ARTICLE

Social Media Compliance Programs and the War Against Terrorism

Susan Klein[·] and Crystal Flinn[†]

[·] Alice McKean Young Regents Chair in Law at the University of Texas at Austin School of Law. Professor Klein can be reached at sklein@law.utexas.edu.
[†] J.D., UT School of Law, 2016. Ms. Flinn is currently Legal Counsel for Shell Oil Company.

The authors would like to thank Norman Abrams, Philip Bobbitt, Robert Chesney, Orin S. Kerr, Jennifer Laurin, Daniel Richman, and Stephen Vladeck for reading early drafts of this Article. They also appreciate the research assistance of UT law students Sara Catherine Clark, Abdulmomin R. Ghuman, Michael P. Heitz, and Brittany L. Siscoe. Finally, they benefitted from the excellent research services of UT School of Law librarian Matthew R. Steinke and UT assistant Nicholas D. Charlesworth.

Abstract

Widespread Internet use by terrorists had made the prevention of terror attacks increasingly difficult. This Article argues that social media companies, like other corporate entities, should be legally required to institute compliance programs that ferret out and report terrorist activity at the earliest possible opportunity. To this end, the Article proposes text for new legislation that would criminalize social media companies' failure to discover and release terrorism-related posts to the government. The authors alternatively suggest borrowing from the white-collar crime arena to secure company assistance in government investigations by granting leniency at sentencing to offending companies. The Article concludes by addressing anticipated constitutional arguments and opposition to the proposed legislative framework.

Table of Contents

Introduction

According to press reports in December 2015, terrorist Tashfeen Malik posted her allegiance to the Islamic State of Iraq and al Sham (ISIS) on her Facebook account before killing fourteen innocent civilians at the County Health Department in San Bernardino, California.[1] Though Facebook had removed her account as violative of internal company rules, the company did not immediately alert the government to the existence of the post—or the possibility of an attack.[2] In a more recent example, gunman Omar Mateen checked his own Facebook posts and other social media accounts to verify that his pledge to Abu Bakr al-Baghdadi, the leader of ISIS, had been properly publicized during the five-hour standoff in the Orlando bar where he killed 49 people on June 19, 2016.[3]

We suggest in this Article that social media companies,[4] like other corporate entities, should be legally required to institute compliance programs that discover and report terrorist activity at the earliest possible opportunity. Most of these companies, such as Facebook, Twitter, YouTube, and Instagram, already have in place internal rules against messages that might violate the federal prohibition against material support to terrorists or to a Foreign Terrorist Organization (FTO).[5] Additionally, many of these companies already have both a

---

[1] Michael S. Schmidt and Richard Perez-Pena, *F.B.I. Is Treating Rampage as Act of Terrorism*, N.Y. TIMES (Dec. 4, 2015), http://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html (reporting that the Federal Bureau of Investigation (FBI) assistant director in charge of the Los Angeles office admitted he was aware of the post, which was taken down by Facebook).

[2] However, the FBI had uncovered evidence that Ms. Malik's husband and co-shooter, Syed Rizwan Farook, had "contact" with five separate extremists, domestically and abroad, a few years prior to the shootings. Christine Hauser, *San Bernardino Shooting: The Investigation So Far*, N.Y. TIMES (Dec. 4, 2015), http://www.nytimes.com/2015/12/05/us/san-bernardino-shooting-the-investigation-so-far.html. To the extent those communications occurred on social media, they too would be covered by our proposals.

[3] Eric Tucker and Mike Schneider, *911 transcript: Orlando gunman said he was Islamic soldier*, ASSOCIATED PRESS (June 20, 2016), http://bigstory.ap.org/article/196c91013aa1461a91efb0abf1774933/fbi-releasing-conversations-between-gunman-and-police.

[4] We would include in this group Internet service providers (ISP), mobile application companies, humanitarian aid groups, and others similarly situated. We only include entities that serve as vehicles to post messages in a group setting. We do not include service providers of e-mails or telephone service companies where most communications are between two individuals only. Thus, we express no opinion on Apple's refusal to help the FBI obtain the user-generated passcode of the San Bernardino shooters' iPhone, despite a federal judicial order requiring it. We note that Fourth Amendment issues surrounding encryption of personal communications are quite different from privacy issues in social media settings, where third parties are invited to view the messages and thus the reasonable expectation of privacy is lost.

[5] The federal statutes, originally enacted in 1994 and 1996, now include 18 U.S.C. § 2339 (2002) (harboring or concealing terrorists); 18 U.S.C. § 2339A (2009) (providing material support to terrorists); 18 U.S.C.A. 2339B (2015) (providing material support or resources to designated foreign terrorist organizations (FTO)); 18 U.S.C. § 2339C (2006) (prohibitions against the financing of terrorists); and 18 U.S.C. § 2339D (2004) (receiving military-type training from a FTO). The statutes were amended in 2002 to clarify the *mens rea* requirement and to define "material support" in a manner consistent with the First Amendment.

method of internal reporting by other users against rule-breakers and computer programs that seek out key words to alert company monitors that a breach of internal rules might be occurring.[6] Companies without policies, such as Dropbox and LinkedIn, lesser-known and newer sites, such as Tumblr and Soundcloud, and even nonprofit organizations, such as Internet Archive in San Francisco, should be forced to follow suit. We suggest two supplementary federal proposals.

The first would create a new substantive offense by criminalizing the failure of social media companies to institute programs that discover terrorism-related posts by their users and to immediately release such posts to the government. A social media company would be guilty of this new crime if it knowingly, recklessly, or negligently failed to institute a government-approved compliance program and report any suspicious results it discovered through its program to federal authorities. This proposal is limited to public wall-postings and similar shared content; it excludes e-mails or other private communications solely between two individuals.[7] We realize that this proposal is strong medicine.[8] However, we believe that the danger of online terror activity warrants such a vigorous federal response. This proposal does not replicate the Online Terrorism Activity Act recently proposed by Senator Dianne Feinstein,[9] though we agree that her bill ought to be enacted. We are not suggesting merely that the social media companies be required to report known terrorist activity to federal law enforcement agents. Rather, we would require such companies to develop programs that would monitor users for compliance with 18 U.S.C. §§ 2339 to 2339D and other terrorism offenses on pain of criminal liability, and report all offending posts to law enforcement officials. And rather than automatically

---

In both examples given by Senator Feinstein in support of her anti-terrorism legislation, discussed *infra* note 9, the social media companies had already shut down the particular sites used to provide material support. Twitter had shut down multiple accounts of Syrian based terrorist Junaid Hussain and Facebook had removed the account of Tashfeen Malik. Office of Senator Dianne Feinstein, *Bill Would Require Tech Companies to Report Online Terrorist Activity* (Dec. 8, 2015), http://www.feinstein.senate.gov/public/index.cfm/2-15/12/ill-would-require-tech-companies-to-report-terrorist-activity.

[6] Such programs may use key words in particular groupings, such as "jihad," "ISIS," and "weapons," or they may uncover violative messages by tracing location or interaction with other online posters who have already violated such rules.

[7] We recognize that the line between shared and private content will not always be clear. We anticipate that any group with more than two members is no longer private. For example, if I create a Facebook group with five members and only they can view the content, that is considered a public wall posting, and not a private communication, so it would be covered by our first proposal.

[8] While more radical than Senator Feinstein's proposal, our proposal is tame compared with Professor Posner's idea. He would make it a crime to access websites that "glorify, express support for, or provide encouragement for ISIS." Eric Posner, *ISIS Gives Us No Choice But to Consider Limits on Speech*, SLATE (Dec. 15, 2015), http://www.slate.com/articles/news_and_politics/view_from_chicago/2015/12/isis_s_online_radicalization_efforts_present_an_unprecedented_danger.html.

[9] The bill was read twice and referred to the Committee on the Judiciary, and there has been no further action on it. Requiring Reporting of Online Terrorist Activity Act, S. 2372, 114th Cong. (2015) (as proposed by Senate Intelligence Committee Vice-Chairman Dianne Feinstein (D-Calif.) and Chairman Richard Burr (R-N.C.) on December 8, 2015).

shutting down such accounts when they are discovered, which may have adverse and unintended consequences, we would shift this decision to the Federal Bureau of Investigation (FBI) experts best suited to make them. In some cases, it might serve intelligence needs to allow the postings to continue. Moving the loci of such decision-making from private companies to the government might also allow innocent and aggrieved users to pursue avenues of redress.

The second proposal is a fallback in the event that Congress does not enact our first proposal. We recognize that Internet companies would strenuously oppose our first proposal, and that they have tremendous power on Capitol Hill. This second proposal would grant those social media companies that instituted the anti-terror compliance programs suggested in proposal number one leniency at sentencing should they be held criminally liable under the federal doctrine of *respondeat superior* for the material support crimes of their agents.[10] Perhaps more importantly, prosecutors would consider the existence and effectiveness of such a program in their charging decisions against the social media companies. The federal government does this already with corporate sentencing, primarily in the white-collar crime arena, to assist the government in discovering who within the corporation committed the federal criminal offense, and to prevent its recurrence.[11] The Federal Sentencing Guidelines grant corporations large sentencing discounts if they had instituted a corporate compliance program prior to the commission of the offense by their agent.[12] This strategy will likely not be nearly as effective as would our first proposal as a tool against terrorism, as federal prosecutors have not yet attempted to charge social media companies for the crimes committed or assisted by their agents. Such a strategy works best when the corporation faces a high likelihood of criminal liability, with its attendant high

---

[10] For example, if an executive, computer programmer, or any other agent employed by Facebook knew that client Tashfeen Malik has posted her allegiance to ISIS on her account, and this employee knew that ISIS is a FTO and wishes to help ISIS gain new members, such employee might be guilty of violating 18 U.S.C.A. §2339B (2015), which criminalizes knowingly providing material support to a FTO. Her guilt may be direct, or may rest on her assistance to the poster, 18 U.S.C. § 2, because she had the opportunity and responsibility to remove the post and failed to do so. Facebook itself might also be liable for this crime committed by its employee if the employee discovered the post within the scope of her duties (as is quite likely) and the government can prove that the programmer acted, in part, with intent to benefit Facebook (if she knows, for example, that the company makes money in part based upon on the number of posts it can claim per month, or on selling advertising).

[11] *See* U.S. DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL § 9-28.000, Principles of Federal Prosecution of Business Organizations (Aug. 28, 2008), https://www.justice.gov/usam/usam-9-28000-principles-federal-prosecution-business-organizations#9-28.900 (providing that prosecutors consider "the corporation's timely and voluntary disclosure of wrongdoing, and its willingness to cooperate in the investigation of its agents" as well as the "adequacy of pre-existing compliance programs" in deciding whether to prosecute a corporation); Letter from Sally Quillian Yates, Deputy Assistant Att'y Gen., U.S. Dep't of Justice (Sept. 9, 2015) (announcing that the DOJ should "fully leverage its resources to identify culpable individuals at all levels in corporate cases" because this is one of the "most effective" ways to fight corporate crimes).

[12] U.S. SENTENCING GUIDELINES MANUAL § 8C2.5(f)(3)(B) (2004) (determining culpability score in part by whether the organization had an "effective compliance and ethics program").

dollar fines for violations. Unless federal prosecutors take the lead from private plaintiffs now suing under 18 U.S.C. § 2333(a)[13] and step up prosecutions of social media companies in situations where their Internet services are used in terrorist-related posts, social media companies may not consider themselves sufficiently exposed to bother with the expense of such programs. However, because it will be less effective at criminalizing the behavior of social media companies, and because it does not as directly or as frequently impinge on the privacy rights of social media users, this proposal might be more politically palatable. It applies to a social media company only after there is probable cause to believe it has committed a serious federal felony, and it does not require the company to reveal offending user posts to the government until after the company has been charged.

In Part I of this Article, we review the development of terror activity in today's globalized environment, including the high rate of reliance on the Internet and mobile applications. In describing the well-known danger of terrorism, we focus on "lone-wolf" terrorists and the difficulty of finding such individuals and stopping them before they attack. The Internet has made this problem all but impossible to solve, and therefore companies that make their fortunes utilizing the Internet must become part of the solution. A Brookings Institute report estimates that between 46,000 and 70,000 Twitter accounts were used by ISIS supporters from September 2014 to December 2014,[14] and a George Washington University study counted approximately 300 Americans and/or U.S.-based ISIS sympathizers active on social media.[15]

In Part II, we respond to perceived insufficiencies in existing legislation and recent legislative proposals. We will also set forth proposals to address the liabilities of companies to enable the governmental review and discretion of potential terror activity online. In addition to both of our proposals, we also offer precedents for such governmental action, including the Federal Sentencing Guidelines pertaining to organizations,[16] the Bank Secrecy Act,[17] and international bodies in the enforcement of copyright law.[18] Once compared to

---

[13] *See, e.g.*, Complaint, Gonzalez v. Twitter, Inc., Google Inc., and Facebook, Inc., No. 4:16-cv-03282-DMR (N.D. Cal. filed June 14, 2016).

[14] J.M. Berger and Jonathan Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, THE BROOKINGS PROJECT ON U.S. RELATIONS WITH THE ISLAMIC WORLD (Mar. 2015), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

[15] Lorenzo Viddino and Seamus Hughes, *ISIS in America: From Retweets to Raqqa*, GEORGE WASHINGTON UNIVERSITY PROGRAM ON EXTREMISM (Dec. 2015), https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report_0.pdf.

[16] U.S. SENTENCING GUIDELINES MANUAL § 8 (2004).

[17] Bank Secrecy Act of 1970 31 U.S.C. § 5311–22 (requiring financial institutions to report case transactions over $10,000 to government officials); *see also* USA PATRIOT Improvement and Reauthorization Act of 2005, 18 U.S.C. 1801 §§ 401–10 (strengthening banks' reporting requirements through "know your customer" regulations).

[18] Digital Millennium Copyright Act, Pub. L. No. 105-304, 17 U.S.C.A. §§ 512, 1201–05, 1301–32 (1998); *see also* 28 U.S.C.A. § 4001 (1998).

these other criminal and regulatory measures, our proposals are not as unconventional as they might first appear.

In Part III, we respond to both historical and anticipated opposition, grounded in constitutional arguments, to the proposed legislative framework in Part II. We believe that neither proposal would violate the First Amendment's protection of speech and association or the Fourth Amendment's protection against unreasonable searches and seizures. We cannot deny the concerns of civil libertarians that when firms monitor posts for content, at the behest of the government, there might be some chilling of speech that is not illegal under the material support analysis. However, the Court's relatively recent 6-3 opinion in *Holder v. Humanitarian Law Project*,[19] upholding the material support statute against a First Amendment freedom of speech and freedom of association challenge and a Fifth Amendment Due Process Clause vagueness challenge, lends significant support to the validity of our proposals. A long line of precedent confirms that the Fourth Amendment offers no reasonable expectation of privacy in communications voluntarily revealed to third parties.[20] Were either of our proposals to extend to e-mails intended to remain private between two individuals, the issue becomes a much closer one.

I. Malignant Misuse of Global Communications

The benefits of globalized communication are not sequestered from criminal enterprise. Terror groups have been quick to accept the assistance of ubiquitous communications technology, thereby opening the pathways for terrorists to easily access people around the globe. However, attempts by intelligence agencies to harness these global communications benefits, such as through data mining and monitoring of communications, has been met with significant public resistance. For example, the federal government's legal monitoring scheme was roundly criticized by news media and the public in 2013 after Edward Snowden revealed the government's counterterrorism methods.[21] A statutory framework allowing our government to monitor criminal use of globalized communication is critically necessary, both for the legitimacy of such monitoring and the practicality of preempting terror attacks.

---

[19] 561 U.S. 1 (2010).

[20] *See, e.g.*, United States v. White, 401 U.S. 745 (1971) (holding that the Fourth Amendment did not bar from evidence testimony of government agents who overheard and taped a conversation through electronic monitoring of a government informant); United States v. Miller, 425 U.S. 435 (1976) (finding no reasonable expectation of privacy in bank records stored by third parties); Smith v. Maryland, 442 U.S. 735 (1979) (holding that defendant had no reasonable expectation of privacy in the telephone numbers he dials).

