World War Web: Rethinking "Aiding and Abetting" in the Social Media Age

Rebecca J. Cambron
World War Web: Rethinking “Aiding and Abetting” in the Social Media Age

Rebecca J. Cambron

ISIS’s use of social media presents a new challenge for counterterror efforts. The organization aims to recruit followers and incite violence through social media. Given that this is a new medium for terrorist organizations, social media companies have come under fire for indirectly providing ISIS with far-reaching platforms to spread its content. The companies, as well as national governments and international entities, have attempted to respond to the threat posed by such content. These responses, however, have proven ineffective. This Note argues that to effectively respond to and combat the threat posed by terrorist speech, national governments should adopt a new approach—an approach which holds social media companies responsible for aiding and abetting terrorist speech inciting violence. Identifying the specific threat as stemming from terrorist speech recruiting for or directly inciting violence narrows the scope of social media companies’ potential liability. Additionally, the use of INTERPOL’s existing information-sharing systems provides a means of maintaining a “bird’s eye view” of terrorism’s trends, while its National Central Bureaus provide nation-specific notifications of terrorist speech. Subsequently, national law enforcement should impose the aiding and abetting standard on social media companies that fail to remove the content identified by INTERPOL. Through this blend of international and national enforcement, freedom of expression receives protection through the limited scope of liability while moving towards improved national and global security.

CONTENTS

I. Introduction ........................................................................... 294
II. ISIS’s Development and Established Use of Social Media Has Yet To Be Effectively Countered By Social Media Companies or Government Entities................................................................. 296
   A. Fueled by its Ideology, ISIS Melds its Religious Zealotry with Social Media to Facilitate its Ideological and Political Goals......... 297

* Rebecca J. Cambron is a J.D. candidate at Case Western Reserve University School of Law, Cleveland, Ohio, May 2019; B.A. in Government, Patrick Henry College, Purcellville, Virginia, May 2016.
B. Current Responses by Social Media Companies and Government Entities Fail to Appreciate the Long-Term, Global Threat Posed By the Combination of Social Media and ISIS........................................299

III. Social Media Companies Should Be Held Liable for Aiding and Abetting Terrorist Organizations When They Knowingly Permit Terrorist Speech to Remain on Their Platforms.................................................................312

A. A Limited Definition of “Terrorist Speech” In Conjunction with the Use of An International Aiding and Abetting Standard Best Facilitates Holding Social Media Companies Responsible for Terrorist Content.................................................................312

B. Joint Implementation Through INTERPOL’s Existing Resources and National Judicial Systems Provides the Best of International and National Systems for Combatting Terrorist Speech........................................317

IV. Holding Social Media Companies Responsible Addresses the Residual Concerns Related to Free Expression and National Sovereignty.................................................................322

A. The Limited Scope of Liability Respects Free Expression While Securing a Means of Increasing National and Global Security........322

B. States Maintain Control Over The System, Protecting Their Sovereignty, Through the Integration of State Terrorist Designations and Judicial Systems..................................................324

V. Conclusion..................................................................................325

I. Introduction

The world has changed significantly since it first came in contact with those who orchestrated the bombing of the World Trade Center in September 2001. While many have used terrorism as a tactic to achieve their political or religious ends, al-Qaeda blazed a new trail. Fast-forward to today, the non-state actor birthed by al-Qaeda presents a host of new challenges to the national security community. Unlike those who have relied on terrorism before, the non-state actor has no formal government which the U.N. or national governments may sanction.1 Fluid boundaries make precise counterattacks challenging.2 Government must now launch wars against groups few have heard of, lacking a definition of who or what it can declare war against.3

The traditional understanding of terrorism and counterterrorism tactics no longer provides an adequate response to the threat posed


2. Id.

3. Id.
by non-state terrorist organizations, like ISIS and al-Qaeda. The characteristics of their groups alone posed a challenge to the defense and intelligence communities following 9/11. But an additional complication emerged in the early 2000s: society changed. Following the increased use of the internet, the rise of social media platforms catalyzed non-state actors’ abilities to spread their message. Social media effectively eliminated organization costs, allowing terrorist groups to easily create a global, structured threat.

The confluence of non-state terrorist organizations and social media generates a host of new challenges for combating terrorism. ISIS, also known as the Islamic State, IS, Daesh, or ISIL, exemplifies how terrorist organizations may use social media companies’ platforms in the future. Viewing the online, social-media world as a new “theater of war” for terrorism requires experts, policy makers, and those tasked with combating terrorism to think differently about counterterrorism methods. More fundamentally, however, it forces them to prioritize the value judgments they make in creating policies and strategies.

Those combating terrorism have attempted to reduce the threat through a variety of methods. But the threat persists. This Note argues that to address the new challenges, national governments should hold social media companies responsible for aiding and abetting terrorist speech used to recruit for and incite violence through an international standard. Relying on the foundation laid in customary international law for complicity-based liability, national jurisdictions can impose responsibility when social media companies facilitate terrorist speech by permitting the speech to remain on the platforms. A limited definition of “terrorist speech” based on the type of content and the terrorist organization posting it aids in limiting the

4. See id. (commenting that non-state actors, such as terrorists, challenge governments and are using new technology).

5. Id.


scope of liability. Within the limited scope, INTERPOL and national judicial systems may combine efforts to effectively address the new threat to global security.

Part I of this Note will discuss the background of terrorist organizations’ current use of social media and the short-sighted and patchwork responses from social media companies, national governments, and international entities. It will identify key obstacles to effective responses and potential ways to overcome them. Subsequently, Part II will argue that a more effective solution can come from holding social media companies responsible for aiding and abetting the terrorist organizations under a system of joint enforcement by national jurisdictions and INTERPOL. Part II will also define the scope of liability based on a limited definition of “terrorist speech” and how the presence of such speech on social media platforms constitutes aiding and abetting. Using this definition to limit the scope of enforcement, Part II will continue by describing the system of implementation through both INTERPOL’s monitoring and notification processes, and national governments’ law enforcement. This collaborative system of operation ensures the most responsive means of addressing developments in terrorist speech. Should companies fail to remove the content after notification, national law enforcement and judiciaries may step in and prosecute under the international standard. Lastly, Part III concludes that imposing responsibility does not undermine free speech or national sovereignty, but instead utilizes a narrow definition of “terrorist speech,” restricting a limited form of communication connected to violent actions of national concern. In such a manner, joint implementation simultaneously respects national sovereignty and individual rights while combating the global threat posed by terrorist speech on social media.

II. ISIS’s Development and Established Use of Social Media Has Yet To Be Effectively Countered By Social Media Companies or Government Entities.

