the P2P program abroad. For more information about the P2P program, and other online counter-messaging efforts as they pertain to the government, private-sector, and non-governmental organizations, see: Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html

[39] Hughes, Seamus. 2018. "Whose Responsibility is it to Confront Terrorism Online?" *Lawfare Blog.* April 27, 2018. https://www.lawfareblog.com/whose-responsibility-it-confront-terrorism-online

[40]Ibid.

[41]Ibid.

[42]Kang, Cecilia, and Matt Apuzzo. 2016. "U.S. Asks Tech and Entertainment Industries Help in Fighting Terrorism." The New York Times, February 24, 2016. https://www.nytimes.com/2016/02/25/technology/tech-and-media-firms-called-to-white-house-for-terrorism-meeting.html

[43]*BBC News*. 2018. "Social Media Faces EU Fine If Terror Lingers for an Hour," August 20, 2018. https://www.bbc.com/news/technology-45247169; Leading officials in the U.K. regularly call for technology providers to expedite their efforts to remove extremist content. Stewart, Heather. 2017. "May Calls on Internet Firms to Remove Extremist Content within Two Hours." *The Guardian*, September 19, 2017. http://www.theguardian.com/uk-news/2017/sep/19/theresa-may-will-tell-internet-firms-to-tackle-extremist-content. In a similar vein, the European Commission recently started taking steps to threaten similar penalties against platforms that fail to delete terrorist propaganda from their sites within an hour. *BBC News*. 2018. "Social Media Faces EU Fine If Terror Lingers for an Hour," August 20, 2018.

https://www.bbc.com/news/technology-4524716; Lomas, Natasha. 2017. "Germany's Social Media Hate Speech Law Is Now in Effect." *TechCrunch*, October 2, 2017. http://social.techcrunch.com/2017/10/02/germanys-social-media-hate-speech-law-is-now-in-effect/; Bennett, Owen. 2018. "The EU Terrorist Content Regulation – a Threat to the Ecosystem and Our Users' Rights." Open Policy & Advocacy. https://blog.mozilla.org/netpolicy/2018/11/21/the-eu-terrorist-content-regulation-a-threat-to-the-ecosystem-and-our-users-rights; Satariano, Adam. 2019. "Europe Is Reining In Tech Giants. But Some Say It's Going Too Far." The New York Times, May 6, 2019, https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html; For more articles, visit the following archive: "Censorship Archives." VOX - Pol (blog) https://www.voxpol.eu/tag/censorship/.

[44]Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html

[45]For more information on this dynamic, see: Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html; For further consideration, consider the perspectives of technology providers who were approached by different government agencies with unique requests and styles of engagement (carrot vs. stick dynamic). To complicate matters more, even as the White House worked to *encourage* companies to moderate their own platforms, lawmakers proposed legislation like the "Combat Terrorist Use of Social Media Act of 2015" to *require* social media providers to alert federal authorities about terrorist activities - https://www.feinstein.senate.gov/public/_cache/files/9/b/9bdfe0ca-fb12-4beb-b64d-dc9239d93070/888F738137108ACED16ECC8AAC9D026D.social-media-reporting-bill.pdf; On several occasions, congressional committees called a few of the major social media companies to testify on Capitol Hill about what they were doing to address terrorist and violent extremist content on their sites, see: Breland, Ali. 2018. "Facebook, Twitter and YouTube to Testify on Capitol Hill about Terrorism and Social Media." The Hill. January 9, 2018. https://thehill.com/policy/technology/368184-facebook-twitter-and-google-to-testify-on-capitol-hill-about-terrorism-and

[46]Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html

[47]Holt, Thomas, Joshua Freilich, and Steven Chermak. 2017. "Can Taking Down Websites Really Stop Terrorists and Hate Groups?" *VOX - Pol* (blog). November 29, 2017. https://www.voxpol.eu/can-taking-websites-really-stop-terrorists-hate-groups/; Lomas, Natasha. 2017. "Germany's Social Media Hate Speech Law Is Now in Effect." *TechCrunch*, October 2, 2017. http://social.techcrunch.com/2017/10/02/germanys-social-media-hate-speech-law-is-now-in-effect/; Alexander, Audrey, and William Braniff. "Marginalizing Violent Extremism Online." *Lawfare*, January 21, 2018. https://www.lawfareblog.com/marginalizing-violent-extremism-online.