[21] *See* George Gao, *What Americans think about NSA Surveillance, National Security and Privacy*, PEW RESEARCH CTR. (May 29, 2015), http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/ (estimating that although more Americans say anti-terrorism policy is a bigger concern than policy going too far in restricting the average person's civil liberties, Americans "briefly held the opposite view in July 2013, shortly after the Snowden leaks").

A. *The Reshaping of Criminal Enterprises in a Global Environment*

Contemporary globalization has brought a host of benefits for states opting into globalization policies, such as increased wealth, technological developments, and sociopolitical alliances.[22] However, globalization also brings a dark side: more permeable state borders, which greatly increase the threat of violent groups committing widespread attacks and globalizing their aims in a parallel fashion.[23] The globalization of terror threats is widely acknowledged[24] and dramatically punctuated by the mass killings in several attacks in the United States from the past decade, such as the 2001 attacks on the World Trade Center,[25] the 2009 Fort Hood shooting,[26] the 2015 Garland, Texas copycat of the Charlie Hebdo attack,[27] and the 2015 San Bernardino shooting.[28] And, of course, the terror activities outside our borders are too numerous to list.[29]

What is not widely acknowledged is the significance of government efforts to prevent more frequent and more devastating terror attacks.[30] Despite an overall reduction in the probability of an attack similar to the 2001 World Trade Center attack, the National Counterterrorism Center notes that "the array of extremist terrorist actors around the globe is broader, wider, and deeper than it has

---

[22] *See* T.V. PAUL AND NORRIN RIPSMAN, GLOBALIZATION AND THE NATIONAL SECURITY STATE 5–8 (2010) (describing definitions of economic, political, social, and cultural globalization and some of the international benefits and changes as a result of the globalization process).

[23] *See id.* at 23 ("As modern technology has made national borders porous, the state cannot effectively prevent hostile groups from entering national territory and harming its citizens.").

[24] *See, e.g.*, ROBERT LEACH, THE POLITICS COMPANION 131 (2008) ("Global terrorism is the latest manifestation of the globalization of politics.").

[25] Douglas Kellner, *Globalization, Terrorism, and Democracy: 9/11 and its Aftermath*, FRONTIERS OF GLOBALIZATION RESEARCH 243, 245 (2007) (showing "the ways that globalization and a networked society were involved in the 9/11 events").

[26] RONALD A. MARKS, SPYING IN AMERICA IN THE POST 9/11 WORLD: DOMESTIC THREAT AND THE NEED FOR CHANGE 42 (2010) (stating that Major Hasan, who was radicalized "by way of communicating online" and committed the 2009 Fort Hood shooting, which injured 28 and killed 13, demonstrates "that significant threats materialize not only abroad in weak and failed states but also right here at home").

[27] *See infra* note 33.

[28] Matt Apuzzo, Michael S. Schmidt, and Julia Preston, *U.S. Visa Process Missed San Bernardino Wife's Online Zealotry*, N.Y. TIMES (Dec. 12, 2015), http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html? (describing online jihadist support of the San Bernardino terrorist's wife, discovered too late to prevent the killing of fourteen U.S. civilians).

[29] *See*, *e.g.*, Karen Yourish, Derek Watkins, Tom Giratikanon, and Jasmine C. Lee, *How Many People Have Been Killed in ISIS Attacks Around the World*, N.Y. TIMES (July 16, 2016), http://www.nytimes.com/interactive/2016/03/25/world/map-isis-attacks-around-the-world-DE.html (reporting on national and international terror incidents such as the Brussels airport bombings in 2016, the Paris attacks in 2016, and the cafe attack in Australia in 2014).

[30] *Current Terrorist Threat to the United States: Hearing Before the Senate Select Comm. on Intelligence*, 114th Cong. (2015) (statement of Nicholas J. Rasmussen, Dir., Nat'l Counterterrorism Center) ("The growing number of individuals going abroad as foreign terrorist fighters to Iraq and Syria only emphasizes the importance of prevention. Any hope of enduring security against terrorism or defeating organizations like ISI[S] rests in our ability to diminish the appeal of terrorism and dissuade individuals from joining them in the first place").

been at any time since 9/11, and the threat landscape is less predictable."[31] The studies indicate that terrorism remains a prevalent threat: worldwide in 2011, there were more than 10,000 terrorist attacks, resulting in 12,500 deaths.[32] Similarly, the changing nature of the threat of terror by activity on the Internet has been overlooked all too often.[33] In 2015, there were more instances of terrorism in the United States involving domestic perpetrators recruited online than in any year since 2001.[34] Furthermore, ISIS currently faces the loss of physical territory in Iraq and Syria.[35] Counterterrorism officials warn that this loss of physical territory could result in two highly negative outcomes: (1) the return of ISIS members to home countries in Europe, leading to increased attacks in the fighters' home countries; and (2) an increase in its efforts to ensure virtual (if not physical) cohesion through social media.[36]

This increase in terror activity can be attributed, at least in part, to the proliferation of international communications facilities and to the use of these facilities by terror groups.[37] While "lone-wolf terrorism" is an especially dangerous threat due to the unpredictability of these actors,[38] online platforms reveal that "lone wolves" are not truly alone, but rather connected on the Internet to a "virtual pack."[39] The danger posed by the widespread Internet use of terror

---

[31] *Worldwide Threats and Homeland Sec. Challenges: Hearing Before the H. Comm. on Homeland Sec.*, 114th Cong. (2015) (statement of Nick Rasmussen, Dir., Nat'l Counterterrorism Center).

[32] THE NAT'L COUNTERTERRORISM CTR., 2011 REPORT ON TERRORISM 9 (2012) (indicating that "over 10,000 terrorist attacks occurred in 2011 . . . resulting in over 12,500 deaths" and that these numbers "underscore the human toll and geographic reach of terrorism").

[33] *Terrorism Gone Viral: The Attack in Garland, Texas, and Beyond: Hearing Before the H. Homeland Sec. Comm.*, 114th Cong. (2015) (statement of John Mulligan, Deputy Director, Nat'l Counterterrorism Center) (discussing how the Garland, Texas terrorist attack, in which attackers opened fire on an event with semi-automatic rifles, exemplifies the threat of homegrown extremists and "highlights the growing threat our nation faces from a new generation of terrorists who find like-minded associates on the internet and social media to share their violent extremist ideology").

[34] *Worldwide Threats and Homeland Sec. Challenges: Hearing Before the H. Homeland Sec. Comm.*, 114th Cong. (2015) (statement of Chairman Michael McCaul, House of Representatives) ("ISIS alone has inspired or directed 17 terrorist plots in America since early 2014, and overall the group has been linked to more than 60 plots against Western targets . . . [t]his pace of terror plotting is unprecedented/unrivaled even by al Qaeda at its peak.").

[35] Eric Schmitt, *Caliphate in Peril, More ISIS Fighters May Take Mayhem to Europe*, N.Y. TIMES (Sept. 17, 2016), http://www.nytimes.com/2016/09/18/us/politics/caliphate-in-peril-more-isis-fighters-may-take-mayhem-to-europe.html/.

[36] *Id.*

[37] THE UNITED NATIONS OFFICE ON DRUGS AND CRIME, THE USE OF THE INTERNET FOR TERRORIST PURPOSES 3 (2012) (discussing the benefits of enhanced communications technology, which "can also be exploited for the purposes of terrorism").

[38] *See, e.g.*, *Current Terrorist Threat to the United States: Hearing Before the S. Select Comm. on Intelligence*, 114th Cong. (2015) (statement of Nicholas J. Rasmussen, Dir., Nat'l Counterterrorism Center) [hereinafter *Rasmussen Statement*] ("We face a much greater recurring threat from lone offenders and possibly loose networks of individuals."). *See generally* JEFFREY D. SIMON, LONE WOLF TERRORISM: UNDERSTANDING THE GROWING THREAT (1st ed. 2013).

[39] Gabriel Weimann, *There's no such thing as lone wolf in cyberspace*, REUTERS BLOG (June 25, 2015), http://blogs.reuters.com/great-debate/2015/06/25/theres-no-such-thing-as-a-lone-wolf-in-

groups is a growing concern. A decade-long study published in 2012 revealed that "90 per cent of organized terrorism on the internet is being carried out through social media."[40] Reports about the widespread use of the Internet, and especially of social media, by terrorist groups begin to demonstrate the scale of the problem.[41] Extensive Internet use by terrorists makes the prevention of terror attacks increasingly difficult.[42] These terrorists "make use of a diverse online environment that is dynamic, evolving, and self-sustaining," and they are difficult to identify and detect before they carry out attacks "because they often exhibit few behaviors that law enforcement and intelligence officers traditionally used to detect a readiness to commit violence."[43] Furthermore, the use of the Internet in facilitating criminal activity is not limited to terror organizations; social media is also a recruiting tool for domestic gangs.[44] Internet usage as a tool for criminal enterprise is not going away, either in the United States or abroad.

Thankfully, the unpredictability of these actors can be mitigated by counterterrorism activity designed to track, intercept, and strategically disable these communications.[45] The primary obstacle appears to be public relations—Americans love their social media platforms. Notably, police data mining of domestic gang-related activity[46] does not receive the same amount of media attention and criticism that confronts police sifting through terror-related social media activity, though it does get its share.[47] In addition, various private data

---

cyberspace/ (referring to "lone wolf" terrorists as having a "virtual pack" online, in which "solo terrorists are often recruited, radicalized, trained and directed by others online," and asserting that the "current wave of lone-wolf attacks has been propelled by websites and online platforms that provide limitless opportunities for individuals to explore and locate their virtual pack").

[40] *Terrorist groups recruiting through social media*, CBC NEWS (Jan. 10, 2012), http://www.cbc.ca/news/technology/terrorist-groups-recruiting-through-social-media-1.1131053.

[41] J.M. Berger and Jonathan Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, THE BROOKINGS PROJECT ON U.S. RELATIONS WITH THE ISLAMIC WORLD (Mar. 2015), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf (estimating that between 46,000 and 70,000 Twitter accounts were being used by ISIS from only September to December of 2014).

[42] Eben Kaplan, *Terrorists and the Internet*, COUNCIL ON FOREIGN RELATIONS (Jan. 8, 2009), http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005 (describing several advantages to terrorist groups using the Internet, including "stealth," "sophisticated encryption tools," "a global pool of potential recruits and donors," "spreading ideology," and "creative techniques that make the Internet an efficient and relatively secure means of correspondence").

[43] *See Rasmussen Statement*, *supra* note 38.

[44] *See generally* David C. Pyrooz, Scott H. Decker & Richard K. Moule, Jr., *Criminal and Routine Activities in Online Settings: Gangs, Offenders, and the Internet*, 32 JUST. Q. 471 (2015).

[45] *See* Weimann, *supra* note 39 (asserting that "virtual packs can be monitored and studied," and suggesting a "countermeasure to locate potential lone-wolf attackers . . . with online undercover agents and informants").

[46] *See, e.g.*, Brian Kuebler, *Law Enforcement Monitors Gangs' Social Media Movements*, ABC2 NEWS (Oct. 17, 2013), http://www.abc2news.com/news/local-news/investigations/law-enforcement-monitors-gangs-social-media-movements.

[47] The disparity in treatment of data mining involving gang activity and social media platforms involving terrorism remains, despite the differences in the nature of the search. For example, the publicly announced opposition from Apple following a judicial order to the company to help the

sharing arrangements, such as the collection of blood and tissue for medical testing and scientific research,[48] the sale of university student information to the highest bidder,[49] and the collection and publication of photographs by mapping companies[50] have survived legal challenge even though they do not address anything as weighty as the government's obligation to prevent terrorist attack on our soil. These private actions are not generating the same public outcry as government use of available technology for terror prevention purposes.[51]

B. *Proliferation of Terror Facilitation on Social Media*

Terror strategies relying on globalized communication networks are nearly as creative and quick to develop as the variety of means of communications available. As a result, "foreign terrorist organizations now have direct access into the United States like never before."[52] These terror communications strategies can be roughly grouped by the use to which each service is put[53]: (1) targeting and

---

FBI unlock the iPhone of one of the San Bernardino attackers reveals the divide in public opinion regarding data privacy and law enforcement investigations. Eric Lichtblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, N.Y. TIMES (Feb. 16, 2016), http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html. While the increased use of social media by police to monitor gang activity has received First Amendment criticism, this issue is definitely less prominent than First Amendment criticism of searches for terrorism, as in the FBI-Apple dispute or the NSA searches. For scholarship outlining the debate on police monitoring of social media for gang activity, *see, e.g.*, Vinh Hua, *Law Enforcement's Growing Use of Social Media to Target Gang Activity*, FORDHAM URB. L.J. ONLINE (Nov. 11, 2015), http://urbanlawjournal.com/social-media-and-anti-gang-law-enforcement.

[48] *See* Arielle Duhaime-Ross, *Scientists want to do research on your tissues without asking you first*, VERGE (Jan. 5, 2016), http://www.theverge.com/2016/1/5/10718832/consent-biospecimen-human-research-samples-us-scientists ("Currently, scientists are allowed to use leftover tissues from blood tests, surgeries, and biopsies for research without patients' permission if the patient's identity is removed.").

[49] *See* Jonathan D. Glater, *Colleges Profit as Banks Market Credit Cards to Students*, N.Y. TIMES (Dec. 31, 2008), http://www.nytimes.com/2009/01/01/business/01student.html.

[50] *See* NEWTON LEE, FACEBOOK NATION: TOTAL INFORMATION AWARENESS 85–86 (2d. ed. 2014) (describing Google Street View cars, which take pictures "contain[ing] unsuspecting individuals and private vehicles that happened to be in the . . . wrong place at the wrong time" in "streets, national parks, university campuses, sports stadiums, and museums around the world").

[51] *See, e.g.*, Amicus Curiae Brief of Law Professors in Support Apple, Inc., In the Matter of the Search of an Apple IPhone Seized During Execution of Search Warrant on a Black Lexus IS300, CA License Plate 35KGD203 (No. 5:16-cm-00010-SP), 2016 WL 1134148 (C.D. Cal. 2016).

[52] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy, Hearing before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Sally Quillian Yates, Deputy Att'y Gen., Department of Justice and James B. Comey, Director, Federal Bureau of Investigation) [hereinafter *Going Dark Statement*].

[53] Terrorists' use of cyber communications has been grouped in different ways by different bodies. *See, e.g.*, UNITED NATIONS OFFICE ON DRUGS AND CRIME, *supra* note 37, at 3 (classifying "the means by which the Internet is often utilized to promote and support acts of terrorism [into] six sometimes overlapping categories: propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communications and open-source information); execution; and cyberattacks"). The use of Internet services for the commission of cyberattacks and for the financing of terror activity is beyond the scope of this

outreach for recruitment, mostly facilitated by social media sites such as Facebook and Twitter; (2) private communications for finalizing recruitment and for use in communication among dispersed terror cells to provide for widespread attacks, mostly facilitated by mobile applications such as WhatsApp, Line, and Kik; and (3) the dissemination of information aimed to either assist in lower-level attacks or to terrorize the public of developed nations, facilitated by Facebook, Google, and YouTube. Grouping these categories by use can help to examine responsibilities and liabilities that will later be contemplated for the companies providing these services.

1. Targeting and Outreach

Terror organizations' use of Internet resources as recruiting platforms has been widely known since at least 2009, when "A Course in the Art of Recruiting"—an Al Qaeda manual—was discovered in Iraq by U.S. forces.[54] Since then, the use of the Internet for terror recruitment and radicalization has increased exponentially.[55] Most recently, ISIS has drawn over 20,000 foreign fighters to Syria from more than 90 countries, mainly through cyber contacts.[56] Over 150 of these fighters were recruited from the United States, and some have since died there.[57] Estimates from 2014 indicate that ISIS has recruited more than 16,000 members from around the world using social media.[58] What may be a bigger threat, however, is the concern "that fighters will attempt to return to their home countries . . . and look to participate in or support terrorism and the radicalization to violence."[59] As a result, some argue that homegrown violent extremists (HVEs) pose "the most likely and immediate threat" to the United States.[60] Importantly, recruitment can focus even on extremely unlikely candidates. For example, the *New York Times* recently detailed the recruitment of a 23-year-old Sunday school teacher.[61]

Article, but is also worthy of recognition by law enforcement, and indeed is normally handled in more specialized investigation and prosecution procedures.