Social media companies and governments have struggled in their counterterrorism efforts to appropriately respond to the nature of the threat posed by terrorist speech on social media. With the birth and subsequent proliferation of social media into everyday life, the Islamic State discovered a global medium for its message. The example set by ISIS for future terrorist organizations creates a new challenge for countering such organizations’ behavior. Responses by the platform’s


companies and governments inadequately address terrorism-related content that incites violence or participation in violence; ignoring the inevitable development of terrorist tactics requires more long-term, systematic solutions.\textsuperscript{12}

A. Fueled by its Ideology, ISIS Melds its Religious Zealotry with Social Media to Facilitate its Ideological and Political Goals

The new world created by social media transformed not only the way regular individuals engage with each other, but also opened up a new means of communication exploitable by non-state terrorist organizations. Social media’s growth during the early 2000s coincided with the rise of a new ideological strand of Islamic jihadist teachings—teachings which formed ISIS’s foundation.\textsuperscript{13} This collision of events enabled ISIS to use social media to advance its ideological goals more effectively and directly than its predecessors.\textsuperscript{14} Despite ISIS and al-Qaeda sharing a similar desire for the creation of a caliphate, a nation-state based on Islamic laws,\textsuperscript{15} the two organizations varied in how to achieve their political goals.\textsuperscript{16} These different strategies condense into a disagreement as to how much support for their political ends each organization seeks from the Muslim world.\textsuperscript{17} Al-Qaeda believes in the necessity of “winning the hearts and minds” of local Arab tribes, recalling the Prophet Muhammad’s uniting of tribal factions in creating his Islamic state.\textsuperscript{18} ISIS, on the other hand, does not require support from the Muslim community in the Middle East.\textsuperscript{19,20}

\begin{footnotes}
\footnotelineup
12. See id. at 6-7 (noting the continuous analysis of the threat posed by Islamic extremism and the need for constant re-assessment).
13. Id.
14. Id.
15. Id.
16. Id.
17. Id.
19. 9/11 Memorial & Museum, supra note 8.
20. Though both ascribing to the teachings of Muhammad, ISIS and al-Qaeda have developed into two different strands of Islam, much like differing protestant denominations. Despite sharing a desire to create a caliphate the two organizations varied in three major aspects: (1) strategies for achieving caliphates, (2) the timing of when to establish a caliphate, and (3) the interpretation of the end times. The strategies for achieving a caliphate reflect each “denomination’s” reliance on Muslim tribes. Al-Qaeda reflects back on Muhammad’s actions and believe in
\end{footnotes}
These differing viewpoints on the role of the Muslim community directly influence the willingness of each organization to use violence in order to achieve their political objectives. Because it has no need for support from the Muslim community and therefore openly uses violence against those within its geographic control, ISIS turns to and relies on foreign fighters and international terror attacks to bolster recruitment and keep it in the minds of the public and other jihadists. The Guardian’s series *The Raqqa Diaries* recounts life inside the ISIS-held city. A young man writes of how ISIS first came through the city in March 2013 saying:

They took advantage of our confusion and ignorance. .. At first they would charm people with a softly spoken manner, promising them the world. .. Those who actually believe they have come to save us were the first to enter the city; the second are much more violent.

This approach contrasts with the concern al-Qaeda had with maintaining the support of those under their political control, as Bin Laden counseled members to avoid killing any other Muslims so as to not alienate the community. Because they can use violence against the Muslim community, social media plays a valuable role in building support for ISIS outside of the Middle East. By giving ISIS a way of shaping its image, social media helps the organization hide the reality experienced in Raqqa and other cities and maintain an online presence. International attention—and social media as a means of

the need to create a “greater religious identity” within all of the Muslim world. Thus, al-Qaeda hesitates to take actions which may alienate other Muslims. ISIS, on the other hand, does not believe this “greater identity” is required, leaving it free to be more forceful and violent against Muslims in the Middle East as it seeks to establish a new caliphate. See 9/11 Memorial & Museum, *supra* note 6 and McCants, *supra* note 8 for Dr. McCant’s further explanation of the intellectual development of ISIS from al-Qaeda.

21. *Id.*

22. *Id.*


24. *Id.*


26. See 9/11 Museum & Memorial, *supra* note 8 (noting the need for both propaganda and public attention).
it—therefore plays a key role in fulfilling the ideological basis for ISIS’s mission.27

B. Current Responses by Social Media Companies and Government Entities Fail to Appreciate the Long-Term, Global Threat Posed By the Combination of Social Media and ISIS.

Fully addressing the presence of ISIS and its related content on social media has proved a challenge on two fronts, namely, (1) in undermining why terrorists use social media platforms and (2) in constructing adequate and effective responses to that use. Social media provides a particularly attractive means for ISIS to promote its ideology through its global influence, accessibility, and evolving nature.28 These uses, in turn, generate problems for creating effective responses by those seeking to prevent the spread of terrorism.29 Current methods failed to adequately address the long-term, global threat with the limited resources devoted to counterterrorism efforts.

1. Social Media Platforms Create an Attractive Environment for ISIS to Spread its Content.

The environment formed by the internet and social media platforms benefits terrorist operations like ISIS. As discussed above, ISIS’s ideological background creates a need for international attention.30 The internet’s global reach provides a stage for ISIS to make its call for violence, amplified through social media’s increasing number of users.31 The ease at which those related to or expressing support for the organization can create social media accounts, create multiple accounts, or re-create accounts, even if banned, fashions an environment encouraging the spread of harmful messages.32 This ease of access, in combination with the evolving nature of the

27. Id.

28. See Patrikarakos, supra note 9 (noting the ease of access, popularity and inadequate responses incentivizing ISIS’s use of social media for propaganda).


30. 9/11 Memorial & Museum, supra note 8.


internet, facilitates the spread of terrorist speech, unrestricted by the most popular social media sites.

i. Social Media Platform’s Global Reach Attracts Terrorist Organizations Seeking to Spread Their Message and Shape Their Perception In the World.

Social media’s global influence provides an attractive avenue for ISIS to facilitate their ideological goals. Foreign terrorist fighters flock from over 100 countries to fight with ISIS, al-Qaeda, or an affiliate. Sally Jones, from the United Kingdom, was one such fighter. Jones went to Syria to marry an ISIS member and became active in the recruitment of other young girls to become “jihadi brides” and marry other ISIS members. Twenty Twitter accounts linked to her information expressed support for ISIS. Recruitment to the Middle East, however, is only part of the global influence ISIS wields. The call issued by clerics and Islamist leaders like Abu Musab al-Zarqawi, leader of al-Qaeda in Iraq, and Osama Bin Laden incited violence across the globe. In questioning how the Boston Marathon Bombing by the Tsarnaev brothers came about, investigators found jihadist writings, al-Qaeda propaganda, as well as YouTube videos of speeches by radical clerics on one of the brother’s computers. Similarly, in December 2017, a U.S. district court sentenced a Massachusetts man to 28 years in prison for supporting ISIS and using a Twitter page for the “Lions of America” to call on his followers to kill Americans.