[48]This article examines the outcome of a Europol operation against IS coordinated and conducted between six European countries, as well as Canada and the United States. Binder, Laurence, and Raphael Gluck. 2018. "Assessing Europol's Operation Against ISIS' Propaganda: Approach and Impact." *International Centre for Counter-Terrorism*. June 18, 2018. https://icct.nl/publication/assessing-europols-operation-against-isis-propaganda-approach-and-impact/; CBS News. 2018. "ISIS' Media Mouthpiece Amaq Was Silenced, but Not for Long," May 12, 2018. https://www.cbsnews.com/news/isis-amaq-online-propaganda-hit-cyber-takedown-bounces-back-in-just-days/; Binder, Laurence, and Raphael Gluck. 2017. "Wilayat Internet: ISIS' Resilience across the Internet and Social Media." *Bellingcat* (blog). September 1, 2017. https://www.bellingcat.com/news/mena/2017/09/01/wilayat-internet-isis-resilience-across-internet-social-media/; Martineau, Paris. 2018. "How Right-Wing Social Media Site Gab Got Back Online." *Wired,* November 6, 2018. https://www.wired.com/story/how-right-wing-social-media-site-gab-got-back-online/; Schulberg, Jessica, Dana Liebelson, and Tommy Craggs. 2017. "The Neo-Nazis Are Back Online." Huffington Post, October 3, 2017. https://www.huffpost.com/entry/nazis-are-back-online_n_59d40719e4b06226e3f46941.

[49]Alexander, Audrey, and William Braniff. 2018. "Marginalizing Violent Extremism Online." Lawfare. January 21, 2018. https://www.lawfareblog.com/marginalizing-violent-extremism-online;

[50]While non-binding and voluntary, the subtitle of the Christchurch Call states its aims "to *eliminate* terrorist and violent extremist content online." To read the original "Christchurch Call" document, visit: https://www.documentcloud.org/documents/6004545-Christchurch-Call.html

[51]Keller, Daphne. 2018. "Internet Platforms: Observations on Speech, Danger, and Money." National Security, Technology, and Law. Hoover Institution. https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money; Bennett, Owen. 2018. "The EU Terrorist Content Regulation – a Threat to the Ecosystem and Our Users' Rights." Open Policy & Advocacy. https://blog.mozilla.org/netpolicy/2018/11/21/the-eu-terrorist-content-regulation-a-threat-to-the-ecosystem-and-our-users-rights; Satariano, Adam. 2019. "Europe Is Reining In Tech Giants. But Some Say It's Going Too Far." The New York Times, May 6, 2019. https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html; Citron, Danielle Keats. 2017. "Policy Analysis: What to Do about the Emerging Threat of Censorship Creep on the Internet," CATO institute, November 28, 2017, https://www.cato.org/publications/policy-analysis/what-do-about-emerging-threat-censorship-creep-internet; "Germany: Flawed Social Media Law." 2018. Human Rights Watch. February 14, 2018. https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law; Cave, Damien. 2019. "Australia Passes Law to Punish Social Media Companies for Violent Posts." *The New York Times*, April 4, 2019, https://www.nytimes.com/2019/04/03/world/australia/social-media-law.html.; "Freedom of the Net 2018: France." Freedom House. November 1, 2018. https://freedomhouse.org/report/freedom-net/2018/france.

[52]Ruane, Kathleen Ann. 2016. "The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes." Congressional Research Service, https://fas.org/sgp/crs/terror/R44626.pdf; Haughom, Jaclyn. 2016. "Combating Terrorism in the Digital Age: First Amendment Implications," Freedom Forum Institute, https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/combatting-terrorism-in-a-digital-age-first-amendment-implications/; "Which Types of Speech Are Not Protected by the First Amendment?" Freedom Forum Institute (blog). https://www.freedomforuminstitute.org/about/faq/which-types-of-speech-are-not-protected-by-the-first-amendment/; For more information about the First Amendment, particularly in the context of propaganda and incitement, see: Raban, Ofer. 2018. "Observation on the First Amendment and the War on Terror," *Tulsa Law Review*, 53:2, https://law.uoregon.edu/images/uploads/entries/2018_Observations_on_the_First_Amendment_and_the_War_on_Terror_Tulsa_Law_Review.pdf.