[54] *See* Abdullah Warius & Brian Fishman, *A Jihadist's Course in the Art of Recruitment*, CTC SENTINEL, Feb. 15, 2009.

[55] *See Rasmussen Statement*, *supra* note 38 ("This online environment is likely to play a critical role in the foreseeable future in radicalizing and mobilizing [Homegrown Violent Extremists] towards violence.").

[56] *Id.* ("The rate of travelers into Syria exceeds the rate of travelers who went to Afghanistan/Pakistan, Iraq, Yemen, or Somalia at any point in the last ten years.").

[57] *Id.*

[58] Dan Verton, *Are social media companies doing enough to stop terrorist recruitment?*, FEDSCOOP (Dec. 10, 2014), http://fedscoop.com/social-media-companies-enough-stop-terrorist-recruitment.

[59] *Rasmussen Statement*, *supra* note 38 (emphasizing further that "[w]e have witnessed this phenomenon in the lone offender attack[s]" in Belgium (killing four) and Libya (killing nine, including one American)).

[60] *Id.*

[61] *See* Rukmini Callimachi, *ISIS and the Lonely Young American*, N.Y. TIMES (June 27, 2015), http://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html?_r=1.

Several think tanks and defense commentators aim to discover exactly how terror organizations are recruiting online.[62] The first stage of recruitment generally begins with targeting and outreach, a stage that entails making initial contact, profiling the target, and developing a relationship with an online user.[63] In establishing initial contact, ISIS recruiters "seek to communicate with potentially disenfranchised or disaffected people by tweeting, retweeting, and using popular hashtags or hashtags relating to divisive current events."[64] Recruiters then create an online micro-community around the targeted recruit through which the recruiters are able to stay in nearly constant contact with the target to progress the relationship and encourage the recruit to isolate himself from "moderating influences."[65] The most useful terror recruiting tools are the same sites most useful to data miners and advertisers[66]: social media websites such as Twitter[67] and Facebook.[68]

2. Private Communications

Terror organizations use the Internet and mobile applications, such as WhatsApp, Kik, Surespot, Skype, and Telegram,[69] for private communications to "reel in" recruits, plan attacks, and execute those attacks.[70] The shift to private communications, which generally indicates the "deepening radicalization" of an

---

[62] *See, e.g.*, J.M. Berger, *How terrorists recruit online (and how to stop it)*, BROOKINGS: MARKAZ BLOG (Nov. 9, 2015), http://www.brookings.edu/blogs/markaz/posts/2015/11/09-countering-violent-extremism-online-berger (analyzing the online terror recruitment strategy as a targeted progression from discovery to the creation of a micro-community, isolation, a shift to private communications, and encouragement to take action).

[63] *See* J.M. Berger, *Tailored Online Interventions: The Islamic State's Recruitment Strategy*, 8 CTC SENTINEL 19 (2015).

[64] *Id.* at 21.

[65] *Id.*

[66] *See* Ulrike Klinger & Jakob Svensson, *Network Media Logic: Some Conceptual Considerations*, *in* THE ROUTLEDGE COMPANION TO SOCIAL MEDIA AND POLITICS 33 (Axel Bruns et al. eds., 2015) ("By spending time online and updating their social media profiles, users allow capitalist companies to exploit their information—knowingly or not. Social media companies accumulate capital through data mining of displayed personal information, which they sell to commercial actors or other organizations interested in targeting users with information.").

[67] *See generally* Lorenzo Viddino & Seamus Hughes, *ISIS in America: From Retweets to Raqqa*, THE GEORGE WASHINGTON UNIVERSITY PROGRAM ON EXTREMISM (Dec. 2015).

[68] *See* Nick Allen, *Facebook emerges as 'terrorist recruiting ground,'* TELEGRAPH (Dec. 10, 2010), http://www.telegraph.co.uk/technology/facebook/8195214/Facebook-emerges-as-terrorist-recruiting-ground.html.

[69] These applications are preferred by terror organizations because they sport strong encryption. However, Facebook and Twitter are also used for private messaging. *See* Berger, *supra* note 63, at 21–22.

[70] *See, e.g.*, David E. Sanger & Nicole Perlroth, *Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks*, N.Y. TIMES (Nov. 16, 2015), http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html?_r=0; Evan Perez & Shimon Prokupecz, *Paris attackers likely used encrypted apps, officials say*, CNN (Dec. 17, 2015), http://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/.

individual target, can be troublesome for law enforcement investigations.[71] Indeed, Department of Justice (DOJ) and FBI officials have noted that the use of private encrypted messaging platforms "are tremendously problematic when used by terrorist plotters."[72] The movement from public, open source communications such as Facebook and Twitter posts to private communications, such as encrypted messaging, is referred to as "going dark."[73] This increased difficulty is due to the procedural requirements needed to legally monitor private communications,[74] the time and expense required to crack encryption technology,[75] and the public debate over the necessity of government monitoring generally.[76] Civil libertarians who celebrate the increasing inaccessibility of encrypted conversations must recognize that the government counterterrorism response has to be an increase in upfront surveillance in less private contexts and a shift toward more "anticipatory prosecutions" like our first proposal.

However, despite public unease over government monitoring, a 2013 report demonstrates that "more than 50 potential terrorist attacks have been thwarted" by NSA electronic surveillance programs.[77] This type of monitoring can be accomplished through currently legal means: the private communications described in this report were either legally tapped under the Foreign Intelligence Surveillance Act[78] or a Title III wiretap application,[79] or acquired under the Electronic Communications Privacy Act.[80]

Some of the public opposition to electronic surveillance seems misguided in that it ignores several important facts, such as the ability of companies to buy

---

[71] *See* Berger, *supra* note 62 (describing ISIS' efforts to isolate their targets and then shift to private communications to continue the radicalization and recruitment process); Theodore Schleifer, *FBI director: We can't yet restrain ISIS on social media*, CNN (Jun. 18, 2015), http://www.cnn.com/2015/06/18/politics/fbi-social-media-attacks/.

[72] *Going Dark Statement*, *supra* note 52.

[73] *Id*.

[74] *See generally* ELIZABETH B. BAZAN, CONG. RESEARCH SERV., RL30465, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW (2007) (outlining requirements for obtaining permission to monitor under FISA).

[75] Margaret Steen, *The Ethics of Encryption*, SANTA CLARA UNIV. (Feb. 1, 2015), https://www.scu.edu/ethics/focus-areas/business-ethics/resources/the-ethics-of-encryption/ (recording FBI agent David J. Johnson's statement that the difficulty of cracking encrypted data and enumerating the problem of encryption as an issue of "whether to help the government get access to information it is legally entitled to have").

[76] *See* JONATHAN MASTERS, COUNCIL ON FOREIGN REL., ISSUE GUIDE: THE DOMESTIC SURVEILLANCE DEBATE (2013).

[77] John R. Parkinson, *NSA: 'Over 50' Terror Plots Foiled by Data Dragnets*, ABC NEWS (June 18, 2013), http://abcnews.go.com/Politics/nsa-director-50-potential-terrorist-attacks-thwarted-controversial/story?id=19428148.

[78] The Foreign Intelligence Surveillance Act of 1978 is codified at 50 U.S.C. §§ 1801–71 (West 2015).

[79] The Wiretap Act of 1968 is codified at 18 U.S.C. §§ 2510–22 (West 2015).

[80] Enacted in 1986, this Act created the Stored Communications Act, codified at 18 U.S.C. §§ 2701–11 and the Pen Register Statute, codified at 18 U.S.C. §§ 3121–27 (West 2015).

and sell data about users (for instance, public universities often sell information about students), the lack of privacy of much data that could potentially be mined (open-source nature of the information), and the existence of data centers that network together urban cities' surveillance infrastructure (including features such as facial recognition.)[81] Recent declassification of NSA reports also indicates that the actual amount of monitoring has been much less widespread than believed.[82]

Public opposition to electronic surveillance may also underestimate the tangibility of the thwarted threats.[83] When the government successfully prevents an attack, it is easy to argue that a terrorist threat is only speculative in nature.[84] However, government officials have warned that concerns about terrorist use of encrypted messaging in expanding terror organizations and plotting terror activity "are not just theoretical," but "remain among the highest priorities for the Department of Justice, including the FBI, and the United States government as a whole."[85]

3. Dissemination of Information

Another category of Internet services used by terrorist organizations are those that aid in the ability to distribute terror propaganda and facilitate terrorist activity. This category includes beheading videos and other displays of violence,[86] as well as instructional information for criminal activity such as the manufacture and deployment of bombs[87] and the building of biological weapons.[88] It may also include the use of Internet services to buy and sell components for weapons of

---

[81] *See, e.g.*, Catherine Crump, *Surveillance Policy Making by Procurement*, 90 WASH. L. REV. (forthcoming 2016).

[82] Charlie Savage, *N.S.A. Gets Less Web Data Than Believed, Report Suggests*, N.Y. TIMES (Feb. 16, 2016), http://www.nytimes.com/2016/02/17/us/report-says-networks-give-nsa-less-data-than-long-suspected.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=0.

[83] *See supra* Section 1.A.

[84] PHILIP BOBBITT, TERROR AND CONSENT: THE WARS FOR THE TWENTY-FIRST CENTURY 139 (2008) ("considering as an example of the criticism of the Clinton administration for preclusive action taken with an alleged lack of proof that Khartoum was shipping weapons, despite ample proof otherwise").

[85] *Going Dark Statement*, *supra* note 52.

[86] *See, e.g.*, Jeff Bercovici, *YouTube's Policies Are Clear: Beheading Is Not An Act Of Free Speech*, FORBES (Sept. 3, 2014), http://www.forbes.com/sites/jeffbercovici/2014/09/03/youtubes-policies-are-clear-beheading-is-not-an-act-of-free-speech/#10adfce91b04 (describing use of Twitter, YouTube, and Facebook to post beheading videos); Leo Kelion, *Facebook lets beheading clips return to social network*, BBC (Oct. 21, 2013), http://www.bbc.com/news/technology-24608499.

[87] Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet*, U.S. INSTITUTE OF PEACE, at 9 (2004) ("These sites and related forums permit terrorists . . . to exchange not only ideas and suggestions but also practical information about how to build bombs, establish terror cells, and carry out attacks.").

[88] *Terrorists Take Advantage of Technology*, THE TRUMPET (Sept. 5, 2005), https://www.thetrumpet.com/article/1769.1 ("Instructions for just about any terrorist technique—including, for example, directions detailing how to make a biological weapon from the pneumonic plague—can be found on al Qaeda websites.").

mass destruction.[89] Terrorist dissemination and manipulation of media not only play a large role in recruitment;[90] they also craft an environment in which the general public is subjected to a constant state of terror.[91]

Terrorist organizations use websites like YouTube, Google,[92] Facebook,[93] and other public Internet sites (including ISIS's English-language webzine)[94] to disseminate propaganda, enlist followers, and provide weapons training. This use of the Internet "permit[s] Islamist terrorist groups to maintain an active, pervasive, and amplified voice" that offsets intelligence and law enforcement successes.[95] Commentators often criticize the tendency of these Internet platforms to "robotically amplify the ISIS message."[96] For example, these sites contain terrorist videos displaying American soldiers being shot, action figures recreating beheadings of journalists, tributes to suicide bombers, and propaganda promoting terrorist leaders and praising terrorist attacks.[97] Any effective counterterrorism operations should therefore involve the curtailment of the use of these web functions.[98] As long as these sites continue to openly provide fora for the

---

[89] OFFICE OF THE COORDINATOR FOR COUNTERTERRORISM, *The Global Challenge of WMD Terrorism* at 178–79 (2010) ("The diffusion of scientific and technical information regarding the assembly of nuclear weapons, some of which is now available on the Internet, has increased the risk that a terrorist organization with the right material could develop its own nuclear weapon.").

[90] *Current Terrorist Threat to the United States: Hearing Before the Senate Select Comm. on Intelligence*, 114th Cong. (2015) (statement of Nicholas J. Rasmussen, Dir., National Counterterrorism Center) (crediting ISIS's "adept exploitation of the media attention generated by the group's actions" in creating "unprecedented opportunities for the group to reach potential recruits or influence those inspired by the group's message").

[91] E. Alison Holman, Dana Rose Garfin & Roxane Cohen Sliver, *Media's role in broadcasting acute stress following the Boston Marathon bombings*, 111 PSYCHOLOGICAL AND COGNITIVE SCIENCES 93, 93 (noting that the U.S. population is the "terrorists' intended psychological target" in perpetuating widespread media coverage following terrorist acts).

[92] *Lieberman Calls on Google to Take Down Terrorist Content,* U.S. Senate Comm. on Homeland Security & Governmental Affairs (May 19, 2008), https://www.hsgac.senate.gov/media/majority-media/lieberman-calls-on-google-to-take-down-terrorist-content.

[93] DEP'T OF HOMELAND SECURITY, DHS Terrorist Use of Social Networking Facebook Case Study, PUBLIC INTELLIGENCE (Dec. 5, 2010), https://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/ (showing terrorist use of Facebook as "a way to share operational and tactical information, such as bomb recipes, AK-47 maintenance and use, tactical shooting, etc.," as "a gateway to extremist sites" and as "a media outlet for terrorist propaganda and extremist ideological messaging").

[94] PETER BERGEN, UNITED STATES OF JIHAD 9 (2016).

[95] *Lieberman Calls on Google to Take Down Terrorist Content,* U.S. Senate Comm. on Homeland Security & Governmental Affairs (May 19, 2008), https://www.hsgac.senate.gov/media/majority-media/lieberman-calls-on-google-to-take-down-terrorist-content (transcribing the entirety of Homeland Security and Governmental Affairs Committee chairman Lieberman's letter to Google chairman Eric Schmidt).

[96] Berger, *supra* note 62.

[97] *Terror on YouTube: The Internet's Most Popular Sites are Becoming Tools for Terrorist Recruitment*, THE FORENSIC EXAMINER (2010), http://www.theforensicexaminer.com/archive/fall08/10/.

[98] *Internet Terror Recruitment and Tradecraft: How Can We Address an Evolving Tool While Protecting Free Speech?: Hearing Before the House of Representatives Comm. on Homeland Security,* 111th Cong. (2010) (statement of Rep. Harman) ("[W]e need to find the right way and

distribution of terrorist material, each one of them provides material support to an FTO, which, if done knowingly, would be in direct contravention of 18 U.S.C. § 2339B. These social media sites must be encouraged to discover offending posts and report them to federal law enforcement authorities to avoid what on a practical level constitutes complicity with terrorist organizations.

C. *Current Problems with Private Sector Discretion Regarding Accounts*

In January 2016, Twitter publicized its unilateral closing of more than 125,000 accounts of "suspected terrorists" since 2015.[99] Twitter did not, however, indicate what measures the company used to decide whether an account was sufficiently linked to terror-related crime to warrant termination, how it monitored such accounts, or whether it had any standard practices in place to address these issues.[100] The closing of an account also does not seem to prevent users from creating a new account under a different name to resume posting. These open questions demonstrate a few of the reasons why the placement of responsibility and discretion to private companies to shut down social media accounts is not conducive to the overall counterterrorism strategy. In addition, the self-censorship of private companies does not seem to be genuinely effective. Indeed, even after Facebook's implementation of its "more aggressive suppression tactics" of ISIS-related use of its website, about half of ISIS-related arrests in the U.S. involved the use of Facebook.[101] Since private companies have increased their suspensions

---

place to intercept those who would do us harm. Developing a strategy around the internet is not optional. It has to be part of the equation.").

[99] Patrick Smith, *Twitter Closes 125,000 Accounts Suspected of Inciting Terrorism*, *Violence*, NBC (Feb. 5, 2016), http://www.nbcnewyork.com/news/national-international/Twitter_Closes_125000_Accounts_Suspected_Of_Inciting_Terrorism_Violence-367855381.html.