33. 9/11 Memorial & Museum, supra note 8.
35. Id.
36. Id.
These incidents demonstrate the role of social media as a global resource—facilitating terrorist activity by publishing content for incitement and recruitment for violent actions. Far beyond the physical presence of ISIS in the Middle East, social media serves to magnify ISIS’s ideology.

ii. The Ease of Access Many Social Media Platforms Have Creates a Unique Environment for Terrorist Organizations to Exploit, Constantly Reappearing Even After Removal.

Social media also attracts terrorist content due to the ease at which those associated with the organizations can access the platforms. To create a Twitter account, an individual only needs to provide a name, phone number or e-mail, and create a password. Facebook requires the same information, in addition to a birth date. In turn, internet-based e-mail accounts, such as Gmail and Yahoo, also require minimal information to set up, typically only a phone number and birth date. Such ease of access creates few, if any, barriers to individuals creating multiple accounts, further complicating the issue. The ease of rejoining Twitter after an account suspension or creating multiple Facebook accounts means eliminating users is ultimately only a delay in—not a denial of—the posting of terrorist content. Because of this simplicity, the environment generated by social media platforms welcomes those

41. See Office of Public Affairs, supra note 37; see also O’Neill, supra note 34 (noting the use of social media to publish content recruiting for and incitement to violence).


45. See Cellan-Jones, supra note 32 (discussing how a terrorist supporter used multiple accounts, despite prohibitions against having multiple accounts on social media networks).

46. Laura Huey, This is Not Your Mother’s Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming, 6 J. TERRORISM RES. 1, 4 (2015), available at https://www.researchgate.net/publication/281275705_This_is_Not_Your_Mother’s_Terrorism_Social_Media_Online_Radicalization_and_the_Practice_of_Political_Jamming.
attempting to spread an unwelcome message. Hostile messages, although perhaps in name disowned, in reality face few roadblocks to reappearing on the platforms.

iii. Social Media’s Constant Evolution Makes an Environment Open to Abuse by Terrorist Organizations as They Quickly Gain Access and Recreate Their Perception for Each New Platform.

The internet’s evolving nature makes it an environment ripe for abuse as ISIS seeks new, unregulated means of spreading its message. Just over the past decade, the internet has changed dramatically.\(^ {47} \) From the launch of the iPhone in 2007,\(^ {48} \) to Facebook’s billionth user in 2012,\(^ {49} \) and new interactive content,\(^ {50} \) the internet bears limited resemblance to the worldwide web introduced in 1990.\(^ {51} \) Social media, likewise, has undergone dramatic changes from the early time of AOL\(^ {52} \) and Myspace.\(^ {53} \) Since that time, social media platforms such as YouTube, Facebook, Twitter, Instagram, and others, have allowed users to take part in the ever-expanding worldwide web, generating content and creating a new type of connectedness between people.\(^ {54} \)

---

47. Grace Reader, 11 Big Changes to the Internet from the Past Decade, ENTREPRENEUR (July 28, 2016), https://www.entrepreneur.com/article/279844 [perma.cc/C5UQ-UYD7].

48. Rene Ritchie, 11 Years Ago Today, Steve Jobs Introduced the iPhone, iMORE (Jan. 9, 2018), https://www.imore.com/history-iphone-original [perma.cc/VNQ3-3TVB].


Terrorist organizations take advantage of these evolving networking opportunities, adapting their message to new cultural trends. Via social media, ISIS uses pop culture references to lure in younger generations and change the way they view the organization and its goals, a technique known as “jihadi cool.” Described as a “new hipster pop-jihadism,” jihadi cool accentuates the new “brand” of jihad. As EUROPOL notes:

The religious component in recruitment and radicalization is being replaced by more social elements such as peer pressure and role modelling. Additionally, the romantic prospects of being part of an important and exciting development, apart from more private considerations, may play a role. Suicide bombers see themselves more as heroes than as religious martyrs.

Terrorist organizations also manipulate media in an effort to draw attention to themselves, such as using a picture of German Chancellor Angela Merkel with a refugee and connecting the refugee to terrorism. A study by the Brookings Institute found that, in an effort to increase viewership, 40 percent of ISIS’s videos included “cultural images of modernity in order to promote a political project based on anti-modern values.” The constantly-evolving nature of social media and pop culture creates an opportunity for ISIS to infiltrate the platforms and use current trends to aid in the spread of their content.

55. Huey, supra note 46, at 1.
56. Id.
2. Current Government Responses Fail to Effectively Address the Appeal of Social Media for Terrorist Organizations and Their Presence on Various Platforms.

Despite the numerous angles and tactics employed to combat ISIS’s use of social media, social media companies and government entities have failed to construct effective means of reducing its presence online.61 This failure stems from two underlying concerns unaddressed by the entities’ efforts, namely the long-term threat posed by ideologies like ISIS’s and jurisdictional gaps in coverage. Current efforts support only short-term solutions to a long-term problem thereby promoting inefficiency. Resource limitations further exacerbate this problem. Similarly, jurisdiction-based responses fail to appreciate the global nature of Islamic extremism. With these various limitations, current solutions cannot achieve a meaningful barrier to terrorist content.

i. Short-term Solutions Typify Social Media Companies’ and Government Entities’ Responses, Ignoring the Long-Term Ideological and Methodological Threat Posed by ISIS’s Example.

Limited responses with a short-term perspective plague current approaches to terrorists’ exploitation of social media. Without fully appreciating the expansive threat posed by radical Islamic ideologies and the powerful tool social media companies have placed in the hands of the ordinary people, those responding to the threat present flawed solutions.62 The possibility for future terrorist organizations to develop from ISIS, when considered in light of the limitations faced by current responses both in terms of software and resources, highlights the challenge faced by those tasked with reducing the threat posed by terrorist content on social media.63

National governments focus their solutions on addressing the threats here-and-now, overlooking the long-term ideological and methodological threats posed by the current use of social media by ISIS. Just as ISIS developed from the foundation laid by al-Qaeda, so too could the next major terrorist threat to global safety and

61. Patrikarakos, supra note 9.

62. See Bruce Hoffman, INSIDE TERRORISM 214-220 (2006) (noting the difficulty those combating terrorism may have in identifying the religious motivations of terrorist groups).

security. In his cultural history of terrorism, Michael Burleigh follows the trends of Islamic terrorism starting in the late 1970s, noting the combination of religious enthusiasm and secondary events which spurred increased terrorist activity. Such trends can easily continue into the future. For example, Boko Haram in Nigeria and Al-Shabaab in Somalia, both originally affiliated with al-Qaeda, have pledged allegiance to ISIS. Each holds the same ideological goals of establishing a caliphate and, based on the attacks each has committed on the citizens of their "home" countries, appears to accept ISIS's perspective on violence as well. Should these two organizations seek to develop a larger international presence, they would likely look to ISIS's use of social media as an example.