[53]Ruane, Kathleen Ann. 2016. "The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes." Congressional Research Service, https://fas.org/sgp/crs/terror/R44626.pdf; Haughom, Jaclyn. 2016. "Combating Terrorism in the Digital Age:

First Amendment Implications," Freedom Forum Institute, https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/combatting-terrorism-in-a-digital-age-first-amendment-implications/; "Which Types of Speech Are Not Protected by the First Amendment?" Freedom Forum Institute (blog). https://www.freedomforuminstitute.org/about/faq/which-types-of-speech-are-not-protected-by-the-first-amendment/.

[54]In *Custodians of the Internet,* Tarleton Gillespie stated that content moderation is difficult "because it is resource intensive and relentless; because it requires making difficult and often untenable distinctions; because it is wholly unclear what the standards should be; and because one failure can incur enough public outrage to overshadow a million quiet successes," as quoted in Kaye, David. 2019. *Speech Police: The Global Struggle to Govern the Internet.* Columbia Global Reports; Killion, Victoria. 2019. "Terrorism, Violent Extremism, and the Internet: Free Speech Considerations." Congressional Research Service. https://fas.org/sgp/crs/terror/R45713.pdf.

[55]Alexander, Audrey and Helen Christy Powell. 2018. "Gray Media Under the Black and White Banner," *Lawfare Blog.* https://www.lawfareblog.com/gray-media-under-black-and-white-banner

[56]Ibid.

[57]"Technology Against Terrorism: How to Respond to the Exploitation of the Internet." 2017. Chatham House Panel Event. July 12, 2017. https://www.chathamhouse.org//node/30156; "More Support Needed for Smaller Technology Platforms to Counter Terrorist Content." 2018. Trends Alert. UN CTED. https://gallery.mailchimp.com/8343c3b932a7be398ceb413c9/files/ffbb7fe9-5a06-4390-8861-50e488ecad69/CTED_Trends_Alert_November_2018.pdf; Keller, Daphne. 2018. "Internet Platforms: Observations on Speech, Danger, and Money." National Security, Technology, and Law. Hoover Institution. https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money;

[58]To learn more about strategic and tactical approaches companies might take to manage content removal orders by governments, see: Fishman, Brian. 2019. "Crossroads: Counter-terrorism and the Internet*," National Security Law Review,* 2(2). https://tnsr.org/2019/04/crossroads-counter-terrorism-and-the-internet/; See also, Keller, Daphne. 2018. "Internet Platforms: Observations on Speech, Danger, and Money." National Security, Technology, and Law. Hoover Institution. https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money;

[59]"Technology Against Terrorism: How to Respond to the Exploitation of the Internet." 2017. Chatham House Panel Event. July 12, 2017. https://www.chathamhouse.org//node/30156; "More Support Needed for Smaller Technology Platforms to Counter Terrorist Content." 2018. Trends Alert. UN CTED. https://gallery.mailchimp.com/8343c3b932a7be398ceb413c9/files/ffbb7fe9-5a06-4390-8861-50e488ecad69/CTED_Trends_Alert_November_2018.pdf.

[60]For a more comprehensive discussion about intermediary liability, see: Keller, Daphne. 2018. "Internet Platforms: Observations on Speech, Danger, and Money." National Security, Technology, and Law. Hoover Institution. https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money;

[61]Keller, Daphne. 2015. "Empirical Evidence of 'Over-Removal' by Internet Companies under Intermediary Liability Laws." The Center for Internet and Society at Stanford Law School (blog). October 12, 2015. http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws; Woodruff, Betsy. 2017. "Exclusive: Facebook Silences Rohingya Reports of Ethnic Cleansing," Daily Beast. September 18, 2017. https://www.thedailybeast.com/exclusive-rohingya-activists-say-facebook-silences-them; Warner, Bernhard. 2019. "Tech Companies Are Deleting Evidence of War Crimes." *Defense One.* May 8, 2019. https://www.defenseone.com/ideas/2019/05/tech-companies-are-deleting-evidence-war-crimes/156845/; "Gatekeepers or Censors? How Tech Manages Online Speech." The New York Times, August 7, 2018. https://www.nytimes.com/2018/08/07/technology/tech-companies-online-speech.html; Kinstler, Linda. 2018. "Germany's Attempt to Fix Facebook Is Backfiring." *The Atlantic.* May 18, 2018. https://www.theatlantic.com/international/archive/2018/05/germany-facebook-afd/560435/;