[100] *See* Ronan Farrow, *Why aren't YouTube, Facebook, and Twitter doing more to stop terrorists from inciting violence?*, WASH. POST (July 10, 2014) https://www.washingtonpost.com/posteverything/wp/2014/07/10/farrow-why-arent-youtube-facebook-and-twitter-doing-more-to-stop-terrorists-from-inciting-violence/ (quoting a media company's senior executive, who asserts that distinguishing what should be taken down for terror involvement and what should be left alone is "not something we'd want to do"); Julia Greenberg, *Why Facebook and Twitter Can't Just Wipe Out ISIS Online*, WIRED (Nov. 21, 2015), http://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/ (discussing the challenge for sites like Twitter and Facebook in defining what content "promotes terrorism"); Deepa Seetharaman, Alistair Barr & Yoree Koh, *Social-Media Sites Face Pressure to Monitor Terrorist Content*, WALL ST. J. (Dec. 6, 2015), http://www.wsj.com/articles/social-media-sites-face-pressure-to-monitor-terrorist-content-1449448238 (describing Facebook's removal of San Bernardino shooter Tashfeen Malik's Facebook page, but noting Facebook's refusal to "disclose its contents" or to "say how it found the profile and determined its authenticity").

[101] J.M. Berger, *Tailored Online Interventions: The Islamic State's Recruitment Strategy*, COMBATTING TERRORISM CTR. AT WEST POINT (Oct. 23, 2015), https://www.ctc.usma.edu/posts/tailored-online-interventions-the-islamic-states-recruitment-strategy.

of social media accounts, "the ratio of Islamic State supporters to non-supporters in monitored social networks has increased."[102]

Social media companies certainly realize that ISIS relies upon them to summon new recruits, spread propaganda, and instigate further attacks. Yet many of these companies do little or nothing to curb these activities. For example, an ISIS terrorist used Twitter to announce attacks on tourists months before he carried them out,[103] and YouTube has refused to remove grisly videos of three separate mass killings.[104] Twitter attended a meeting with the French official investigating the Charlie Hebdo attack and concomitant Twitter postings showing the execution of police officer, but it refused his request to remove the posts. Twitter's excuse was that the algorithm to remove child pornography is much easier to set up than an algorithm to find jihadi information. [105] Facebook is the only company that proactively removes posts related to terrorist organizations. Facebook has a former federal prosecutor heading that effort, which relies on users to alert the company to posts that celebrate terrorism and then hires screeners to review the reported content.[106] Twitter, when pressed, will sometimes remove tweets in real time (like the live-tweet of the terrorist attack at the Nairobi mall), but will allow the users to quickly create new Twitter accounts under different names and repost.[107]

In addition to official, company-sanctioned cancellation of social media accounts for violations of internal company policy, several individuals have been able to hack and shut down social media accounts of suspected terrorists believed to be connected to ISIS, particularly after the 2015 Paris attacks.[108] This is not the first time that private, independent hackers have interfered with others' social

---

[102] *Id*.

[103] Lizzie Dearden, *Tunisia attack: Isis-affiliated group sent tweet threatening Western tourists with massacre*, THE INDEPENDENT (June 30, 2015), http://www.independent.co.uk/news/world/africa/tunisia-attack-isis-affiliated-group-posted-tweet-threatening-western-tourists-with-massacre-10356183.html.

[104] Scott Higham & Ellen Nakashima, *Why the Islamic State Leaves Tech Companies Torn between Free Speech and Security*, WASH. POST (July 16, 2015), https://www.washingtonpost.com/world/national-security/islamic-states-embrace-of-social-media-puts-tech-companies-in-a-bind/2015/07/15/0e5624c4-169c-11e5-89f3-61410da94eb1_story.html (describing YouTube videos of ISIS killing men accused of cooperating with U.S. coordinated airstrikes in Iraq and Syria by incineration in a car, drowning in a cage lowered into a swimming pool, and decapitation by explosive necklaces, and other terrorists live-tweeted Al-Shabab attacks in an upscale Westgate shopping mall in Nairobi).

[105] *Id*.

[106] *Id.*

[107] Mark Gollom, *Kenya attack: Why al-Shabaab live-tweeted the assault*, CBS News (Sept. 24, 2013), http://www.cbc.ca/news/world/kenya-attack-why-al-shabaab-live-tweeted-the-assault-1.1865566 (mentioning that al-Shabaab tweeted from a different Twitter feed after the previous one was shut down).

[108] Elizabeth Weise, *Anonymous, 'hunters' claim to thwart Islamic State online*, USA TODAY (Nov. 19, 2015), http://www.usatoday.com/story/tech/2015/11/18/anonymous-isis-paris-attacks-terrorists-ghostsec-online-twitter-telegram-facebook/76000506/.

media accounts,[109] but it makes a weighty statement regarding the ease of access and monitoring of social media—such that even an independent citizen can do it.[110] It might also align with a broader viewpoint of the public that existing governmental measures are inadequate to the extent they allow terrorist activity on the Internet.[111]

The turn to vigilante counterterrorism by civilians,[112] however noble their motives, does not adequately contribute to an effective and just counterterrorism policy.[113] Continued failure to address terror activity online will undoubtedly lead to increased vigilante justice by independent hackers, pulling control and ability to monitor from the government and creating uncertainty in the current methodology used to combat terrorism online.[114] The FBI must have access to the information on these sites before it can begin making decision on which accounts to shut down, and whether there are any U.S.-based extraditable defendants to charge.

The activities described above demonstrate several important findings regarding social media regulations, including: (1) the current online counterterrorism strategy (or lack of strategy) is inadequate and unacceptable, even in the minds of ordinary citizens, and requires improved legislation; (2) private companies and vigilante hackers are not the correct parties on which to place a burden of evaluating what constitutes legally impermissible terror-related online activity, and therefore, the placement of discretion on the company or

---

[109] *See, e.g.*, *'We know everything about ISIS online': Hackers claim foiling terror attacks in Tunisia & New York*, RT NEWS (Aug. 31, 2015), https://www.rt.com/news/313940-ghostsec-foils-isis-terror-plots/ (discussing the independent hacking of terrorist social media accounts prior to the November 2015 Paris attacks).

[110] Chris Hoffman, *How Hackers Actually 'Hack Accounts' Online and How to Protect Yourself*, HOW-TO GEEK (Aug. 10, 2013), http://www.howtogeek.com/169847/how-attackers-actually-hack-accounts-online-and-how-to-protect-yourself/ (reporting on the availability of leaked passwords, usernames, and e-mails online, and further asserting that "accounts are hacked in fairly simple ways").

[111] *See* George Gao, *What Americans think about NSA surveillance, national security and privacy*, PEW RESEARCH CTR. (May 29, 2015), http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/ ("Americans also say anti-terrorism policies have not gone far enough to adequately protect them."); *see also* BERGEN, *supra* note 94, at 18 ("Polls taken every year since 9/11 have found that four out of ten Americans worry that they or a family member will be the victim of an act of terrorism.").

[112] Tammy Leitner & Lisa Capitanini, *'Patriotic Hackers' Claim to Fight Cyber War Against Terrorists*, NBC CHICAGO (Feb. 19, 2015), http://www.nbcchicago.com/news/local/Patriotic-Hackers-Cyber-War-Against-Terrorists-292825571.html ("[Cyber hackers] claim they are doing what the Government does not do—taking down terrorist-run websites that recruit Westerners and support Jihadi propaganda.").

[113] Jack Smith IV, *This Is How Anonymous' Fight Against ISIS Hurts Actual Counterterrorism*, TECH.MIC (Nov. 18, 2015), http://mic.com/articles/128797/how-anonymous-ghostsec-and-ctrlsec-are-really-fighting-isis-online#.I9nRUL0cP.

[114] David F. Gallagher, *HACKERS; Government Tells Vigilantes Their 'Help' Isn't Necessary*, N.Y. TIMES (Feb. 20, 2003), http://www.nytimes.com/2003/02/20/technology/hackers-government-tells-vigilantes-their-help-isn-t-necessary.html (reporting on the increase in anti-U.S. hacking "as international tensions rise").

hacker is the incorrect approach; and (3) the blanket shutdown of social media accounts related to terrorism is not adequately preventative and may be counterproductive to the counterterrorism strategy of the government.

II. Two Proposals to Correct Anti-Terrorism Legislative Deficiencies

It is no doubt useful to discover individual terror recruits, but the aims of U.S. counterterrorism online stretch far beyond identification—they include finding recruits, terminating wider terror conspiracy operations, and shutting down the communications infrastructure enabling terror cells.[115] Legislators have pleaded for nearly a decade with the private sector to take action that would "curtail the use of [websites] to disseminate the goals and methods of those who wish to kill innocent civilians."[116] As discussed above, these pleas have been met with halfhearted and short-lived responses.[117]

The harms posed by terror organizations online may seem remote in that there are proportionally few instances of terror activity coming to fruition. The exponential increase in terror activity and dissemination of terrorist-related information and propaganda in recent years and the proliferation of Internet connectivity, however, indicates that online facilitation will only become more frequent. Legislative reform is therefore imperative to combat terror on the technological media that terrorist organizations are able to access.[118]

---

[115] U.S. DEP'T OF JUSTICE, FY 2013 ANNUAL PERFORMANCE REPORT & FY 2015 ANNUAL PERFORMANCE PLAN (2013) (listing the FBI's counterterrorism goals, such as: preventing, disrupting, and defeating terrorist operations before they occur; prosecuting those involved in terrorist acts; investigating and prosecuting espionage activity against the U.S.; proactively preventing insider threats; and combatting "cyber-based threats and attacks through the use of all available tools, strong private-public partnerships, and the investigation and prosecution of cyber threat actors").

[116] *Lieberman Calls on Google to Take Down Terrorist Content*, U.S. Senate Comm. on Homeland Security & Governmental Affairs (May 19, 2008), https://www.hsgac.senate.gov/media/majority-media/lieberman-calls-on-google-to-take-down-terrorist-content.

[117] *Terror on YouTube: The Internet's Most Popular Sites are Becoming Tools for Terrorist Recruitment*, THE FORENSIC EXAMINER (2010), http://www.theforensicexaminer.com/archive/fall08/10/ (finding that "weeks after the Lieberman [request for collective private sector assistance], many videos remained on YouTube that appeared to promote or affiliate with terrorist groups such as Hamas, Hezbollah, Al-Qaeda, and the Iraqi insurgency").

[118] State of Homeland Security Address: House Committee on Homeland *Security* (2015) (statement of Michael McCaul, Chairman, H. Comm. on Homeland Security) (affirming that "[i]t is time for Congress to act" in response to terrorists' use of secure communications in plotting attacks); *In Presidential Statement, Security Council Calls for Redoubling Efforts to Target Root Causes of Terrorism as Threat Expands, Intensifies*, U.N. MEETINGS AND PRESS COVERAGE (Nov. 19, 2014), http://www.un.org/press/en/2014/sc11656.doc.htm (reporting on the U.N. Security Council's urging to the States "to counter violent extremist propaganda on the Internet and social media by developing effective counter-narratives, stressing the importance of partnering with civil society and the private sector in such efforts").

A. *Current Statutes Insufficient to Address Harms*

1. Material Support Statutes

The material support statutes are codified in 18 U.S.C. §§ 2339A through 2339D.[119] Originally enacted in response to domestic terrorist attacks in the 1990s,[120] these statutes criminalize the provision of "material support or resources" to a foreign terrorist organization,[121] as well as the provision of financial support[122] and fundraising efforts for terrorist organizations,[123] and the receipt of "military-type training" from any designated FTO.[124] The statutes provide a list of specific, though nonexclusive, examples of material support, including money, training, expert advice or assistance, communications equipment, service, and personnel.[125] Legislative revisions of the material support statutes, enacted as recently as 2015,[126] have further clarified the definition of "material support" to comply with First Amendment vagueness concerns, added specific acts which constitute material support, and increased the penalties under the material support statues.[127]

These innovative statutes are purposefully written quite broadly—they are in effect extremely expansive attempt provisions that impose liability at an early stage.[128] A defendant need not take a "substantial step" as required under the Model Penal Code, federal code, and most state statutes defining attempts,[129] nor does the defendant need to agree to commit a terrorist offense or commit an overt act, as required under the federal conspiracy statute.[130] A wide range of speech

---

[119] 18 U.S.C. § § 2339A-2339D (West 2016). *See generally* NORMAN ABRAMS, ANTI-TERRORISM AND CRIMINAL ENFORCEMENT (4th ed. West 2012).
[120] *See* Federal Code and Rules (West 2016) (Historical and Statutory Notes sections after each code section). *See also* Holly Chapin, *Clarifying Material Support to Terrorists: The Humanitarian Project Litigation and the U.S. Tamil Diaspora*, J. OF INT'L SERVICE 69 (2011).
[121] *See* most pertinently, 18 U.S.C. § 2339B (West 2016).
[122] 18 U.S.C. § 2339A (West 2016).
[123] 18 U.S.C. § 2339C (West 2016).
[124] 18 U.S.C. § 2339D (West 2016).
[125] 18 U.S.C. § 2339B(g)(4) (West 2016).
[126] USA Freedom Act, Pub. L. No. 114-23, 129 Stat. 300 (2015).
[127] *Id.*, Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, title VI, §§ 6602–6603(c)-(f), 118 Stat. 3761, 3762–63 (2004).
[128] *See* Robert M. Chesney, *Beyond Conspiracy? Anticipatory Prosecution and the Challenge of Unaffiliated Terrorism*, 80 S. CAL. L. REV. 425 (2007) (arguing that material support offenses can be employed at a much earlier stage than traditional inchoate offenses such as attempt and conspiracy); Norman Abrams, *The Material Support Terrorism Offenses: Perspectives Derived from the (Early) Model Penal Code*, 1 J. NAT. SEC.L. & POL'Y 5, 9–11 (2005) (suggesting that 2339A and 2339B are doctrinally innovative and, while they sound in complicity, they are much broader in scope).
[129] *See, e.g.*, MPC § 5.01, Criminal Attempt (official Draft, 1985); TPC 15.01; MCL 750.92 (Michigan's criminal attempt statute). The federal code has no general attempt statute, but, where specific offenses include attempts, federal courts follow the MPC definition. *See* United States v. Urban, 404 F.3d 754, 767 (3d Cir. 2005) (attempted extortion in violation of 18 U.S.C. section 1951).
[130] *See* 18 U.S.C. § 371 (West 2016).

and conduct has been held to violate the material support provisions. Some examples include an individual transferring funds to, or engaging in fundraising efforts on behalf of, a designated FTO,[131] an aspiring terrorist planning to set up a terrorist training facility in his home state,[132] an attorney facilitating the passing of information from her client,[133] friends of an FBI informant obtained video equipment and taking photographs and videos of federal buildings,[134] an individual producing a video swearing allegiance to the Islamic State and expressing his intent to provide himself as a fighter,[135] and a medical doctor promising the future provision of medical services.[136] The court upheld the material support conviction for each defendant in these cases. Many of these prosecutions involve nothing more than online posts recruiting new members for FTOs[137] or teaching FTO members how to use domestic and international law to advocate for their cause.[138] Since communication might violate these statutes if a

---

[131] United States v. Afshari, 446 F.3d 915 (9th Cir. 2006), *cert. denied*, Rahmani v. United States, 549 U.S. 1110 (2007); United States v. El-Mezain, 664 F.3d 467 (5th Cir. 2011).

[132] Earnest James Ujaama, who allegedly was trying to set up a terrorist training facility in the state of Washington. *See also* United States v. Mehanna, 735 F.3d 32 (1st Cir. 2013), *infra* note 247; United States v. Kaziu, 559 Fed. Appx. 32 (2d Cir. 2014) (upholding conviction for attempting to provide material support by traveling overseas with the goal of joining al-Shabaab's war against the Somali government).

[133] United States v. Stewart, 590 F.3d 93 (2d Cir. 2009) (rejecting the defendant's First Amendment argument that, because "the government established only that they provided the underlying conspiracy with Abdel Rahman's 'pure speech,'" the defendant "did not provide 'personnel' within any constitutional interpretation of section 2339A.). *See also* United States v. Hassan, 742 F.3d 104 (4th Cir. 2014) (holding in an 18 U.S.C. section 2339A case that the First Amendment was no bar to the government's use of defendants' Facebook and cellphone speech to demonstrate their participation in the charged conspiracy).

[134] United States v. Augustin, 661 F.3d 1105 (11th Cir. 2011).