Similarly, terrorist organizations do not copyright or trademark their tactics—they may freely develop off the "successes" of others. Terrorist organizations can take, develop, and manipulate the methods of violence previously used by others to fit their needs. As such, the use of one tactic by an organization can quickly spread to others, even if they do not share ideological similarities.

The development of suicide bombings as a means of terrorist attack demonstrates the auxiliary nature of shared ideological fervor. Suicide bombing, according to historian Jeffrey Lewis, developed alongside the creation of dynamite. Prior to the Russian Revolution, one radical held the dynamite while approaching the czar, not detonating until close enough to kill them both. The Japanese

---

64. See Michael Burleigh, BLOOD AND RAGE: A CULTURAL HISTORY OF TERRORISM 346 (2009) (noting the pattern of Islamic terrorism and its development off of trends formed in the Middle Ages).
65. Id.
67. Yan, supra note 66.
69. Id.
70. Id.
71. Id.
72. Id.
adopted this approach for the Kamikazes in World War II.73 Hezbollah in the 1980s generated the type of suicide bombing typical of today, using the tactic against U.S. military installations.74 This form of development presents a problem for national governments’ current responses. No international database of terrorist methods exists.75 National governments tend to focus on those threats most concerning to them in the present or near future, as evidenced by their special designations of “terrorist organizations.”76 Relying on restricted perspectives and lack of appreciation for the long-term ideological and methodological threat stemming from ISIS’s example, counterterrorism efforts will necessarily have limited prospective impact.

Limitations in technology used to identify and eliminate terrorist content further compounds the failings created by a short-term perspective. Social media companies, especially Facebook, rely on artificial intelligence software to identify content that infringes on copyrights or contains child pornography.77 More recently, companies have tried to alter the algorithms to identify extremist images or language and delete the accounts created by banned users.78 Through such tools, Twitter removed nearly 300,000 accounts linked to terrorism.79 Terrorist content, however, is far more likely to be used in news articles or non-propaganda settings than restricted content—a

73. Id.
74. Id.
77. Emily Dreyfuss, Facebook’s Counterterrorism Playbook Comes Into Focus, WIRED (June 17, 2017), https://www.wired.com/story/facebook-counterterrorism/ [https://perma.cc/QTB2-TFSA].
78. Id.
contextual distinction difficult for computer programs to accurately determine. For example, in 2011, a French teacher sued Facebook for removing a picture he posted of a piece of artwork by Gustave Courbet, on the grounds that the work depicting a naked woman was art, not explicit material.

Relying on artificial intelligence to make such contextual distinctions undermines the full effectiveness of the algorithms as mathematical calculations struggle to make the determination. As one author notes, only through “human hand-holding” and years of training do machines like IBM’s Watson win against Jeopardy greats. The years necessary to hone the technology to address specific content fails to effectively counter the evolving nature of terrorist organizations. Altering programs to perform at the level necessary takes time—time which works in terrorist’s favor.

National governments’ offensive efforts likewise demonstrate their short-sighted perspective on the distribution and use of limited resources. The U.S., for example, produces counter-propaganda to dilute the influence of ISIS publications. During 2013-2014, the State Department published over 300 videos on YouTube to specifically counter ISIS, the most popular video having 120,000 views. On Twitter, the U.S. operates six different accounts for this purpose. These posts, however, face an uphill battle. Not only do they miss the long-term threat from future terrorist organizations who may adopt ISIS’s example, they must also gain attention in the overwhelming

80. See Heidi Glenn, How Facebook Uses Technology To Block Terrorist-Related Content, NPR (June 22, 2017), https://www.npr.org/sections/alttechconsidered/2017/06/22/533855547/how-facebook-uses-technology-to-block-terrorist-related-content [https://perma.cc/FJ76-B37C] (discussing anecdotes where Facebook’s algorithms have flagged news content and employees restored the content after reviewing it themselves).


82. See Baciu, supra note 63 (describing A.I.’s continued reliance on humans for context-based determinations).

83. Id.


85. Id.

86. Id.

87. See Kriel & Duggan, supra note 66 (reporting an Al Shabaab faction’s declaration of allegiance to ISIS).
sea of social media content. Such counter-narratives must fight for influence amongst the 6,000 tweets made per second.\footnote{INTERNET LIVE STATS, http://www.internetlivestats.com/twitter-statistics/ (last visited Mar. 21, 2018) [https://perma.cc/26J5-PTV7].} Not only must the counter-propaganda reach those same individuals targeted by ISIS to be truly effective, but they must attempt to do so amidst a staggering amount of other material. Even videos face a battle as YouTube estimates that users upload 48 hours of content every minute, accumulating to eight years of content a day.\footnote{U.N. OFFICE OF DRUGS AND CRIME, THE USE OF THE INTERNET FOR TERRORIST PURPOSES 126 (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [https://perma.cc/TLL3-XSQB].}

Additionally, these efforts do little to groups like ISIS who do not care about local, popular support and have the sheer quantity of user-generated content on their side.\footnote{World Affairs, William McCants: The ISIS Apocalypse, YOUTUBE (Dec. 21, 2015), https://www.youtube.com/watch?v=kur-qWNkzng [https://perma.cc/52YP-8JFT].} Providing a counter-narrative undoubtedly contributes to the disruption of ISIS’s presence on platforms. Such counter-propaganda, however, challenges a narrative ISIS cares little about as evidenced by the treatment of those in Raqqa.\footnote{Lesaca, supra note 84; see also The Raqqa Diaries, supra note 20.} Instead of using these social media resources to generate fewer but more impactful posts or to head-off developing terrorist organizations, the best counter-propaganda comes from those with likely even fewer resources. Footage leaked by a Kurdish media network showed the rescue of ISIS-held, Kurdish prisoners.\footnote{Lesaca, supra note 85.} That video received 1.2 million views in five days.\footnote{Id.} Lacking analytics to see the trends in terrorist organizations and their tactics across platforms and nations,\footnote{See Stieglitz et al., supra note 75.} social media companies’ and national governments’ work gets only a portion of the overall picture, or ends up drowning in an crushing amount of user content unable to have a truly effective response.

\textit{ii. Reliance on National Regulations to Combat Terrorist Content on Social Media Creates Gaps in Coverage Exploitable by Terrorist Organizations.}

Jurisdictional and treaty gaps additionally plague the ability of those combatting terrorism to do so effectively. Conflicts of jurisdiction arise as each nation attempts to address the threat in its own way. These conflicts stem from a variety of factors, including
each nation’s different regulatory schemes and the international community’s lack of a comprehensive response, resulting in the absence of a universal standard underlying jurisdictional differences. Without uniformity at either the national or international level, terrorist organizations will be quick to exploit any gaps in coverage they discover.