[62]Ironically, along with a range of "major collection pages" including the Smithsonian Library and PubMed Central archives, one of the URLs flagged as "terrorist" content by the French IRU included a Voice of America Broadcast transcript that discussed the Online Civil Courage Initiative, an online counter-speech effort seeking to reduce hate, violence, and terrorism online in Germany, France, and the UK. Butler, Chris. 2019. "Official EU Agencies Falsely Report More Than 550 Archive.org URLs as Terrorist Content," *Internet Archive Blogs,* April 10, 2019. https://blog.archive.org/2019/04/10/official-eu-agencies-falsely-report-more-than-550-archive-org-urls-as-terrorist-content/

[63]For more discussion of such tradeoffs, see: Whittaker, Joe. 2019. "How Content Removal Might Help Terrorists." Lawfare (blog). June 30, 2019. https://www.lawfareblog.com/how-content-removal-might-help-terrorists.

[64]Geltzer, Joshua, and Dipayan Ghosh. 2018. "The Next Big Internet Threat." POLITICO Magazine. October 27, 2018. https://politi.co/2Q6C9gM. For more examples of the challenges facing technology companies, see posts on Facebook's blog: "Hard Questions." Facebook Newsroom. Accessed January 1, 2019. https://newsroom.fb.com/news/category/hard-questions/.

[65]Braniff, William. 2017. "Recasting and Repositioning CVE as a Grand Strategic Response to Terrorism." National Consortium for the Study of Terrorism and Responses to Terrorism. November 14, 2017. http://www.start.umd.edu/news/recasting-and-repositioning-cve-grand-strategic-response-terrorism.

[66]Alexander, Audrey, and William Braniff. 2018. "Marginalizing Violent Extremism Online." Lawfare. January 21, 2018. https://www.lawfareblog.com/marginalizing-violent-extremism-online

[67]Wiktorowicz, Quintan. 2013. "Working to Counter Online Radicalization to Violence in the United States." Whitehouse.Gov. February 5, 2013. https://obamawhitehouse.archives.gov/blog/2013/02/05/working-counter-online-radicalization-violence-united-states; "Remarks by Assistant Attorney General John Carlin Opening of Madison Valleywood Project." 2016. Department of Justice. https://epic.org/foia/MadisonValleywood_2.pdf.

[68]Ibid.

[69]"Countering Violent Extremism Task Force." 2017. Department of Homeland Security. January 19, 2017. https://www.dhs.gov/cve.

[70]"House Homeland Security Hearing on Domestic Terrorism," C-SPAN, May 8, 2019. https://www.c-span.org/video/?460516-1/fbi-justice-dhs-officials-testify-rise-domestic-terrorism.

[71]A tempered approach will distinguish democratic governments, and the U.S. in particular, from authoritarian counterparts. Shahbaz, Adrian. 2018. "Freedom on the Net 2018: The Rise of Digital Authoritarianism." Freedom House. https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism; Kaye, David. 2019. *Speech Police: The Global Struggle to Govern the Internet.* Columbia Global Reports.

[72]To offer another consideration, the working group should examine how policy priorities and laws concerning terrorism, domestic terrorism, and hate crimes influence efforts to prevent and counter the exploitation of ICTs. Amidst calls for political leaders and lawmakers to enact change, the government's policies and laws concerning terrorism, domestic terrorism, and hate crimes ripple out and affect non-governmental responses,