[135] United States v. Nader Salem Elhuzayel, 2016 U.S. Dist. LEXIS 104328 (S.D. Cal. Aug. 15, 2016) (upholding conviction for attempting to provide material support in violation of 18 U.S.C. section 2339B where defendant "told the FBI that after he reached Istanbul, he was going to post on Twitter some hint that he wanted to make 'hijra' – a migration to ISIS – in order to solicit assistance in traveling to the Islamic State, that someone would send a tweet to him in response, he would get from that person a Surespot contact, and then he would tell the Surespot contact he was in Istanbul waiting for assistance in traveling to the Islamic State.").

[136] United States v. Farhane, 634 F.3d 127 (2d Cir. 2011), *infra* note 258.

[137] Change of Plea Memorandum, United States v. Khalid, No. 11-420 (E.D. Pa. Mar. 27, 2012);.United States v. Nagi, 2015 WL 4611914 (W.D.N.Y. July 31, 2015) (upholding detention order where defendant was charged with attempting to provide material support and resources to a designated FTO by using social media extensively to promote ISIL, by traveling to Turkey with the intent to enter Syrian areas controlled by ISIL, and by stockpiling tactical gear); United States v. Bell, 81 F.Supp.3d 1301 (M.D. Fla. 2015) (upholding sentence of American defendant inspired by video teaching of foreign member of ISIL); United States v. Amawi, 695 F.3d 457, 466 (6th Cir. 2012*). See also* United States v. Ciccolo, 2015 WL 9294206 (D. Mass. Dec. 21, 2015) (upholding submission of redacted video against motion by Boston newspaper to obtain version of video recording with defendant's face visible, as government established that the un-redacted video of an American defendant expressing his support for ISIL would have less online recruitment value for the FTO).

[138] *See* Holder v. Humanitarian Law Project, 561 U.S. 1 (2010), *infra* note 240 (noting that Plaintiffs wished to engage in "(1) train[ing] members of [the] PKK on how to use humanitarian and international law to peacefully resolve disputes; (2) engag[ing] in political advocacy on behalf of Kurds who live in Turkey; and (3) teach[ing] the PKK members how to petition various

defendant has the appropriate *mens rea*, the FBI must review public speech in order to discover these violations. This is particularly important given that material support violations may be the first step in a lone wolf's decision to engage in physical acts of terrorism; locating such individuals before they act is critical.

Many governmental actors have claimed that the material support statutes are "front and center" in recent counterterrorism efforts.[139] In reality, however, they play a relatively minor role in our overall counterterrorism strategy, particularly in regard to lone-wolf situations. The aim of the statutes, and the major shift in the FBI's priority of combatting terrorist-related offenses after 9/11,[140] is to prevent terrorist acts from occurring. These statutes have failed to achieve the aim of catching would-be terrorists before they attack. Law enforcement is frequently unable to identify those individuals violating material support statutes, to stem any financial aid leaking to foreign terrorist organizations [141] or to capture terrorists before they engage in physically destructive terrorist behavior.[142] The reality of the limitations of the federal material support legislation is clear from the statistics: in scholarly data compiled over six years, only 108 defendants were charged with violations of § 2339B.[143] Moreover, the Department of Justice statistics show slightly more than 150 defendants for all "category I" offenses between September 11, 2001 and March 18, 2010.[144] For the fiscal year ending in 2014, federal prosecutors charged 105

---

representative bodies such as the United Nations for relief" (internal quotation marks omitted)). In the interest of clarity, we note that none of the plaintiffs in *Holder* were actually criminally prosecuted for teaching FTOs, as the case was one for injunctive relief. However, the Court made it clear that the conduct plaintiffs wished to engage in could well be criminal under the material support statute.

[139] Nicole Hong, *'Material Support' Statute is Front and Center in Antiterror Push,* WALL ST. J. (May 27, 2015), http://www.wsj.com/articles/material-support-statute-is-front-and-center-in-antiterror-push-1432719002. *See also Attorney General's Guidelines for Domestic FBI Operations*, U.S. DEP'T OF JUSTICE (rev. 2008).

[140] *See* JEROME P. BJELOPERA, CONG. RESEARCH SERV., REPT. TO CONGRESS, R41780: THE FEDERAL BUREAU OF INVESTIGATION AND TERRORISM INVESTIGATIONS 2 (Apr. 24, 2013) (noting that since September 11, 2011, the FBI has devoted a significant amount of its resources to the War on Terror, most notably by increasing the number of its Joint Terrorism Task Forces from 26 to more than 100).

[141] *See* Jeff Breinholt, *Resolved or Is It? The First Amendment and Giving Money to Terrorists*, 57 AM. U. L. REV. 1273 (2008).

[142] This is not to say there are not successes as well, particularly from the NSA in preventing foreign attacks, though they often do not result in prosecutions. See Parkinson, *supra* note 77.

[143] Robert M. Chesney, *Prosecution Patterns in Post-9/11 Terrorism Cases*, WAKE FOREST LEGAL STUDIES RESEARCH PAPER SERIES No. 1005478 49 (2007), http://ssrn.com/abstract=1005478 (collecting available prosecution data from Sept. 2001 through July 2007).

[144] *Report on International Terrorism and Terrorism-Related Conviction Statistics from Sept. 11, 2001 through March 18, 2010*, U.S. DEP'T OF JUSTICE, NAT'L SEC. DIV. COUNTERTERRORISM SECTION (2010), http://www.fas.org/irp/agency/doj/doj032610-stats-pdf (chart showing number of convictions, and including in Category I aircraft sabotage, WMD threats, hostage taking, bombings, material support, and violations of IEEPA). *See also* Letter from Assistant Att'y Gen. Ronald Weich to Senator Leahy and Senator Sessions Regarding Statistics Relating to the

terrorism-related offenses, comprising zero percent of federal felony offenses.[145] While this represents an increase from 2010, there is still no good method for prosecutors to assist in preempting terror activity aside from waiting for the FBI to deliver actionable information.

Thus, the most glaring issue with current material support statutes is that these laws form a reactive, rather than a proactive, counterterrorism prosecution strategy. While FBI agents certainly engage undercover operatives and attempt to infiltrate terrorist cells, this is of limited effectiveness, particularly with lone-wolf individuals. The results of this reactive strategy are potentially devastating: for every conviction, there is another conspirator that evades conviction by fleeing overseas,[146] or by simply not appearing on law enforcement radar.

2. Senator Feinstein's Proposal

In recognition of the inadequacy of existing law, a number of proposals have been put forward, most notably the Feinstein bill. Senator Feinstein's proposal in her Online Terrorism Activity Act demands only that social media companies contact the authorities when they have "actual knowledge" of terrorist activities. There is nothing wrong with such a proposal, but it will have little if any effect on social media company operations. The bar is set so high that the mandate may never be triggered. A company will almost never have actual knowledge of anti-terror violations engaged in by their users and customers because they are not looking for such violations,[147] and Senator Feinstein's bill

---

Prosecution of Terrorism, Terrorism Related Crimes and Incarceration of Terrorists by the Bureau of Prisons (Sept. 14, 2014), http://www.justice.gov/cvs/docs/terrorism-crimes-letter.html.

[145] Federal Judicial Caseload Statistics, Table D-2, U.S. District Courts—Criminal Defendants Commenced, by Offense, During the 12-Month Periods Ending June 30, 2010 Through 2014, ADMIN. OFFICE OF THE U.S. COURTS, STATISTICS DIV. (Mar. 21, 2014), http://www.uscourts.gov/statistics/table/d-2/federal-judicial-caseload-statistics/2014/03/31.

[146] *See, e.g.*, Press Release, *Fourth Minnesota Man Pleads Guilty to Conspiracy to Provide Material Support to ISIL*, U.S. Dep't of Justice Office of Pub. Affairs (Sept. 17, 2015), http://www.fbi.gov/contact-us-filed-offices/minneapolis/news/press-releases/minnesota-man-pleas-guilty-o-conspiracy-to-provide-material-support-to-isil (describing the conviction of defendant who had attempted to join ISIS, as well as the fact that his "co-conspirator . . . had successfully traveled to Syria").

[147] Some social media companies are expending some resources policing violations of their internal rules against "offensive" posts, and will sometimes delete posts that violate their rules. But such "offensive" posts are not necessarily the ones that may violate the federal criminal material support statute. Even if companies were searching for posts which potentially violate the material support statute (which they are not), the employees enforcing the company's internal rules are not lawyers, and the issue of whether a particular post violates the material support statute is a close and case-specific one. For a social media company to violate Senator Feinstein's proposal, it would have to have "actual knowledge" that a user was providing material support to a FTO; it would be insufficient for it to be reckless regarding whether users were engaged in such postings, for it to be on notice that such conduct was occurring, or that a reasonable company in its position would have been aware of such conduct. *See* MPC 2.02(2)(a)–(d) (ALI 1985) (defining culpable mental states necessary to impose criminal liability); Posters 'N' Things, Ltd. v. United States, 511 U.S. 513, 523 (1994) (using Model Penal Code terminology to frame mental state required by Mail Order Drug Paraphernalia Control Act).

does not require that they undertake any such search. Her short two-page bill purports to mirror the existing law governing child pornography. However, because of its lack of an overall framework governing social media companies in relation to terrorism, and the lack of the quick technological fix similar to the one available to electronic communications services in the child pornography area, the analogy is inapt. Thus the first problem with this model is that the comprehensive statutes governing social media companies' obligation to discover and report child pornography far exceed the detail of Feinstein's bill; a second is that the easy technological solution to finding child pornography may not be as easily applied in the terrorism context.

The two statutory schemes governing the reporting of "known" violations of child pornography offenses are complex and detailed. The Missing Children's Assistance Act of 1984 established the National Center for Missing and Exploited Children (NCMEC).[148] This is an independent private agency[149] created, in large measure, to discover methods of identifying child pornography on the Internet and to assist communication service providers and law enforcement in prosecuting the offenders. The federal substantive statutes prohibiting child pornography were enacted between 1978 and 2003.[150] NCMEC launched the CyberTipline in 1998, to provide a central location to report information regarding child sexual exploitation. It provides online users, members of the general public, and Internet service providers with a method of reporting suspected child sexual exploitation either online or through its 24-hour toll free hotline.[151] In 2008, Congress imposed the obligation on any "electronic communication service" provider or any "remote computing service" provider to forward a report to the NCMEC whenever they have "actual knowledge" of a violation of one of the child pornography statutes listed above.[152] This report includes the sender's geographic location, IP address, and copies of the child pornographic photographs or videos.

No law requires that communication service providers actually create or use tools to scan user content for known child pornography images—in fact, the

---

[148] PL 98-473, 98 Stat. 1837 (1984), codified at 42 U.S.C. § 5773(b) (2015) (delineating precisely what NCMEC is authorized to do with its federal funding); 42 U.S.C. § 5777 (2013) (authorizing $32 million in federal funds for each of fiscal years 2014 to 2018).

[149] NCMEC is a 501(c)(3) nonprofit organization. Seventy-five percent of its funding comes from federal sources. Whether the NCMEC is actually a private company, or whether it might instead be considered a state actor, is presently the subject of a controversy in the federal district courts. *See* United States v. Keith, 980 F.Supp.2d 33 (D. Mass. 2013); *see also* United States v. Ackerman, 2014 WL 2968164 (D. Kan. July 1, 2014), *rev'd and remanded* 831 F.3d 1292 (10th Cir. 2016). These cases are discussed in Part III(B), *infra*.

[150] *See* 18 U.S.C. §§ 2251, 2251A, 2252, 2252A, 2252B, 2260, 1466 (West 2016).

[151] Ackerman, *supra* note 149, at *3.

[152] 18 U.S.C. section 2258A(a) (West 2016) (providing that where company has "actual knowledge" of child pornographic pictures they must report this to the NCMEC on pain of a $150,000 fine). The terms "electronic communication service" provider and "remote computing service" provider are defined in 18 U.S.C. §§ 2258E(2) and (5) exactly as Senator Feinstein does in the Online Terrorism Activity Act. The definitions in § 2558E and her new proposal both borrow from 18 U.S.C. § 2510(15) (enacted as part of Title III in 1968) and 18 U.S.C. § 2711(2) (enacted as part of Title II in 1986).

law makes it clear that they are not required to monitor users or seek out this information.[153] However, many email providers, cloud companies, and other online service providers have decided that it is in the best interests of their users and their companies to keep their services free of illegal content.[154] Consequently, such companies often use automated tools developed by the NCMEC or developed internally to check all of their private e-mails for pornographic pictures and videos involving children.[155] Once the social company files its report with the NCMEC, federal law requires that the NCMEC shall forward these reports to appropriate law enforcement agencies designated by the Attorney General, and that law enforcement agencies use these reports to "investigate child pornography crimes."[156]

How do the communication service providers ferret out the child pornography pictures from the millions of e-mails sent daily? NCMEC developed a simple and effective technological fix. It voluntarily shares sophisticated photographic data called "hash algorithms" with the electronic communication services companies, and the companies check user photos against this data.[157] This is effective because the NCMEC maintains a database of thousands of photographs of child pornography—the same images that are frequently downloaded by pedophiles on the Internet. Companies "may" (but need not) use the "hash algorithms" to easily search their users' content for image matches, without fear of civil liability.[158] These image matches include facial features, body characteristics, size, and other features of photography. A piece of software called Microsoft PhotoDNA allows the NCMEC to scan and identify the frequently used photos using unique digital markers. Every time a new image is uploaded onto a social media site or e-mail service provider, the company can run that photo against this database using this software, which compares the digital markers to the ones in the NCMEC database. Anything that matches is deleted and reported to the federal authorities.

---

[153] 18 U.S.C. § 2258A(f).

[154] Federal District Court Judge Melgren estimates that "[a]bout 1,000 of the approximate[ly] 5,000 internet service providers in the United States have a reporting relationship with the NCMEC." Ackerman, *supra* note 149, at *3.

[155] Many companies use tools developed by the NCMEC. Others use tools developed internally. *See* Ackerman, *supra* note 149, at *2 (describing AOL's Image Detection and Filtering Process, which includes a database of hash values to check for child pornography, and noting that "AOL does not obtain hash values from any outside company and has only developed its database of hash values from the graphics review team at AOL").

[156] 18 U.S.C. § 2258A(c) (requiring that NCMEC forwards reports to appropriate federal, state, and foreign agencies); 18 U.S.C. §§ 2258A(g)(2)(A) and 2258C(e) (providing that law enforcement agencies use these reports to investigate child pornography crimes).

[157] 18 U.S.C. § 2258C(a)–(b) (providing that NCMEC "may" provide pictures of known child pornography to social media companies, and that such companies "may" check all user photos against such images).

[158] 18 U.S.C. § 2258B (providing that there can be no civil liability in state or criminal court for Internet companies performing reporting activity that identifies child pornography transmitted by users so long as the Internet company does not engage in "intentional misconduct" or act "for a purpose unrelated to the performance" of their responsibilities under this section).

Most social media outlets have been aggressive in their efforts to combat what has been termed "child exploitation material."[159] Facebook, in particular, has continued to publicly commit itself to meaningfully combatting child exploitation. While reporting by users has been central to their efforts in this regard in the past, it is by no means the only or even the primary method today. Automatic screening software like PhotoDNA scans every uploaded photo, and Facebook, like the NCMEC itself, continuously improves that software to achieve better results. Hash values representing any new offending images that the social media company finds are relayed to the NCMEC, along with the user account information required by law. After disabling offending accounts, Facebook uses additional software that either blocks sharing of such material, or flags it for expedited review by the screening team.[160] Facebook is a model in the field, and Instagram and Twitter appear to be following suit.

While this is a step in the right direction, not all social media and data-sharing sites or applications put forth the same effort.[161] This highlights an important limitation on the reporting statute: the law imposes no affirmative duty on service providers to ferret out child pornography.[162] Service providers determine the extent to which they want (and are able) to collaborate with law enforcement. These same problems will arise under a terrorism-monitoring statute, like Senator Feinstein's bill, that requires reporting only when the social media company has *actual* knowledge of a child pornography violation. Moreover, in that particular context, the public pressure and law enforcement interests may be less perfectly aligned. The public may want terror-related messages removed, and be incensed if their reporting goes unheeded, while law enforcement may wish in particular cases to retain the content, so that it can better track suspected terrorists or their recruits.