At its core, the nature of terrorism alters the stakes at issue when discussing terrorist content on social media, limiting the effectiveness of purely national responses. Unlike crimes which occur wholly within one jurisdiction, the spread of terrorist content across social media absorbs the characteristics of terrorism and cybercrimes, generating a transnational conflict. According to the U.S. Director of National Intelligence, cyber instability poses a growing threat to international security, rivaling terrorism, organized crime, and weapons of mass destruction. Given this threat, national governments seek better responses to terrorist organizations’ use of social media, but conflicting regulatory measures fail to create an effective obstacle to the influence wielded online. For example, both France and Germany have proposed regulations for social media companies for the content posted on their platforms. Germany proposed to fine the companies for any hate speech not removed within 24 hours. France, in comparison, proposed a regulation requiring platforms to reveal sponsored content or the government would block internet access to their platform. Such differences in regulations create hurdles for the companies to comply with and potentially cause jurisdictions to become safe harbors for terrorist content because of lax or non-


98. Burns, supra note 97.

99. Su, supra note 97.
existent regulations on an issue.\textsuperscript{100} Because regulation through national jurisdictions promotes gaps and variances in coverage, international law offers a comprehensive alternative.

Current international law, however, fails to take more than a patchwork approach to addressing the impact of terrorist content.\textsuperscript{101} International treaties and agreements make few, if any, references to cyberattacks or terrorist publications.\textsuperscript{102} Rather than comprehensive coverage, the treaties approach terrorism in a piecemeal fashion, each addressing a specific type of terrorism or aspect of its spread.\textsuperscript{103} Further, the lack of a universal definition of “terrorism” inhibits the international community’s ability to create a more comprehensive agreement.\textsuperscript{104} The U.N. Security Council’s resolutions cover more of the threats, including cyberattacks, but maintain the patchwork limitations.\textsuperscript{105} Resolutions and reports, however, pose no binding authority on state action.\textsuperscript{106} Without a means of enforcement against states, many international law resolutions or agreements remain recommendations for state behavior rather than impactful laws addressing a global security issue.\textsuperscript{107} This lack of consensus results in

\textsuperscript{100} See U.N. Office of Drugs and Crime, supra note 86, at ¶ 91 (discussing the lack of a universal instrument addressing terrorist activity online and providing guidance on the criminalization, investigation, and prosecution of terrorist cases involving the internet).


\textsuperscript{102} Lotrionte, supra note 95, at 905-06.

\textsuperscript{103} See U.N. Office of Counter-Terrorism, supra note 94 (reciting the key General Assembly and Security Council resolutions and their targeted application).

\textsuperscript{104} Alan Dershowitz, Why Terrorism Works 4 (2002).

\textsuperscript{105} David P. Fidler, Cyberspace, Terrorism and International Law, 21 J. Conflict & Security L. 475, 478-79 (2016).


\textsuperscript{107} See Are UN Resolutions Binding?, DAG Hammarskjöld Library, http://ask.un.org/faq/15010 (last visited Mar. 21, 2018) (lists examples of resolutions and discusses how the nature of resolutions determines the extent to which they are binding on States); see also Oberg, supra note 103.
nothing more than suggestions for states to follow, with no impact on states’ actions and maintaining the regulatory gaps.

Social media’s role in facilitating terrorist content raises the question of social media companies’ responsibilities for self-censoring posts that recruit for or incite violence. Throughout the U.S. and Europe, individuals have filed civil legal claims against social media companies for their role in facilitating and/or radicalizing terrorists.108 Twitter, specifically, faces legal claims from families of the victims of the ISIS terror attacks in Paris and Brussels.109 The families argue that Twitter aided and abetted ISIS before, during, and after the attacks; they allege that “among social media platforms, Twitter has been the most stubborn one to refuse to cut off its service to terrorists, taking the position that ‘the tweets must flow,’ even if it means assisting in mass murder.”110 A Dallas police officer injured in the 2016 shooting filed a claim against Facebook, Google, and Twitter alleging the same concerns.111 But for the use of these platforms, according to the officer, the attacker would not have shot at the police.112 German courts heard a similar case against Facebook brought by the refugee whose picture with Chancellor Merkel was manipulated by terrorist organizations.113 Though these cases have yet to hold social media companies liable, they demonstrate the judicial system’s openness to holding social media companies responsible for their role in facilitating terrorist violence.


110. Id.


112. Id.

113. Eddy, supra note 59.
III. **Social Media Companies Should Be Held Liable for Aiding and Abetting Terrorist Organizations When They Knowingly Permit Terrorist Speech to Remain on Their Platforms.**

Without a redirection of incentives, few long-term barriers to terrorist content on social media platforms will develop. Utilizing a narrow definition of prohibited “terrorist speech,” enforced through national criminal justice systems, social media companies should now be held liable for aiding and abetting terrorism. The combination of an international aiding and abetting standard and a universal definition of “terrorist speech” counters the commercial incentives, enabling companies to self-regulate and avoid liability. Having social media companies take responsibility for knowingly permitting the most dangerous forms of “terrorist speech” to remain on their platforms after notification refutes social media companies’ incentives. If the companies fail to respond, however, a means of imposing punishment is available. Joint implementation through both international monitoring and national enforcement provides a means of holding companies responsible and further counters the incentives towards short-term, ineffective solutions.

A. **A Limited Definition of “Terrorist Speech” In Conjunction with the Use of An International Aiding and Abetting Standard Best Facilitates Holding Social Media Companies Responsible for Terrorist Content.**

1. Limiting the Scope of Liability by Narrowly Defining What Type of Speech and Whose Speech Can Create Liability for Social Media Companies Protects Free Expression While Providing a Means of Self-Censorship to Companies.

Prior to any discussion of liability, a clear articulation of what content creates liability is necessary. To formulate a definition of what type of speech should justify liability, a careful balance must be struck between national security concerns and free expression. The International Covenant on Civil and Political Rights codified the principles of freedom of expression in Article 19, stating that,

---

“Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.”115

It recognizes, however, that such freedom is subject to restriction when necessary to protect the rights of others or for the protection of national security or public order.116 U.S. law also recognizes this principle in the Supreme Court case Brandenburg v. Ohio, which prohibits speech that “is directed to inciting or producing such imminent lawless [i.e., violent] action that is likely to incite or produce such action.”117 Similarly, international treaties have not protected “speech likely to incite violence or recruit[e] others for the incitement of violence.” 118 Defining “terrorist speech” within the confines of the Brandenburg test would severely limit the speech in question and subject to prosecution. Terrorist organizations, despite their flaws, could still peacefully advocate for their views and would only have a restriction placed on their speech when used in a manner to threaten national security and public safety through their advocacy of violent action. Through this limited restriction, disagreement and dissent can flourish while violence and participation in terrorism faces a barrier.