to these threats in the digital sphere. While resource allocation and rules constrain how officials deal with domestic terrorists compared to suspected members of designated foreign terrorist organizations on U.S. soil, the working group must consider how these dynamics shape the actions non-governmental partners, too. Private companies attempting to prevent and counter terrorist and violent extremist exploitation of their platforms, for example, might come to mirror the priorities of the government. This configuration has its merits, but also invites risks by allowing some organizations to operate online without interference. To learn more about this point, see the following articles: Tiku, Nitasha. 2019. "Tech Platforms Treat White Nationalism Different From Islamic Terrorism." Wired, March 20, 2019. https://www.wired.com/story/why-tech-platforms-dont-treat-all-terrorism-same/; Goldman, Adam. 2019. "F.B.I., Pushing to Stop Domestic Terrorists, Grapples with Limits on Its Power." *The New York Times*, June 4, 2019.https://www.nytimes.com/2019/06/04/us/politics/fbi-domestic-terrorism.html; Birnbaum, Emily. 2019. "FBI Official Sees 'tide Change' in How Platforms Handle Extremist Content." The Hill. May 8, 2019. https://thehill.com/policy/technology/442777-fbi-counterterrorism-official-says-there-has-been-a-tide-change-in-how-tech; McCord, Mary and Jason Blazakis. 2019. "A Road Map for Congress to Address Domestic Terrorism." *Lawfare*. February 27, 2019. https://www.lawfareblog.com/road-map-congress-address-domestic-terrorism; Geltzer, Joshua, Mary McCord, and Nicholas Rasmussen. 2019. "The Christchurch Shooting: Domestic Terrorism Goes International." Lawfare (blog). March 19, 2019. https://www.lawfareblog.com/christchurch-shooting-domestic-terrorism-goes-international; Stransky, Steve. 2019. "Learning From the Past in Addressing Domestic Terrorism." *Lawfare*, April 12, 2019. https://www.lawfareblog.com/learning-past-addressing-domestic-terrorism; Watkins, Ali, and Josh Meyer. 2017. "Domestic Hate Groups Elude Feds." POLITICO. August 15, 2017. https://www.politico.com/story/2017/08/15/us-hate-groups-legal-protections-241653.

[73]For additional information about Section 230 and context for other regulatory considerations, see: Kosseff, Jeff. 2019. *The Twenty-Six Words that Created the Internet*. Cornell University Press; Citron, Danielle Keats. 2014. *Hate Crimes in Cyberspace.* Harvard University Press; Kaye, David. 2019. *Speech Police: The Global Struggle to Govern the Internet.* Columbia Global Reports; Killion, Victoria. 2019. "Terrorism, Violent Extremism, and the Internet: Free Speech Considerations." Congressional Research Service. https://fas.org/sgp/crs/terror/R45713.pdf.

[74]47 U.S. Code § 230 - Protection for private blocking and screening of offensive material. https://www.law.cornell.edu/uscode/text/47/230

[75]Wittes, Benjamin, and Zoe Bedell. 2016. "Did Congress Immunize Twitter Against Lawsuits for Supporting ISIS?" *Lawfare* (blog). January 22, 2016. https://www.lawfareblog.com/did-congress-immunize-twitter-against-lawsuits-supporting-isis.

[76] Keller, Daphne. 2018. "Internet Platforms: Observations on Speech, Danger, and Money." National Security, Technology, and Law. Hoover Institution. https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money; Keller, Daphne. 2015. "Empirical Evidence of 'Over-Removal' by Internet Companies under Intermediary Liability Laws." The Center for Internet and Society at Stanford Law School (blog). October 12, 2015. http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws

[77]Citron, Danielle Keats, and Benjamin Wittes. 2017. "The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity." *Fordham Law Review* 86 (2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3007720.

[78]Ibid.

[79]Ibid.

[80]Freilich, Jaime. 2018. "Section 230's Liability Shield in the Age of Online Terrorist." Brooklyn Law Review 83 (2). https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=2135&context=blr; Citron, Danielle Keats, and Benjamin Wittes. 2017. "The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity." *Fordham Law Review* 86 (2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3007720.

[81]For some examples, see: "Section 230 of the Communications Decency Act." Electronic Frontier Foundation. https://www.eff.org/issues/cda230; Mackey, Jason Kelley and Aaron. 2019. "Don't Repeat FOSTA's Mistakes." Electronic Frontier Foundation. March 29, 2019. https://www.eff.org/deeplinks/2019/03/dont-repeat-fostas-mistakes.