Even more importantly, so far there is no automatic algorithm set up to find phrases or videos to identify posts that may be interpreted as providing material support for terrorism. The automatic algorithm PhotoDNA identifies every offender picture in the child pornography context. In the anti-terrorism realm, reviewing speech for terms of service compliance is not presently

---

[159] *See, e.g.*, *Meet the Facebook Safety Team*, FACEBOOK (Aug. 9, 2011), https://www.facebook.com/notes/facebook-safety/meet-the-safety-team/248332788520844/.

[160] *See Facebook Safety Wall Post*, FACEBOOK (Nov. 12, 2015), https://www.facebook.com/fbsafety/ (announcing Facebook's partnership with Thorn).

[161] Kik Interactive, Inc., for example, is a Canadian-based company that supports a messaging application that is popular among teenagers. Until last year, Kik had focused its child exploitation policy on educating parents and users about the dangers of child exploitation, rather than taking an active role in prevention. Perhaps in response to an increase in child exploitation activity on the Internet and through these platforms, as well as the bad press that it generated, Kik announced in March 2015 that it would adopt the PhotoDNA software already used by Facebook and Twitter. *See* Sara Freir, *Kik Adds Tools to Prevent Child Exploitation on Messaging App*, BLOOMBERG BUSINESS (Mar. 10, 2015), http://www.bloomberg.com/neews/articles/2015-03-10/kik-adds-tools-to-prevent-child-exploitation-on-messaging-app.

[162] *See* 18 U.S.C. § 2258A(f), *supra* note 153. *See also* United States v. Cameron, 729 F.Supp.2d 418, 424 (D. Me. 2010), *aff'd*, 699 F.3d 621 (1st Cir. 2012).

accomplished solely with technology but involves human beings reading the posts and viewing the images. While technology might provide significant assistance (monitoring posts for key phrases, for example, or checking for images of the black flag of the Islamic caliphate), such monitoring is not required under Senator Feinstein's terrorism bill (or under the current framework regulating the distribution of child pornography on the Internet). Our proposal is much broader.[163]

B. *The Feasibility and Text of Our Proposals*

Our first proposal would make it a federal criminal offense for a social media company to fail to institute an effective program to discover users who may be violating material support and other terrorism-related statutes.[164]

Any social media company with 15 or more employees would be required to design or purchase a program to capture posts that might reflect a violation of any terrorism-related crime listed in 18 U.S.C. § 2332b(g)(5).[165] Social media companies would submit their programs to the Department of Justice for review. Each violation of this statute would result in an escalating series of criminal fines. Further, it would be illegal for a social media company to fail to abide by its internal compliance program once approved by the Department of Justice.

We believe such a proposal is technologically feasible. While replicating Microsoft PhotoDNA in the area of terrorism may not be possible, it would be

---

[163] Our proposal shares more similarities with the government and private company partnerships in the U.K.'s Internet Referral Unit. *See* Jessica DaSilva, *Terrorism Bill Puts Social Media Companies in Tough Spot*, BLOOMBERG CRIM. L. REP. (Jan. 6, 2016), http://www.bna.com/terrorism-bill-puts-n57982065821/. Admittedly, these partnerships are "currently under fire from the European Union" for fostering censorship. *Id.*

[164] We anticipate that this crime would apply only to companies, services, or accounts in the United States. Absent explicit language extending the statute to conduct occurring solely outside our borders, federal courts will generally presume that the legislation applies only domestically. *See, e.g.*, RESTATEMENT (THIRD) OF THE LAW OF FOREIGN RELATIONS §§ 401–02; United States v. Kassar, 660 F.3d 108 (2d Cir. 2011) (applying 18 U.S.C. §§ 1114 and 1117 to international arms dealer based in Spain, despite the fact that both statutes lacked express extraterritorial provisions, because the conspiracy to kill U.S. officers targeted U.S. citizens); United States v. Lopez-Vanegas, 493 F.3d 1305 (11th Cir. 2007) (vacating convictions for violating 21 U.S.C. §§ 841 and 846 where the object of the conspiracy was to possess controlled substances outside the United States with the intent to distribute outside the United States). *But see* The USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat, 192, 225 (2006) (codified at 21 U.S.C. § 960a, expanding the extraterritorial jurisdiction of drug trafficking offenses when they are committed in order to fund terrorism).

While there is some minimal risk that if our proposal worked well, a terrorist could go to a foreign-based service that is beyond the reach of this new U.S. law, perhaps that is just as well. In that case, the national security agencies can monitor those postings more easily than internal law enforcement might, even with the new laws.

[165] 18 U.S.C. § 2332b(g)(5) defines terrorist activity. We recognize that the demand for a pre-cleared compliance program favors large companies. We allay such concerns with a size requirement and by suggesting that this function will be contracted out to a large extent. We see examples of this with firms that provide anti-money laundering filters to banks.

possible to download images of the Islamic State's black flag, for example, an image frequently displayed on the group's propaganda posts. A social media company could create "hash values" for that image to search for it online. Much of the work in identifying such posts might not be accomplished by imaging software. It would require software that identified key phrases, or that identified groups that post regularly, post to certain sites, or attempt to steer contacts to encrypted forms of communication.

New technology abounds. For example, Neil Johnson, a physicist at the University of Miami, led a team that created a mathematical model to predict and ultimately prevent terrorist attacks from the online universe of data points. In a study published in the Journal of Science, Professor Johnson and his colleagues describe how they searched for pro-Islamic State posts from 2014 to 2015, mining discussions of beheadings and bloodbaths in multiple languages on Vkontakte, a Russian-based social media service that is the latest European equivalent to Facebook. They focused on small groups of Islamic State supporters that formed online groups. These groups posted pledges of allegiance to the extremists and offered fundraising appeals and survival tips. Professor Johnson found that so called "lone-wolf" sympathizers do not remain alone for long, but form small groups within weeks. Quashing these groups can prevent their members from fusing with those larger pro-Islamic State groups that distribute inciting videos and statements to broader audiences. Professor Johnson claims to have predicted an attack on Kobani, a Syrian town on the Turkish border in September 2014.[166] Whether or not this equation ultimately predicts attacks, it might be utilized by social media companies in finding posts that arguable violate the material support statute.

A second example of a successful compliance program is found in Israel. One recently-proposed new social media law, dubbed "the Facebook Law," would enable courts to order social networks to remove posts in cases where the user cannot be found or is not under Israel's jurisdiction.[167] A second draft bill in Israel goes further, seeking to require social networks to self-monitor for incitement or face a fine.[168] While neither of these laws has yet been enacted, Israel does have an incitement law, which permits the arrest of persons doing the posting or other kinds of incitement to violence (but does not permit the State to order the social media site to remove messages, or require them to self-monitor or pay fines). To enforce the incitement laws currently on the books, as well as to enforce the anticipated Facebook Law, Israeli police scour social networks and sift through hundreds of thousands of posts, primarily looking for "keywords, the type of

---

[166] Pam Belluck, *Scientists Craft Equation for Predicting Terrorism*, AUSTIN AMERICAN STATESMAN (June 21, 2016), at A-5; N.F. Johnson et. al., *New Online Ecology of Adversarial Aggregates: ISIS and Beyond*, 352 SCIENCE 1459–63 (June 17, 2016), http://science.sciencemag.org/content/352/6292/1459.

[167] Tia Goldenberg, *Israel's 'Facebook Law' Raises Controversy*, AUSTIN AMERICAN STATESMAN (July 23, 2016), at A-6.

[168] *Id. See also infra* notes 262–67.

exposure a post gets in terms of followers or likes and whether the user is affiliated with a militant group."[169]

Our second proposal asks social media companies to voluntarily design and implement anti-terrorist compliance programs exactly as does our first proposal. However, the companies are not subject to criminal penalties for failure to institute an effective program to discover users who may be violating material support and other terrorism-related statutes, nor are they subject to criminal penalties for failure to abide by these internal compliance programs once created and approved by the Department of Justice. Instead of using the stick of a criminal conviction to force these companies to create the desired programs, this proposal uses the carrot approach—companies that institute such programs will receive significantly lower fines if they are then convicted of a terrorist-related offense. Federal prosecutors will also consider the existence of a robust compliance program in making charging decisions against social media companies. In essence, rather than creating a separate criminal offense, this proposal simply adds one new provision to U.S.S.G. Manual § 8B—new § 8B2.2—and amends a few existing provisions, current §§ 8C2.5(f) and 8D1.4(b)(1). These guideline provisions would be triggered only if a social media company was convicted or pled guilty to a terrorist offense, and would be employed as a sentencing factor to mitigate the penalty.

Corporations have been liable for federal criminal offenses committed by their agents acting within the real or apparent scope of their authority, and with intent, at least in part, to benefit the corporation, since the Supreme Court applied the tort law concept of *respondeat superior* to federal criminal law in a 1909 opinion.[170] Criminal liability may be imposed even if the criminal action is contrary to corporate policy.[171] Federal judges, calculating according to formulas contained in the Federal Sentencing Guideline's chapter on sentencing of organizations determine the corporate fine, in part, by how effective the corporate compliance program was, and whether the corporation self-reported and

---

[169] *Id.*

[170] New York Central & Hudson River R.R. Co. v. United States, 212 U.S. 481 (1909); 1 U.S.C. § 1 (as amended 1948) (defining words "whomever" and "person" within the meaning of any Act of Congress to include corporations). For a general description of the current doctrine of corporate criminal liability in federal criminal law, *see* ABRAMS, BEALE, & KLEIN, FEDERAL CRIMINAL LAW AND ITS ENFORCEMENT 519–600 (6th ed. 2015); U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL, Title 9, section 9-28.000, *Principles of Federal Prosecution of Business Organizations* (drafted in 1999, amended in 2003 by the Thompson memo, modified in 2006 by the McNulty memo, supplanted in 2008 by the Filip memo, and, most recently, clarified in 2015 by the Yates Memo), http://www.justice.gov/usao/eousa/foia_reading_room/usam/.

[171] *See, e.g.*, United States v. Hilton Hotels Corp., 467 F.2d 1000 (9th Cir. 1972). Federal courts have rejected the Model Penal Code's "due diligence" defense contained in section 2.07(5) (ALI 1962), as well as the MPC's requirement, laid out in sections 2.07(1)(a) and (c) that the corporation is vicariously liable only where senior corporate officers are at fault. However, federal judges working under the Federal Sentencing Guidelines will give steep sentencing discounts where the corporation instituted a compliance program designed to prevent criminal activity. *See also* U.S. SENTENCING GUIDELINES MANUAL, *infra* note 172.

cooperated with the prosecution.[172] Thus, those corporations that fail to institute such programs prior to misconduct by an agent are hammered at sentencing if convicted of a criminal offense.[173] Moreover, corporations without effective compliance programs are much less likely to persuade the prosecutor not to indict, or to be offered Non- or Deferred Prosecution Agreements.[174] This federal sentencing policy spawned a cottage industry of corporate compliance and internal investigation experts.[175] We would like to see this replicated in the anti-terrorism field with our second proposal.

The problem with using this method to achieve our goal, however, is that corporate management must first fear a prosecution before they will invest time and money in prophylactic behavior. At present, it appears unlikely that a social media company will be at risk of a criminal prosecution for providing material support based upon the conduct of its employees. Consider our example in footnote 10, *supra*—a Facebook user posts her plans to commit a terrorist attack in allegiance to ISIS on Facebook. For Facebook to be liable for this user's post, which arguably violates the material support statute, a Facebook agent would have had to have either posted the message or known that the user had posted it. Further, under principles of accomplice liability, the employee would also have to possess the requisite *mens rea* of the underlying offense (knowledge that she is supporting a FTO, for a charge pursuant to 18 U.S.C. section § 2339B), and must have either taken some affirmative action that assisted the perpetrator or failed in her duty to prevent the posting.[176] Finally, under the principles of *respondeat superior*, the prosecution would have to prove that the employee assisted the customer within the scope of his duties, and acted with the intent to benefit Facebook. That last requirement may prove the most difficult, as Facebook will

---

[172] *See* U.S. SENTENCING GUIDELINES MANUAL §§ 8C2.5(f)–(g) (2004). Chapter 8, concerning sentencing of organizations, was added to the FSG Manual in 1991, and the subsection on corporate compliance programs was added in 2004.

[173] For example, a financial institution convicted for a teller's failure to file currency transaction reports may be fined as little as $32,500 or as much as $2,600,000 depending upon whether it had an effective compliance program in place at the time of the withdrawal. *See* ABRAMS, BEALE, & KLEIN, *supra* note 170, at 568–69, note 2.

[174] *See* ABRAMS, BEALE, & KLEIN, *supra* note 170, at 1370–76; Memorandum from Deputy Attorney General Mark Filip to Heads of Department Components, United States Attorneys' Manual (Aug. 28, 2008).

[175] The explosion of corporation internal investigations actually began shortly after Upjohn Co. v. United States, 449 U.S. 383 (1981), when the Court protected a corporation's Sixth Amendment right to resist government efforts to secure the work product of its corporate counsel. The FSG policies of rewarding internal investigations that result in cooperation, and rewarding formal corporate compliance programs, has hugely increased the corporate investigation industry. *See, e.g.*, Julie R. O'Sullivan, *Does DOJ's Privilege Waiver Policy Threaten the Rationales Underlying the Attorney-Client Privilege and the Word Product Doctrine? A Preliminary "No,"* 43 AM. CRIM. L. REV. 1237 (2008).

[176] *See, e.g.*, 18 U.S.C. § 2 (providing that a principal is someone who "aids, abets, counsels, commands, induces, or procures" the commission of a federal offense); Model Penal Code § 2.06, AM. LAW. INST. (1985) (providing that a person is an accomplice if he solicited or aided an offense with the purpose of promoting it).

argue that it is the victim in such scenario, as it is not beneficial to a social media company to be associated with terrorists.[177]

On the other hand, some private actors have recently sued major social media companies for providing material support to foreign terrorist organizations through their agents, and these lawsuits have not been dismissed. In *Reynaldo Gonzalez v. Twitter, Inc., Google Inc., and Facebook, Inc.*, for example, a young woman killed in the November 2015 Paris massacre is claiming that the defendant social media companies provided material support to extremists in violation of 18 U.S.C. § 2333(a), a statute which allows private parties who are nationals of the United States to sue in federal district court and receive treble damages and attorney's fees if they were injured in their "person, property, or business by reason of international terrorism."[178] In particular, the plaintiff in *Gonzalez* alleges that the social media companies knowingly permitted the Islamic State to recruit members, raise money, and spread extremist propaganda via their social media services.[179] The underlying allegation in this matter is that the social media companies provided material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339(A). If this case is successful, federal prosecutors might be more inclined to charge these companies criminally, as the criminal case will not require proof of injury or proximate or actual causation.[180] Some well-known scholars have argued that by simply allowing Hamas to have an account, Twitter is violating the material support provision.[181] Thus, it appears to us not

---

[177] *See* Standard Oil Co. of Texas v. United States, 307 F.2d 120, 128–29 (5th Cir. 1962) (holding that corporation was victim of fraud by employees and thus not vicariously liable for their misconduct).

[178] 18 U.S.C. § 2333(a) (West 2016). *See also* 18 U.S.C. § 2331(1) (providing definition of "international terrorism") and 18 U.S.C. § 2339(b) (providing that any judgment in favor of the United States in certain criminal proceedings shall estop the defendant from denying the criminal offense in a subsequent civil proceeding).

[179] Gonzalez v. Twitter, Inc., No. 4:16-cv-03282-DMR (N.D. Cal. June 14, 2016). The case, as well as a similar case brought against Twitter in January 2015 by the widow of a contractor killed in an attack in Jordan, is summarized in: Benjamin Wittes, *Another Material Support Suit Against Social Media Companies*, LAWFARE (June 21, 2016), http://www.lawfareblog.com/another-material-support-suit-against-social-media-companies. *See also* Cain v. Twitter, No. 1:17-cv-00122 (S.D.N.Y. Jan. 8, 2017) (lawsuit against Twitter for damages pursuant 18 U.S.C. § 2333 for allowing Islamic State to flourish on the popular network ultimately leading to murder of New York man and his sister in a Belgium airport bombing).