In addition to restricting what form of speech would trigger liability, whose speech creates liability should also be determined. National and international bodies already provide a means of determining what “terrorist” expressions should be targeted. The United States, United Kingdom, United Arab Emirates, European Union, and the United Nations all have “terrorist lists” which identify the scope and legal effect of being designated as a “terrorist organization.”119 Though these designations vary in whether they identify only groups or groups and individuals, each symbolizes the nations’ concerns—concerns which flow into the online environment with every post containing terrorist speech. Using these lists in each respective country for the identification of “terrorist speech”

116. Id.
118. See International Covenant, supra note 112 (regarding the art. 19 language on restrictions to the right to expression to protect national security or public order).
119. Statewatch Comparative Analysis of the US, UK, UN and EU “Terrorist Lists,” supra note 76; see also List of Groups Designated Terrorist Organizations by the UAE, supra note 76.
eliminates the struggles witnessed in international law for implementing a universal “terrorism” definition.120 Government entities and social media companies’ failure to create effective restrictions on their own necessitates alternatives—alternatives which change the incentives at play between terrorist organizations, social media companies, and government entities. Respecting the Covenant on Civil and Political Rights, a limited understanding of both “terrorist” and “speech” provides a clear distinction of whose and what speech social media companies should be held responsible for, striking an importance balance between national security and free expression.

2. Social Media Companies’ Failure to Act is Most Analogous to Aiding and Abetting, Making it the Best Means of Imposing Liability in Domestic Courts.

Imposing responsibility on social media companies punishes their hesitation to self-censor and the facilitation of terrorist activity which follows. Aiding and abetting provides the best conduit for implementing liability against social media companies because it focuses on the “facilitation” role their lack of self-censorship plays in the promotion of ISIS’s content. In the United States, the aiding and abetting statute reads as follows:

(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

(b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.121

Under this code section, aiding and abetting has constituted participating in an armed drug deal,122 assisting an officer of the Internal Revenue Service receive more compensation than authorized by law,123 and possessing heroin with the intent to distribute.124 Statutes such as this provide the best path for imposing liability because they recognize that, though the companies have not posted the content themselves, they bear a responsibility for their role in facilitating the recruitment for or incitement to violence called for in terrorist speech.

120. See Dershowitz, supra note 104 (discussing the struggle to create a universal definition of terrorism).
In essence, holding social media companies responsible through aiding and abetting would copy the changes made in the U.S. for the Communications Decency Act.\footnote{125} Introduced in 2017 and signed into law in April 2018, the Allow States and Victims to Fight Online Sext Trafficking Act of 2017 (FOSTA) reduces the protections in Section 230 of the Communications Decency Act.\footnote{126} Previously, Section 230 does not impose liability on intermediary websites for sex trafficking-related content posted by others; FOSTA withdraws this immunity for internet companies which permit content that facilitates sex trafficking.\footnote{127} The Senate Commerce Committee’s report on SESTA\footnote{128} cited a lawsuit alleging that the website Backpage.com facilitated sex trafficking through its online classified advertising in the “Adult Entertainment” category.\footnote{129} Plaintiffs alleged that because the website had few verification procedures and allowed workarounds, such as restricting posts containing the words “barely legal” but not “brly legal,” the website’s “rules and processes governing the content of advertisements are designed to encourage sex trafficking.”\footnote{130} The same workarounds are available through social media companies’ procedures. As mentioned previously, platforms have few, if any, real restrictions on the replication of previously-banned accounts, and artificial intelligence struggles to identify terrorist speech.\footnote{131} Because of these similarities, liability should also be imposed on social media


\footnote{128}S. REP. NO. 115-199 (2018).

\footnote{129}Doe v. Backpage.com, LLC, 817 F.3d 12, 16 (2016).

\footnote{130}Backpage.com, 817 F.3d at 16-17.

\footnote{131}See Baciu, supra note 63 (describing the limitations and potential of AI).
companies who fail to take down content after becoming aware of its existence. Connecting the idea of third-party liability provided by SESTA with the responsibility for “facilitation” imposed through aiding and abetting constructs a means of holding social media companies responsible for the terrorist speech spread through the platforms they control.


Relying on customary international law as the basis for the aiding and abetting standard provides the easiest foundation for universal acceptance and application in national jurisdictions. Customary international law reflects those routine state practices that have become so prominent and accepted within the international community as to constitute a legal obligation, such as the immunity granted ambassadors of foreign countries. The concept of aiding and abetting already holds a place in customary international law. Countries from a wide variety of legal and cultural backgrounds already accept the premise of aiding and abetting liability. In its extensive study on the principles of international customary humanitarian law, the International Committee for the Red Cross found the law included that “[n]o one may be convicted of an offence except on the basis of individual criminal responsibility,” with “individual criminal responsibility” including facilitating, aiding, or abetting the commission of a crime. A subsequent rule of customary international law finds that all parties to a conflict, whether international or domestic armed conflicts, have an obligation to respect customary international law. This legal obligation and widespread use already by many national governments provides a simply means of integrating liability into established legal systems


134. See ANIA RAMASATRY & ROBERT C. THOMPSON, COMMERCE, CRIME AND CONFLICT 13 (FAFO 2006) (surveying countries from every hemisphere and from both civil and common law legal systems).

135. HENKAERTS & LOUISE DOSWALD-BECK, supra note 133, at 372-73.

136. Id. at 495
and encouraging adoption across the global—simultaneously creating a more comprehensive barrier to terrorist speech on social media.\footnote{137}

Using customary international law entails the expansion of existing state practice to impose liability and incentivize the elimination of terrorist speech—it requires no new law or concept of responsibility. In her article, Catherine Lotrionte, former Assistant General Counsel at the CIA, calls for the international community to apply preexisting customary international law rules for war to cyberattacks.\footnote{138} This would not require a “reinvention” of current law, but rather would address how current international norms about state behavior apply to cyberspace.\footnote{139} The Fafø Institute in the Netherlands conducted a survey of sixteen countries from around the globe asking whether the countries had statutes imposing liability on corporations for being complicit in a crime.\footnote{140} Though not every country applied the laws to corporations, every country had some form of liability based on knowingly helping the commission of a crime.\footnote{141} Founded on state practice, the international community can generate a sufficiently concrete definition of aiding and abetting mimicking Lotrionte’s suggestion for cyberspace but applying to terrorist speech.\footnote{142} Applying this logic forces the international community to generate a long-term solution for the problem they have thus far only approached in a patchwork fashion.