[82]Llansó, Emma. 2019. "Clearing Up Misinformation about Section 230." Center for Democracy & Technology (blog). https://cdt.org/blog/clearing-up-misinformation-about-section-230/. To read the for legislators, visit: "Liability for User-Generated Content Online Principles for Lawmakers." 2019. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2992&context=historical.

[83]For a broader discussion of how best practices may serve as an alternative to regulatory approaches in the context of cybersecurity, see: Singer, Peter and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press; See also, Haughom, Jaclyn. 2016. "Combating Terrorism in the Digital Age: First Amendment Implications," Freedom Forum Institute, https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/combatting-terrorism-in-a-digital-age-first-amendment-implications/;

[84]"Tech Against Terrorism." https://www.techagainstterrorism.org/; See also, "Tech Against Terrorism: Membership Pledge," https://www.techagainstterrorism.org/membership/pledge/.

[85]Sullivan, David. "Company Assessments." Global Network Initiative (blog). https://globalnetworkinitiative.org/company-assessments/.

[86]U. S. Government Accountability Office. 1977. "The Office of Technology Assessment." https://www.gao.gov/products/103962.

[87]"Office of Science and Technology Policy." 2019. The White House. https://www.whitehouse.gov/ostp/.

[88]U. S. Government Accountability Office. 1977. "The Office of Technology Assessment." https://www.gao.gov/products/103962.

[89]"Office of Technology Assessment." University of Northern Texas - Digital Library. https://digital.library.unt.edu/explore/collections/OTA/; U. S. Government Accountability Office. 1977. "The Office of Technology Assessment." https://www.gao.gov/products/103962; Majumder, Bianca. 2019. "Congress Should Revive the Office of Technology Assessment." Center for American Progress. May 13, 2019. https://www.americanprogress.org/issues/green/news/2019/05/13/469793/congress-revive-office-technology-assessment/.

[90]To learn more about the creation of the OTA, see: The Technology Assessment Act of 1972. http://govinfo.library.unt.edu/ota/Ota_5/DATA/1972/9604.PDF; See also, Hahn, Walter, and Rosemary Chalk. 1972. "The Technology Assessment Act of 1972." Congressional Research Service. https://ota.fas.org/reports/CRS-12-1972.pdf; Majumder, Bianca. 2019. "Congress Should Revive the Office of Technology Assessment." Center for American Progress. May 13, 2019. https://www.americanprogress.org/issues/green/news/2019/05/13/469793/congress-revive-office-technology-assessment/.

[91]Graves, Zach. 2018. "R Street Policy Study: Rebuilding a Technology Assessment Office in Congress: Frequently Asked Questions." R Street. https://2o9ub0417chl2lg6m43em6psi2i-wpengine.netdna-ssl.com/wp-content/uploads/2018/09/No.-152.pdf.

[92]Ruane, Kathleen Ann. 2016. "The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes." Congressional Research Service, https://fas.org/sgp/crs/terror/R44626.pdf; Bjelopera, Jerome. 2017. "Domestic Terrorism: An Overview," Congressional Research Service. https://fas.org/sgp/crs/terror/R44921.pdf.

[93] WatchBlog. 2019. "Our New Science, Technology Assessment, and Analytics Team." WatchBlog: Official Blog of the U.S. Government Accountability Office (blog). January 29, 2019. https://blog.gao.gov/2019/01/29/our-new-science-technology-assessment-and-analytics-team/.