[180] *See, e.g.*, Stanley Boim v. Holy Land Foundation for Relief and Development, 549 F.3d 685 (7th Cir. 2008) (en banc) (affirming judgment against two defendants and reversing and remanding against other two defendants to determine whether those defendants either knew or were reckless regarding whether their donations went to support the FTO called Hamas, a group whose members fatally shot the plaintiff's son, a U.S. national in Israel).

[181] This position has been described, though as a warning rather than a suggestion, in: David Cole, *Is Hamas's Twitter Account Illegal?*, THE DAILY BEAST (Nov. 20, 2012), www.thedailybeast.com/articles/2012/11/20/is-hamas-s-twitter-account-illegal. Professor Cole concedes in this article that Google, Facebook, and Verizon have arguably provided material support to Hamas. Benjamin Wittes, editor-in-chief of *Lawfare* and a Senior Fellow in Governance Studies at the Brookings Institution, believes that Twitter is violating 18 U.S.C. § 2339(B). *See* Benjamin Wittes and Zoe Bedell, *Tweeting Terrorists, Part II: Does it Violate the Law for Twitter to Let Terrorist Groups Have Accounts?*, LAWFARE (Feb. 14, 2016),

implausible that federal prosecutors, especially if more lone-wolf attacks are forthcoming, might begin charging social media companies.

Both of our proposals concern only public postings on social media sites. Neither mandates that a private entity like a social media company identify, read, and turn over private e-mails or oral communications between two customers who wish for that communication to remain private, nor that the social media companies provide the government with the code to encrypted private messages between two individuals. In both instances, the social media company will be identifying, monitoring, and revealing only potentially terroristic communications publicly posted on any Internet site.

We recommend that Congress adopt the first of our two proposals; we added the second proposal as a less effective, but more politically feasible, alternative. The first substantive criminal law proposal would be most appropriately placed at the end of Chapter 113B – Terrorism, currently codified at 18 U.S.C. §§ 2331–2339D. Such placement provides the most notice for the parties impacted. The second proposal would be best placed in Chapter 8 of the U.S. Sentencing Guidelines, governing the sentencing of organizations for violation of the federal criminal code. Federal judges turn first to Chapter 8 when sentencing entities like a social media company.

1. New Federal Crime: 18 U.S.C. § 2339E

We offer the following draft legislation:

18 U.S.C. § 2339E: Failure to Institute a Terrorist-Activity Discovery Program; Noncompliance With Dictates of Program:

(a) Offenses.—

(1) Whomever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce, intentionally, knowingly, recklessly, or negligently fails to institute an effective compliance program as described below in subsection (b) shall be punished as provided in subsection (d)(1).

(2) Whomever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce, intentionally, knowingly, recklessly, or negligently fails to comply with its effective compliance program as described below in subsection (b) shall be punished as provided in subsection (d)(2).

---

http://www.lawfareblog.com/tweeting-terrorists-part-ii-does-it-violate-law-twitter-let-terrorist-groups-have-accounts.

(b) Effective Compliance Program.—Each electronic communication service or remote computing service provider shall create its own compliance program, subject to review and approval by the Department of Justice.

(1) Such a program may include providing simple avenues for complaints by other users, word pattern recognition or keyword filtering software, grammar pattern recognition software, automated processing, Microsoft PhotoDNA software, and any other technology that most effectively and cost efficiently reveals users who may be conspiring to engage, attempting to engage, or engaging in any terrorism-related crime listed in 18 U.S.C. § 2332b(g)(5).

(2) The program shall additionally attempt to capture those posts that make contact with potential followers of terrorist groups and steer those followers off of social media to an encrypted form of communication, so that the appropriate law enforcement agency can then determine if it should seek a warrant or take any other appropriate action regarding the subsequent encrypted communications.

(c) Timing.—Providers have eight months from the date of the enactment of this provision to submit their programs to the Attorney General, the Deputy Attorney General, the Associate Attorney General, or any designated Assistant Attorney General or Deputy Assistant Attorney General for review. The Department has three months from submission to approve the program or state in writing what objections it has to such program, and what specific improvements must be made.

(d) Resolving disputes.—The U.S. Court of Appeals for the D.C. Circuit shall resolve all disputes between service providers and the Attorney General regarding the approval and scope of each compliance program. The court will approve the Attorney General's suggested revisions to each program if reasonable.

(e) Definitions.—

(1) In this section, the term "electronic communication service" has the meaning given that term in 18 U.S.C. § 2258E (regarding sexual exploitation and other abuse of children), which refers to 18 U.S.C.§ 2510(14). That section provides that "electronic communication service" means any service that provides users thereof the ability to send or receive wire or electronic communications.

(2) In this section, the term "remote computing service" has the meaning given that term in 18 U.S.C. § 2258E (regarding sexual exploitation and other abuse of children), which refers to 18 U.S.C. § 2711(2). That section provides that "remote computing service" means the

provision to the public of computer storage or processing services by means of an electronic communications system

(3) Both definitions exclude any companies with less than 15 full-time employees.

(f) Penalties.—

(1) Limitations:

(A) These provisions apply only to entities providing electronic communication services or remote computing services, not to any individual agents of such entities.

(B) These provisions apply only where the electronic communication service or remote computing service involves communication between one individual or entity and two or more distinct individuals or entities.

(2) Violation of subsection (a)(1) shall result in an initial fine of not more than $150,000 per offense. For each month beyond the eight months allowed for the creation of a model compliance program that the service provider fails to submit a program, there may be an additional fine of up to $300,000 per offense. Fines shall be tolled during any time that the Chief of the Section or the Attorney General is considering a submission. Fines shall be tolled during any time that a federal district judge is considering the reasonableness of the AG's modifications to such program.

(3) Violation of subsection (a)(2). In the case of an initial failure to comply with its effective monitoring program, a fine of not more than $150,000 per offense. For any second or subsequent failure to turn over information to the Department as required by its compliance program, a fine of not more than $300,000 per offense.

(g) Protection of privacy.—Nothing in this section shall be construed to prevent an electronic communication service provider or a remote computing service provider from—

(1) Monitoring any user, subscriber, or customer of that provider in conformity with the requirements of subsection (d)(1)(B);

(2) Monitoring the content of any communication of any person described in paragraph (11); or

(3) Affirmatively seeking information regarding the terrorism offenses listed in subsection (b) above.

(h) Limited liability for electronic communication service providers and remote computing service providers.—[182]

(1) Except as provided in subsection (2), a civil claim or criminal charge against an electronic communications service provider or a remote computing service provider, including any director, officer, employee, or agent of such provider rising from the creation of the compliance program or the reporting of users in fulfilling the dictations of the compliance program may not be brought in any Federal or State court.

(2) Intentional or other misconduct.—Subsection (1) shall not apply to a claim if the electronic communication service provider or remote computing service provider, or a director, officer, employee, or agent of that provider—

(A) Engaged in intentional misconduct; or

(B) Acted or failed to act with actual malice, or for a purpose unrelated to the performance of any responsibility or function under this section.

2. New Compliance Program: USSG Manual § 8B2.2

We offer the following amendments to the U.S. Sentencing Guidelines Manual, to be effective only if our new criminal offense is rejected. If our first proposal is enacted, making it a crime for social media companies to fail to institute an anti-terrorist compliance program, then the below sentencing mitigator for instituting the same program would be redundant.

The FSG, § 8B2.1, currently contains a test for determining whether a corporation convicted of a fraud offense had an effective compliance and ethics program in place in order to determine the culpability score of that corporation. The culpability score has a major impact on the amount of the fine imposed. We propose adding § 8B2.2, a test for determining whether a social media company has an effective terrorist-activity discovery program, for the same purpose.

[182] We intend this limitation of liability to protect social media companies who comply with our proposal from liability under 18 U.S.C. § 2520, part of the Title III Wiretap Act of 1968, which provides for civil damages for violation of the Wire and Electronic Communications Interception and Interception of Oral Communications. We further intend to exclude social media companies who comply from civil liability under that part of the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701(a), which prohibits providers of electronic communications services to the public from disclosing the contents, except to the government if it has warrant based upon probable cause). We do not believe anything other than subsection (h) is necessary to accomplish these goals.

USSG Manual § 8B2.2. Effective Terrorist-Activity Discovery Program:

(a) To have an effective terrorist-activity discovery program, for purposes of subsection (f) of § 8C2.5 (Culpability Score) and subsection (b)(1) of § 8D1.4 (recommended Conditions of Probation-Organization), a social media organization shall have instituted a Terrorist-Activity Discovery Program. [This program is identical to our first proposal, § 2339E(b)–(e). Due to space considerations, we will not reprint 2339E (a) through (e) here].

Second, we would amend §§ 8C2.5(f) and 8D1.4(b)(1). Section 8C2.5 is used to determine the culpability score of an entity, which is turn determines the level of fine it will pay as punishment for its crime. Subsection (f) of 8C2.5 adds or subtracts points to an entity's offense level depending upon the existence and effectiveness of its compliance and ethics program. We propose adding a new § 8C2.5(f)(4), which will accomplish the same effect on a social media company's offense level, depending upon the existence and effectiveness of its terrorist-activity discovery program.

USSG Manual § 8C2.5(f)(4). Effective terrorist-activity programs:

The requirements of subsections (1), (2), and (3) also apply where the entity has been charged with a terrorism offense, but the court shall substitute the phrase "effective terrorist-activity program" for the phrase "effective compliance and ethics program" throughout.

Additionally, we would amend current § 8C2.5(f) as follows:

U.S.S.C. Manual § 8C2.5(f): Add the phrase "or effective terrorist-activity program" after every mention of "effective compliance and ethics program" throughout.

Finally, we would amend § 8D1.4(b)(1), which currently requires that an organization develop and submit to the court an effective compliance and ethics program as part of the conditions of probation. We would add to § 8D1.4(b)(1) the requirement that social media companies implement an effective terrorist-discovery program as part of any probation, as follows:

U.S.S.C. Manual § 8D1.4(b)(1): Add the phrase "or effective terrorist-activity program" after the phrase "effective compliance and ethics program."

C. *Precedents for Our Proposals*

While some may view these proposals as extreme, we believe there is substantial precedent in existence that deserves comparison. We offer first a couple of U.S. laws that are similar to our proposals, and second a couple of foreign precedents that resemble what we suggest in our first proposal. The UK

government has also recently passed a very similar and extremely expansive requirement for Internet providers, the Investigatory Powers Bill, that requires data recording and decryption for government use and allows government hacking on the Internet, although this law is too new to discuss in much detail.[183]

1. The Bank Secrecy Act

The Bank Secrecy Act of 1970 required the reporting of large cash transactions by financial institutions.[184] In the mid-1980s, Congress created the new crime of structuring a financial transaction to avoid the reporting laws,[185] two money laundering offenses,[186] and a provision requiring individuals engaged in trade or business (including lawyers) to report the receipt of cash payments in excess of $10,000.[187] The USA PATRIOT Act in 2001 expanded the list of predicate crimes for money laundering offenses (to include foreign crimes, operation of an illegal money remission business, and bulk cash smuggling) and, more importantly for our purposes, required financial institutions to take further precautions when dealing with foreign countries or institutions considered to be of primary money laundering concern.[188] While these statutes were originally enacted to take the profit out of organized crime and drug trafficking, there was a paradigm shift after September 11, 2001, and most of the amendments since that time were designed to track terrorist financing.[189]

---

[183] *See* Zack Whittaker, *Britain has passed the 'most extreme surveillance law ever passed in a democracy'*, ZERO DAY (Nov. 17, 2016), http://www.zdnet.com/article/snoopers-charter-expansive-new-spying-powers-becomes-law/ ("The law will force internet providers to record every internet customer's top-level web history in real-time for up to a year, which can be accessed by numerous government departments; force companies to decrypt data on demand -- though the government has never been that clear on exactly how it forces foreign firms to do that that; and even disclose any new security features in products before they launch. Not only that, the law also gives the intelligence agencies the power to hack into computers and devices of citizens (known as equipment interference), although some protected professions -- such as journalists and medical staff -- are layered with marginally better protections.").

[184] 31 U.S.C. §§ 5311–22. This initially required financial institutions to report any cash transaction over $5,000, and was later raised to over $10,000 by an amendment contained in the Comprehensive Crime Control Act of 1984.

[185] 31 U.S.C. § 5324. This is a five-year felony, plus fines of up to $500,000 or twice the value of the property in question.

[186] 18 U.S.C. § 1956 and 18 U.S.C. § 1957. These are 20-year and 10-year felonies, respectively.

[187] 26 U.S.C. § 6050I. This is a five-year felony under the tax code.

[188] USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat, 192, 225 (2006), codified at 21 U.S.C. § 960a. This expanded forfeiture beyond what was mandated under 18 U.S.C. §982(a) (providing that the sentencing of any person convicted under the currency reporting or bank secrecy laws "shall order that the person forfeit to the United States any property, real or personal, involved in such offense or any property traceable to such property") and its parallel civil provision, 18 U.S.C. § 981(a) (providing for civil forfeiture of any property "involved in" the offenses in question). The PATRIOT Act allows civil forfeiture of all assets of any person, entity, or property engaged in terrorism.

[189] *See, e.g.*, Amos N. Guiora & Brian J. Field, *Using and Abusing the Financial Markets: Money Laundering as the Achilles' Heel of Terrorism*, 29 U. PA. J. INT'L L. 59, 61–64 (2007); ABRAMS, BEALE, & KLEIN, *supra* note 170, at 602–09.

The currency reporting statute makes it a criminal offense for a financial institution or any individual businessperson to fail to file a Currency Transaction Report (CTR) with the IRS and the Treasury Department's Financial Crimes Enforcement Network concerning the receipt or withdrawal of cash in excess of $10,000, regardless of whether this cash is clean or dirty. The statute goes further, however, in corralling financial institutions into law enforcement (as does our first proposal). Beginning in 1996, banks were required to file a new form, the Suspicious Activity Report (SAR). In contrast to the CTR, which requires reporting only when a certain dollar threshold has been met, the SAR requires financial institutions to identify and report particular "suspicious" transactions to the authorities regardless of dollar amount, "effectively conscripting these institutions into the government's investigative team."[190] In 2001, Congress imposed an additional requirement, referred to colloquially as "know your customer" regulations.[191]

As noted above, the USA PATRIOT Act of 2001 directed the Treasury Secretary to promulgate "know your customer" regulations requiring financial institutions to develop and implement reasonable procedures for verifying the identity of persons opening an account, "maintaining records of the information used to verify a person's identity," and determining whether a person appears on any "lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any governmental agency."[192] While prosecutions have not been many, there have been a few high profile prosecutions against major banks for failing to report highly suspicious cash transactions in overseas accounts.[193] When the goal is to deter risk-averse bankers, it does not take much law enforcement presence to trigger a response.

For a few years, it appeared that forcing bankers to be police officers was actually counterproductive; financial institutions were filing large numbers of unnecessary SARs, submitting 1.5 million in 2012 (an increase of over 300 percent).[194] Such defensive filings diluted the value of the information being reported, and implicated privacy concerns. In June 2005, federal regulators responded by publishing anti-money laundering guidelines intended to reduce defensive SAR filings. But it was technology that saved the day. Banks now have

---

[190] ABRAMS, BEALE, & KLEIN, *supra* note 170, at 608.
[191] *Id.*
[192] 31 U.S.C. § 5318(l)(1)(A)–(C).
[193] An illustrative example is the January 2005 prosecution of Riggs Bank in Washington, D.C. for failing to report suspicious cash transactions in the accounts of the Saudi Arabian embassy and foreign dictators. Riggs Bank agreed to pay a $16 million fine and to plead guilty to one count of failure to report suspicious activity. In 2004, AmSouth Bank was investigated for failing to detect suspicions that two of its customers were using their accounts as part of a scheme that defrauded more than 60 investors of millions of dollars. It entered into a deferred prosecution agreement, and paid $40 million in civil forfeitures. HSBC Bank pled guilty of violating 18 U.S.C. §§ 5318(h) and 5322 by failing to implement an effective anti-money laundering program and conduct adequate due diligence on foreign correspondent bank accounts between 2006 and 2010. Trial Pleadings, United States v. HSBC Bank USA, 2012 WL 6120591 (E.D.N.Y. 2012).
[194] ABRAMS, BEALE, & KLEIN, *supra* note 170, at 609.

software that identifies potentially suspicious activity, which bank employees then investigate in order to decide whether to file a SAR. FinCen has also developed data-mining capabilities that enable SARs to be linked into a central system once they have been filed, so agents are not reading though millions of such filings.