\textbf{B. Joint Implementation Through INTERPOL’s Existing Resources and National Judicial Systems Provides the Best of International and National Systems for Combatting Terrorist Speech.}

Nations can impose liability through the international standard on social media platforms should they fail to remove terrorist speech. In a joint effort by nations and INTERPOL, platforms receive more monitoring and better enforcement for the removal of content. Working with each nations’ existing designations of terrorist organizations, INTERPOL’s intelligence and information sharing systems can implement monitoring specific to each jurisdiction’s designations, while maintaining a “bird’s eye view” for the development of international trends.\footnote{143} After the identification of

\footnotesize
\begin{itemize}
  \item 137. \textit{Id.}
  \item 138. Lotrionte, \textit{supra} note 95, at 838.
  \item 139. \textit{Id.}
  \item 140. Ramastry & Thompson, \textit{supra} note 134, at 13.
  \item 141. \textit{Id.}
  \item 142. Lotrionte, \textit{supra} note 95, at 838.
  \item 143. See Data Exchange, INTERPOL, https://www.interpol.int/INTERPOL-expertise/Data-exchange [https://perma.cc/2SLN-8EDV] (last visited
terrorist speech, INTERPOL will notify the social media companies of the content, making them aware of its presence and need for removal. Should social media companies remove the content, the system continues, and the threat posed by such speech is reduced. If they do not remove it, however, national judicial systems may step in and impose liability through the judicial systems, simultaneously providing an appeals process for any misidentification or contextual ambiguity. Dividing enforcement between national jurisdictions and INTERPOL provides for the strongest comprehensive solution to terrorist speech, while recognizing and working within jurisdictional and cultural differences.

The limited definition of “terrorist speech” in turn restricts the scope of INTERPOL’s notifications and monitoring, focusing it on the content produced by terrorist organizations of specific concern to each nation. Created in 1923, the International Criminal Police Commission, changing its name to INTERPOL in 1956, aims to support the policemen and women of its 192 member states in both domestic and international cooperative efforts. Every INTERPOL member country has a National Central Bureau linking national police forces with international efforts. As part of its work regarding terrorism, INTERPOL created two databases, MIND and FIND, to facilitate information-sharing between countries, specifically aiding states in screening people and travel documents at border crossings in order to help identify terrorists, fugitives, and lost or stolen travel documents. A similar database could facilitate the efforts to combat terrorist speech.

Providing consistent monitoring through INTERPOL increases the likelihood of terrorist speech and trends in such speech being found and removed quickly before they can take root on platforms. Utilizing INTERPOL’s existing information-sharing systems while having National Central Bureau’s focus on the specific terrorist organizations of concern to the nation allows the system to function

Oct. 27, 2018) (demonstrating Interpol’s capabilities and connection with other countries).


147. See Satariano, supra note 79 (noting the increased monitoring efforts by Twitter resulted in a reduction in ISIS-related accounts).
with the best of both international and national resources. Through the National Central Bureau’s connection to INTERPOL, monitoring is no longer an isolated activity of each state. Rather, monitoring takes place as part of a global effort to identify new terrorist trends, while each bureau’s monitoring and notification respects national sovereignty through its use of national terrorist designations.

Once the monitoring identifies terrorist speech, INTERPOL may notify social media companies or national law enforcement about its existence. INTERPOL’s system of notices provides an example of how such communication may occur. “Notices” constitute one of the main methods of international information-sharing facilitated by INTERPOL; through them, the international community may assist or is made aware of important crime-related information. These notices undergo a rigorous screening process prior to issuing, including limitations on the nature of the activities which can receive notices and screening of information through INTERPOL’s Rules on the Processing of Data which ensures sufficient substantiation of notices. Many of the hurdles this process creates for the issuance of a notice for criminals, missing persons, or similarly serious crimes, do not pose barriers for the identification of terrorist speech because of the nation’s role in designating the terrorist organizations. Should nations wish a more stringent screening of the notices sent by INTERPOL to social media companies, however, each National Central Bureau could include those procedures or national law enforcement could personally review the would-be notices prior to issuing them to companies. On the whole, such notifications would include information relevant to the social media company for identifying the problematic content and the jurisdictional requirements for removing it. Without the logistical and political barriers weighing down international law and national enforcement, INTERPOL can act faster to identify terrorist speech and sources of new threats.

Should a social media company disagree with or ignore the notification resulting from INTERPOL’s monitoring, national judicial systems may step in and prosecute. By freeing national governments from monitoring, INTERPOL allows the governments to focus more on imposing liability against social media companies should they fail


150. Id.

151. Id.
to remove content. This adds greater weight to the restrictions on content posted and allowed to remain on social media platforms.\textsuperscript{152} National jurisdictions may now redirect efforts toward prosecutions and the enforcement of criminal punishments against social media companies, directly counteracting their commercial incentives.

Liability for aiding and abetting supplies the impetus to influence social media companies towards more self-censorship should the social media companies ignore INTERPOL notices. Once national jurisdictions determine that the social media companies have aided and abetted terrorist activity by knowingly permitting terrorist speech to remain on the platform, criminal or civil penalties can be sought against the company. In the United States, violations for aiding and abetting receive the same punishment as if the actor had committed the crime themselves.\textsuperscript{153} Given the nature of the violation—being speech inciting violence and not violence itself—there is room for courts to impose monetary fines or alternative sanctions against the companies. Regardless of the exact punishment sought, however, criminal liability prevents physical harm sooner than civil liability alone, as cases do not require the manifestation of physical harm prior to liability.\textsuperscript{154} The civil lawsuits filed against social media companies by terror victims’ families all came after people died due to terrorist attacks.\textsuperscript{155} Pursing criminal liability for terrorist speech allows the government to identify the harm not as a completed terrorist act, but as the recruitment for or the potential for inciting one—thus taking action aimed at stopping the violence before it begins.

Additionally, social media companies should not be threatened by the use of government enforcement. Citizens have regularly turned to their governments to address national security concerns. And in an effort to promote the safety and security of the nation, governments have found some rights are not unlimited. For example, U.S. corporations do not have an unrestricted right to be bought. Rather, the Committee on Foreign Investment in the U.S. reviews mergers, acquisitions, and other corporate transactions to ensure that they do not threaten national security.\textsuperscript{156} This proposal simply reflects the

\textsuperscript{152} See Patrikarakos, supra note 9 (citing tech companies’ reluctance to remove certain content unless there is a business incentive).


\textsuperscript{154} Id.

\textsuperscript{155} See, e.g., Messika, supra note 109 (noting the filing of civil claims against social media companies for the companies’ involvement in terrorist attacks after the attacks had been carried out); see also Machado, supra note 103 (same).

\textsuperscript{156} U.S. DEPT. OF TREASURY, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS), (2019), https://home.treasury.gov/policy-
national security concerns arising from the narrowly-defined speech at issue. Likewise, this limited definition fits better within the accepted understanding, at least in the U.S. of protected First Amendment rights. Critics of FOSTA suggest that the elimination of the safe harbor in reality makes the world more dangerous, driving sex workers underground and inadvertently supporting only those large companies which can afford the staff necessary to monitor the website. In comparison, this proposal rests on an established understanding of prohibited speech and actions, and does not require any additional monitoring by social media companies due to the notice they would receive. Only those companies which choose to fight the notification would have to. At the same time however, those concerned with abuse by government officials could take comfort in the procedural safeguards both in the required notice and the judicial system. The unclassified nature of the notices, while this is not a guarantee against abuse, does provide a public record should the government overstep.