[94]Holt, Rush. 2009. "Op-Ed: Reversing the Congressional Science Lobotomy." Wired, April 29, 2009. https://www.wired.com/2009/04/fromthefields-holt/; Tully-McManus, Katherine. 2019. "House Members Call for Office of Technology Assessment Revival," April 2, 2019, sec. congress. https://www.rollcall.com/news/congress/house-members-call-office-technology-assessment-revival; Graves, Zach. 2018. "R Street Policy Study: Rebuilding a Technology Assessment Office in Congress: Frequently Asked Questions." R Street. https://2o9ub0417chl2lg6m43em6psi2i-wpengine.netdna-ssl.com/wp-content/uploads/2018/09/No.-152.pdf.; Majumder, Bianca. 2019. "Congress Should Revive the Office of Technology Assessment." Center for American Progress. May 13, 2019. https://www.americanprogress.org/issues/green/news/2019/05/13/469793/congress-revive-office-technology-assessment/; Pethokoukis, James. 2018. "Congress Should Revive the Office of Technology Assessment." AEI. December 6, 2018. http://www.aei.org/publication/congress-should-revive-the-office-of-technology-assessment/; Editorial Board. 2018. "Legislators Struggle with Tech. That's Why We Need the Office of Technology Assessment." Washington Post, September 17, 2018. https://www.washingtonpost.com/opinions/legislators-struggle-with-tech-thats-why-we-need-the-office-of-technology-assessment/2018/09/17/bb7c30c6-b860-11e8-a7b5-adaaa5b2a57f_story.html?noredirect=on&utm_term=.2122019ad7a7; Sadowski, Jathan. 2012. "The Much-Needed and Sane Congressional Office That Gingrich Killed Off and We Need Back." The Atlantic, October 26, 2012. https://www.theatlantic.com/technology/archive/2012/10/the-much-needed-and-sane-congressional-office-that-gingrich-killed-off-and-we-need-back/264160/.

[95]Matthews, Kyle, and Nicolai Pogadl. 2018. "Big Tech Is Overselling AI as the Solution to Online Extremism." *The Conversation*, September 16, 2018. http://theconversation.com/big-tech-is-overselling-ai-as-the-solution-to-online-extremism-102077.

[96]Singer, Peter and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press. For more on the public's knowledge-gap on cybersecurity, see: Smith, Aaron. 2017. "What Americans Know About Cybersecurity." *Pew Research Center: Internet and Technology*. March 22, 2017. http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.

[97]For more on this anecdote, see "Why is there a cybersecurity knowledge gap, and why does it matter?" sections in the introduction of Singer, Peter, and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

[98]Franceschi-Bicchierai, Lorenzo. 2018. "Cyber Sleuths Find Traces of Infamous iPhone and Android Spyware 'Pegasus' in 45 Countries." *Motherboard*, September 18, 2018. https://motherboard.vice.com/en_us/article/bjaz94/nso-group-pegasus-45-countries-map-spyware-citizen-lab; Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. 2018. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." The Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[99]For more on this recommendation, see: Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. 92-93. https://www.rand.org/pubs/research_reports/RR2647.html

[100] For more on how the government might utilize public service media, see Kaye, David. 2019. *Speech Police: The Global Struggle to Govern the Internet.* Columbia Global Reports, p.126;

[101]The Transportation Security Administration's digital media presence serves as a comedic but powerful model for agencies to regularly communicate information about the agency's responsibilities and efforts in an interesting, informative, and accessible way. For more information, see: Chuck, Elizabeth. 2018. "What's behind the TSA's Hilarious Instagram Account." *NBC News*, April 29, 2018. https://www.nbcnews.com/storyline/airplane-mode/why-tsa-s-award-winning-instagram-account-hilarious-unexpected-n869626.

[102]To learn more about this recommendation and approach, see: Wiktorowicz, Quintan. 2013. "Working to Counter Online Radicalization to Violence in the United States." Whitehouse.Gov. February 5, 2013. https://obamawhitehouse.archives.gov/blog/2013/02/05/working-counter-online-radicalization-violence-united-states

[103]Jackson, Brian, Ashley Rhoades, Jordan Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley. 2019. "Practical Terrorism Prevention Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence." RAND. https://www.rand.org/pubs/research_reports/RR2647.html

[104]See, for example, how matters concerning terrorists' use of the internet might fit into the Department of Homeland Security's "Stop.Think.Connect" campaign. "STOP. THINK. CONNECT." 2015. Department of Homeland Security. March 23, 2015. https://www.dhs.gov/stopthinkconnect. To learn more about this recommendation and approach, see: Wiktorowicz, Quintan. 2013. "Working to Counter Online Radicalization to Violence in the United States." Whitehouse.Gov. February 5, 2013. https://obamawhitehouse.archives.gov/blog/2013/02/05/working-counter-online-radicalization-violence-united-states

[105]For example, in December 2016, Facebook, Microsoft, YouTube, and Twitter announced a hashing-centric information-sharing partnership to more effectively flag problematic materials with algorithms. In 2017, the four companies formalized the partnership under the banner of the Global Internet Forum to Counter Terrorism (GIFCT), which develops technological solutions, supports research, and promotes knowledge sharing across the ecosystem of technologies exploited by extremists. Although the GIFCT has its strengths and weaknesses, in partnership with Tech Against Terrorism, it helps many smaller companies develop the capabilities necessary to prevent and counter the abuse of their platforms. "Partnering to Help Curb the Spread of Terrorist Content Online." 2016. Twitter Blogs. December 5. https://blog.twitter.com/2016/partnering-to-help-curb-the-spread-of-terroristcontent-online; "Global Internet Forum to Counter Terrorism." 2017. Twitter Blogs. June 26. https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html. For more information about the GIFCT, visit: Global Internet Forum to Counter Terrorism, 2019, https://www.gifct.org/about/.

[106]"About Tech Against Terrorism." Tech Against Terrorism, https://www.techagainstterrorism.org/about/.

[107]Ibid.

[108]"Knowledge Sharing Platform." Tech Against Terrorism, https://ksp.techagainstterrorism.org/.

[109]Pearce, Matt. 2017. "Squeezed out by Silicon Valley, the far right is creating its own corporate world," *LA Times*, August 12, 2017. http://www.latimes.com/nation/la-na-alt-right-money-20170811-story.html.

[110] Facebook's partnership with the Institute for Strategic Dialogue, for example, led to the Online Civil Courage Initiative which strives to "mount a proportional response to the propagation of hate, violence and terrorism online, across Europe." With relative support from industry, the Institute for Strategic Dialogue also piloted a program that facilitated one-on-one, direct engagement with individuals showing signs of radicalization online. Such efforts are critical to progress as they leverage methods that are not viable to most governments. Online Civil Courage Initiative. 2018. Institute for Strategic Dialogue. https://www.isdglobal.org/programmes/communications-technology/online-civil-courage-initiative-2/; Davey, Jacob, Jonathan Birdwell and Rebecca Skellett. 2018. "Counter Conversations: A model for direct engagement with individuals showing signs of radicalisation online." Institute for Strategic Dialogue. http://www.isdglobal.org/wp-content/uploads/2018/03/Counter-Conversations_FINAL.pdf. The P2P program facilitated by EdVenture Partners offers another illustration of how industry can support alternative approaches to counter violent extremism. "Peer to Peer – Facebook Global Digital Challenge. EdVenture Partners. https://edventurepartners.com/peer-to-peer-facebook-global-digital-challenge/.

[111] "DHS Announces the Launch of the 'Countering Terrorists Exploitation of Social Media and the Internet' Training." 2018. Department of Homeland Security. June 11, 2018. https://www.dhs.gov/blog/2018/06/11/dhs-announces-launch-countering-terrorists-exploitation-social-media-and-internet.

[112] Ibid.

[113] Ibid.

[114] Ibid.

[115] "Santa Clara Principles on Transparency and Accountability in Content Moderation." Santa Clara Principles. https://santaclaraprinciples.org/images/scp-og.png.

[116] Fishman, Brian. 2019. "Crossroads: Counter-terrorism and the Internet*," National Security Law Review,* 2(2). https://tnsr.org/2019/04/crossroads-counter-terrorism-and-the-internet/

[117] Birnbaum, Emily. 2019. "FBI Official Sees 'tide Change' in How Platforms Handle Extremist Content." The Hill. May 8, 2019. https://thehill.com/policy/technology/442777-fbi-counterterrorism-official-says-there-has-been-a-tide-change-in-how-tech;

[118] Ibid.

[119] Birnbaum, Emily. 2019. "FBI Official Sees 'tide Change' in How Platforms Handle Extremist Content." The Hill. May 8, 2019. https://thehill.com/policy/technology/442777-fbi-counterterrorism-official-says-there-has-been-a-tide-change-in-how-tech; "House Homeland Security Hearing on Domestic Terrorism," C-SPAN, May 8, 2019. https://www.c-span.org/video/?460516-1/fbi-justice-dhs-officials-testify-rise-domestic-terrorism.