The outlined approach would simultaneously reinforce a preventative focus, while incentivizing social media companies to self-regulate and monitor for terrorist activity. Holding social media companies liable for aiding and abetting introduces the incentives necessary for the companies to embrace more self-censorship. Responsibility reduces the commercial incentives that undermine the creation and enforcement of the content restrictions necessary to effectively prevent the spread of terrorist speech. Inherently, social media companies are profit-making endeavors. Facebook alone made $8.03 billion from sales in the first quarter of 2017, averaging about $4.23 in sales from each user. Part of the appeal of these platforms, and in turn what makes them popular enough to make such profits, is


158. Patrikarakos, supra note 9.


160. Id.
their perceived role as an open forum for society.\textsuperscript{161} Imposing criminal liability through monetary fines, for example, counters the financial benefits causing social media companies’ hesitancy to self-censor. Now, rather than viewing each new user just as an additional $4.23 of revenue, each user also poses a risk and liability that the company must be willing to take on. Free speech can remain a corporate principle for the companies because the limited definition of “terrorist speech” requires only the restriction of speech likely to incite violence or recruit for violent activities.\textsuperscript{162} Criminal liability permits social media companies to continue to pursue profits but imposes a sanction should they fail to comply and ignore terrorist speech.

IV. HOLDING SOCIAL MEDIA COMPANIES RESPONSIBLE ADDRESSES THE RESIDUAL CONCERNS RELATED TO FREE EXPRESSION AND NATIONAL SOVEREIGNTY.

This proposal resolves the ideological and logistical implementation problems facing current responses to ISIS’s terrorist speech, but also the more fundamental considerations made when determining how to respond in the first place. Each response chosen by a company or government reflects a decision about what values—whether freedom of expression or national security—the decision maker prioritizes. Similarly, when looking at the implementation of any new program, particularly one influenced by international law, nations will likely hesitate to give up sovereignty on such an important issue. The implementation of an aiding and abetting standard through a mixture of international and national systems, however, copes with these challenges by recognizing each state’s different security in the course of pursuing global security.

A. The Limited Scope of Liability Respects Free Expression While Securing a Means of Increasing National and Global Security.

States and companies make decisions about what they should prioritize every single day. When it comes to social media and


\textsuperscript{162} Defining “terrorist speech” as “speech likely to incite violence or recruiting others for the incitement of violence” does not implicate the free expression of opinions or other information protected under the Covenant for Civil and Political Rights. See International Covenant, supra note 112.
terrorism, these decisions often hinge on how much the decision makers value the freedom of speech in comparison to national security. Facebook’s Vice President of Global Public Policy, Marne Levine, addressed the balance Facebook sought to strike between these two concerns stating:

We work hard to remove hate speech [which often includes incitement] quickly, however there are instances of offensive content, including distasteful humor, that are not hate speech according to our definition. In these cases, we work to apply fair, thoughtful, and scalable policies. This approach allows us to continue defending the principles of freedom of self-expression on which Facebook is founded.”

Germany sought to strike a different balance. With the passage of the “Facebook law,” German lawmakers wanted to impose fines on social media platforms which fail to remove hate speech and content inciting violence. Digital rights and free speech activists opposed the measure, arguing the regulation overly-restricted social media platforms. Justifying the restriction, German Justice Minister Heiko Maas stated, “[T]he ability to bring big consequences for companies [is] necessary in combating hate speech and radicalized content online.” The tension between free speech and security raises a question which goes to the heart of how best to respond to terrorist speech, but also highlights the different values held by each state and company. By using the international resources of INTERPOL, but limiting them to the national terrorist lists and specific types of speech, states gain control over the process. This enables the state to target only the specific groups they believe sufficiently threaten their national security to justify a limitation on free speech.

165. Burns, supra note 94.
166. Id.
167. Id.
168. See, e.g., Burns, supra note 94.
B. States Maintain Control Over The System, Protecting Their Sovereignty, Through the Integration of State Terrorist Designations and Judicial Systems.

At any time during this process, nations can choose to completely opt out of the system by blocking social media companies or choosing not to prosecute. Since China gained access to the internet, the government has censored access to certain websites. With over 700 million internet users—equating to 1 in every 4 of the internet’s population—China leads the world in e-commerce and online activity. The security of the government, however, depends on its ability to block those websites that disrupt the Communist Party’s narrative, while permitting the growing technological and commercial benefits the internet facilitates. States dissatisfied with the joint enforcement plan always have the option to completely block social media companies like China has done. Alternatively, states could choose not to pursue prosecutions against the companies, thereby permitting unrestricted free expression on the platforms. Hopefully, states would not choose either option. They always have, however, a means of protecting their national sovereignty should they believe the concerns outweigh the benefits.

Additionally, utilizing existing INTERPOL resources has little impact on current efforts by governments or social media companies to stop terrorist speech. At a minimum, including INTERPOL adds a beneficial resource rather than a challenge to sovereignty or a draw on resources. Little, if anything, about this proposal forces social media companies or national governments to change what they already do. Governments may specify that the content only be taken down after recording all usable information to trace the producers or after storing the content for counter-propaganda purposes. While including INTERPOL in the discussion and imposing liability would change the incentives motivating both social media companies and aid in allocating national resources towards prosecutions, a state does not have to prioritize the resources if it chooses not to.


171. Id.
V. Conclusion

Lacking the traditional trappings of state and country, non-state actors have and are forcing the national security community to rethink their responses. Following 9/11, the U.S. recognized the need for international cooperation and collaboration in preventing future failures in immigration, like those that permitted the 9/11 hijackers to enter the country. A similar solution is necessary to effectively address terrorist speech on social media—a solution found in an international aiding and abetting standard. By relying on customary international law for the standard and using a combination of INTERPOL and national governments for implementation, governments can effectively reduce the threat posed by terrorist content inciting or recruiting for violence. Through national governments’ existing terrorist designations and the increased monitoring by INTERPOL the political concerns in identifying “terrorist speech” and the quantity of terrorist speech are reduced. Subsequent removal or failure to remove such speech by the social media companies then becomes an issue remedied through established court systems. Uniting the strengths of international law with the resources available in national jurisdictions resolves the need for a comprehensive approach while simultaneously recognizing and respecting differences nations may have regarding what constitutes terrorism.

Nations should acknowledge the role social media companies have come to play in society, as well as the companies’ stake in stopping terrorism. When social media companies fail to remove known terrorist speech, their inaction facilitates violence. Free speech and freedom from unnecessary government interference must be balanced against security simultaneously sought from the government. In seeking to reduce or eliminate the corruption of free speech by non-state actors’ liability for those companies maintaining access to the speech should be considered.