Our new federal statute, 18 U.S.C. § 2339E, will act much like 31 U.S.C. § 5318(l)(2)(A)–(C). Social media companies will be required to create and implement programs to determine which customers are violating federal terrorism proscriptions. They will have incentive to limit the number of posts they turn over to federal law enforcement personnel, both to save themselves time and to limit the appearance of privacy infringement.

A second domestic precedent is the Foreign Corrupt Practices Act, enacted in 1977 after an SEC report in which 400 U.S. companies admitted paying over $300 million in bribes to foreign officials.[195] Some scholars criticize the statute on the grounds that the Act punishes companies that voluntarily disclose their bribes.[196] Our proposal to require social media companies to merely monitor their users for violations of federal law is significantly tamer than the FCPA, as complying with the proposal will not subject the companies to criminal penalties.

2. The UK Bribery Act and Current International Copyright Law

The UK Bribery Act of 2010, which came into force in July 2011, was introduced to address foreign and domestic bribery and to meet the requirements of the 1997 Office for Economic Co-Operation and Development anti-bribery Convention.[197] The Bribery Act creates a strict liability offense[198] for companies that fail to prevent bribery, as well as for companies that act on behalf of businesses with a presence in the UK, regardless of where the activity has taken place.[199] In addition, the Bribery Act creates a corporate criminal offense, requiring a company to show that it has adequate procedures in place to prevent bribery.[200] Under the UK's Bribery Act, a company would incur strict penalties

---

[195] The FCPA is codified at 15 U.S.C. §§ 78dd-1 through 78dd-3, and is enforced by the DOJ (for criminal prosecutions) and the SEC (for civil ones). *See A Resource Guide to the U.S. Foreign Corrupt Practices Act*, U.S. DEP'T OF JUSTICE (Nov. 2012), http://www.justice.gov/criminal/fraud/fcpa/guide.pdf; FCPA BLOG, http://www.fcpablog.com/.

[196] *See, e.g.*, Bruce W. Klaw, *A New Strategy for Preventing Bribery and Extortion in International Business*, 49 HARV. J. ON LEGIS. 303 (2002).

[197] *United Kingdom: Phase 2 - Report on the Application of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and the 1997 Recommendation on Combating Bribery in International Business Transactions*, ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT at ¶ 248 (Mar. 17, 2005), https://www.oecd.org/daf/anti-bribery/anti-briberyconvention/34599062.pdf.

[198] In a strict liability crime, an offense may be criminal even if the company does not have knowledge of all of the relevant factors. *See* BLACK'S LAW DICTIONARY 111 (10th ed. 2014).

[199] The United Kingdom Bribery Act 2010, c. 23 (Eng.), http://www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf.

[200] *Id.*

for both "active"[201] and "passive"[202] bribery by individuals and companies.[203] If convicted of an offense under the Bribery Act, individuals can be charged to imprisonment for a maximum of 10 years per offense, and may not participate in tenders for public contracts for works, supply, or services in the European Union.[204] In addition, companies could face unlimited fines for convictions under the Act.[205]

The Bribery Act has extraterritorial reach for UK companies operating abroad and for overseas companies with a presence in the UK.[206] Like our proposal in Section II(B)(2), the UK Bribery Act includes a defense that the company "had adequate procedures in place which were designed to prevent bribery by people associated with the organization."[207] Although only courts can determine what procedures will be deemed adequate for purposes of the Bribery Act, the principles examined in determining the adequacy of the program include proportionate procedures, top-level commitment, risk assessment, due diligence, communication and training, and monitoring and review.[208]

The main differences between the UK Bribery Act and the U.S. Foreign Corrupt Practices Act, briefly mentioned in Section II(C)(1), above, is that the scope of the Bribery Act is materially different, encompassing more activities than the FCPA and allowing fewer defenses. For example, there is no provision in the FCPA "equivalent to the Bribery Act offence of failure to prevent bribery."[209] Moreover, the FCPA defenses "that the payments made were reasonable and bona fide business expenses" and exceptions to facilitation payments "made to foreign officials to speed up or secure the performance of routine governmental action" do not exist under the Bribery Act.[210] Finally, the Bribery Act encompasses the public and private divide and includes all commercial activities--not restricting the criminal bribery to foreign public officials.[211] The failure to prevent bribery is not criminalized in the U.S. Foreign Corrupt Practices Act.

Despite the few prosecutions under the UK Bribery Act, public awareness of the Act has led to a change in corporate compliance standards: "In many cases, non-US companies have put in place an anti-corruption programme for the first

---

[201] "Active" bribery refers to bribes being given to others by a company or its representative or agent. *A Glossary of International Standards in Criminal Law*, ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT at 12 (2008).
[202] "Passive" bribery refers to bribes received by the company from another. *Id*.
[203] United Kingdom Bribery Act 2010, c. 23.
[204] Geoffrey Gauci & Jessica Fisher, *The UK Bribery Act and the US FCPA: The Key Differences*, ASSOCIATION OF CORPORATE COUNSEL (June 1, 2011), http://www.acc.com/legalresources/quickcounsel/UKBAFCPA.cfm.
[205] The United Kingdom Bribery Act 2010, c. 23 sec. 11.
[206] *Id.* at c. 23.
[207] Gauci & Fisher, *supra* note 204.
[208] *Id*.
[209] *Id.*
[210] *Id.*
[211] *Id.*

time.[212] Importantly, private industries operating from the UK recognize that "in order to ensure the UK's anti-bribery system is proportionate and effective, an ongoing dialogue between the Government, regulators and the private sector will be essential."[213] The readiness of private companies to work with the government, in international anti-bribery as well as international counterterrorism efforts, is essential to combatting a recognized public harm.[214]

Another analogy for our first proposal is the move under international copyright law to remove infringing Internet content. A request to limit the freedom of information available on the Internet is simply not a radical or new idea. Internet search engines, service providers, and other sites currently edit the Internet in order to adhere to copyright laws.[215] For example, the Digital Millennium Copyright Act[216] is frequently invoked by search engines in the removal of content that is suspected of violating the Act.[217] The Digital Millennium Copyright Act criminalizes the production and dissemination of devices, technology, and services that intend to circumvent measures controlling access to copyrighted works.[218] Users can file complaints with the search engine, and the search engine can then block the content and decide to litigate a copyright infringement.[219] Some search engines, such as Google, also reserve the right to terminate the accounts of users with multiple copyright infringement violations.[220]

Copyright law, however, is rapidly changing to enable a more comprehensively restrictive regime. With the signature of the Trans-Pacific Partnership[221] in 2016, the United States expressed commitment to the international community to a copyright regime that requires "providers of Internet access and providers of services on the Internet . . . to help police copyright infringement if they see it happening."[222] In this new free trade treaty's

---

[212] Barry Vitou, *Five years on the Bribery Act has led to a 'step-change' in anti-bribery compliance standard, says expert*, OUT-LAW.COM (Apr. 21, 2015), http://www.out-law.com/en/articles/2015/april/five-years-ofn-the-bribery-act-has-led-to--a-step-change-in-anti-bribery-compliance-standards-says-expert/.

[213] British Bankers' Association, Anti-Bribery and Corruption Guidance at 3 (2014).

[214] Bobbitt, *supra* note 84, at 419 (discussing the cooperation necessary in the public and private sectors in combatting terror).

[215] *See generally* COPYRIGHT ENFORCEMENT AND THE INTERNET (Irini A. Stamatoudi, ed., 2010).

[216] Digital Millennium Copyright Act, *supra* note 18.

[217] *Id; see also* David Jones, *Social Media Firms Face Quandary Over Terror Prevention*, TECH NEWS WORLD (Dec. 8, 2015), http://www.technewsworld.com/story/82845.html.

[218] Digital Millennium Copyright Act, *supra* note 18.

[219] *Id.*

[220] *Id.*

[221] The Trans-Pacific Partnership Agreement is a comprehensive free trade agreement between New Zealand, Japan, the United States, Australia, Malaysia, Mexico, Peru, Singapore, Vietnam, Chile, Canada, and Brunei. The United States has signed the Agreement but it has not yet been entered into domestic U.S. law. The Trans-Pacific Partnership (signed Oct. 4, 2015), https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text.

[222] Abigail Abrams, *Intellectual Property Law: Why Internet Freedom Groups Don't Like TPP Trade Agreement*, INT'L BUSINESS TIMES (Nov. 5, 2015), http://www.ibtimes.com/trans-pacific-partnership-intellectual-property-law-why-internet-freedom-groups-dont-2171936.

intellectual property chapter, companies operating on the Internet are required to remove copies of copyright infringing material, as well as search results to the material, if a complaint of copyright infringement is made or if the company becomes aware of material that infringes the copyright requirements of the Treaty.[223] Combined with the investor-State dispute settlement provisions in the Treaty, State signatories to the Treaty could be held liable if a company "believed the country's laws harmed its right to use its copyright interests."[224]

The expectation and requirement for private companies to work with the government to address copyright law is reasonable according to the twelve major countries that are signatories to the Trans-Pacific Partnership Agreement. In this regard, the expectation for private companies to work with the government to address potential terror threats is reasonable, and even less restrictive to First Amendment freedoms of speech than the requirements of the Trans-Pacific Partnership.

III. Our Proposals Are Constitutional

The current U.S. counterterrorism strategy for addressing terrorist activity online is desperately in need of a new approach, and our proposals offer a way forward. Although there are understandable constitutional concerns about these proposals, it is ultimately clear to us that our proposals are both constitutional.

A. *Privacy and the First Amendment are not Bars to Implementation*

Measures that potentially restrict information on the Internet arguably implicate the First Amendment.[225] However, we do not find potential arguments against the proposed reporting requirements from ISPs and social media sites persuasive. ISPs and social media sites are operated by private companies, not governmental bodies against which individuals can claim constitutional violations. While this argument is tempered by the fact that the private companies may turn over communications pursuant to a government mandate, users always have the choice not to log on through these companies, or to use them for private but not public postings. Furthermore, existing Internet and social media provider policies claim to address the proposals in the prior section, even if only to a limited and cherry-picked degree. If it is indeed true that "Facebook's policy is to pass on information to law enforcement as soon as it becomes aware of any planned attack or threat of imminent harm," then the legislation proposed here should not cause protest from the social media company, as it would fit within existing operating norms.[226] Because companies claim to censor terroristic content already, the proposals here would not impose additional harm to privacy interests.

---

[223] *Id.*
[224] *Id.*
[225] U.S. CONST. amend. I.
[226] David Jones, *Social Media Firms Face Quandary Over Terror Prevention*, TECH NEWS WORLD (Dec. 8, 2015), http://www.technewsworld.com/story/82845.html.

While private censorship is permissible under the First Amendment, censorship is not permissible if it is done by or as a stand-in for the government. However, the freedom of speech is not absolute and has been limited in several areas, including child pornography,[227] copyright law,[228] slander,[229] obscenity,[230] protection from imminent or potential violence,[231] and incitement to imminent lawless action.[232] Moreover, there is no First Amendment interest in failing to report criminal activity; thus the Bank Secrecy Act and the FCPA have not been challenged on First Amendment grounds. The material support statutes, which criminalize material support to terror organizations, have been attacked in the past—unsuccessfully—as inhibitions of First Amendment rights.[233] These First Amendment concerns can be grouped into two main issues: privacy concerns and restrictions on the freedom of speech.

Regarding privacy rights,[234] the scope of the proposals in this Article reaches to open-source content only.[235] Open-source data, including data mining,

---

[227] United States v. Williams, 553 U.S. 285 (2008).
[228] Golan v. Holder, 565 U.S. 302 (2012).
[229] N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964); Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974).
[230] Miller v. California, 413 U.S. 15 (1973).
[231] Whitney v. California, 274 U.S. 357 (1927).
[232] Brandenberg v. Ohio, 395 U.S. 444 (1969).
[233] Emily Goldberg Knox, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L. J. 295, 323–24 (2014) (arguing that the application of the material support statute to social media companies should be construed "in a way that does not infringe upon rights protected by the First Amendment" and that social media companies should have a First Amendment defense to material support prosecutions); Sam Adelsberg, Freya Pitts, & Sirine Shebaya, *The Chilling Effect of the "Material Support" Law on Humanitarian Aid: Causes, Consequences, and Proposed Reforms*, 4 HARV. NAT'L SEC. J. 282 (2013) (arguing that the material support statute has had a greater impact on humanitarian aid organizations than the small number of prosecutions might suggest because it has led some organizations to reconsider providing humanitarian aid, particularly in war-torn areas where terrorist organizations are active); Allen F. Williams, *Prosecuting Website Development Under the Material Support to Terrorism Statutes: A time to Fix What's Broken*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 365 (2007–2008) (asserting that "the material support statutes are inadequate for prosecuting … Internet activities" due to First Amendment concerns and suggesting that new federal criminal legislation is needed to address the extensive and alarming use of the Internet by terrorist organizations). *But see* Crystal M. Flinn, *As Support Materializes: An Examination of Contemporary Policy in the Prosecution Under the Material Support Statutes during the Current Wave of Terrorism*, 5 HOMELAND & NATIONAL SEC. L. REV. 79, 84 (2016) (discussing First Amendment opposition to the material support statutes focusing on the freedom of speech and protection of privacy rights and concluding that "[a]llowing social media companies to project a First Amendment defense if prosecuted under the material support statutes would give the terror organizations the legitimacy they desire, fails to guard against gaping holes in national security, and fails to recognize the inherently violent goals and incitements that [Foreign Terrorist Organizations] and their members project online."); Ashutosh Bhagwat, *Terrorism and Associations*, 63 EMORY L. J. 581 (2014) (concluding that material support statutes do not violate the First Amendment's right to freedom of association because that right protects only a right "peaceably to assemble" and so excludes violent groups like terrorists).
[234] We discuss privacy concerns related to the Fourth Amendment in the subsection above.

is permissibly obtained by the U.S. government for national security purposes and has been collected to "track down criminals and terrorists," as well as to track and analyze money flows.[236] Furthermore, persons do not have a legitimate expectation of privacy in records that were voluntarily conveyed to a third party[237] or made public.[238] This lack of reasonable expectation of privacy applies to all public postings, but perhaps not e-mails directed towards a single individual. In those cases, which are not covered by our proposal, the individual probably does have a cognizable privacy interest.[239] We believe that there are no privacy right violations possible because the scope of our proposals reaches solely open-source content. We do recognize, however, that there may be over-reporting by social media companies, which would cause unnecessary expense and would bring some posts to the government's attention for no good reason. Ultimately, any privacy lost is not privacy that is constitutionally protected. We must determine as a society whether law enforcement investigation of public and potentially dangerous postings is worth the cost.

Furthermore, the type of activity encompassed by the proposed reporting requirements is not protected by the First Amendment. In the face of First Amendment challenges, the Supreme Court in *Holder v. Humanitarian Law Project* upheld the criminalization of advocacy in the form of legal support, training for mediation, and negotiating peace agreements on behalf of or in coordination with designated foreign terrorist organizations.[240] *Holder* involved an unsuccessful First Amendment challenge to the validity of the material support statutes by U.S. citizens and domestic aid organizations who had previously provided training to members of two designated foreign terrorist organizations[241] to (in relevant part) resolve disputes peacefully using international law, petition the United Nations for relief, and engage in political advocacy on behalf of these groups.[242] The Supreme Court upheld the constitutionality of potential prosecutions under the material support statutes, even under the strict scrutiny standard applied to content-based speech restrictions.[243] Regarding freedom of speech, the Court noted that "under the material support statute, [a person] may

---

[235] Here, we refer to open-source content as works that are freely available and can be accessed by the general public. While our proposal does not cover encrypted information, we believe it could be easily amended to cover encrypted posts or other online information.

[236] JOHN YOO, WAR BY OTHER MEANS: AN INSIDER'S ACCOUNT OF THE WAR ON TERROR 108 (2006).

[237] Smith v. Maryland, 442 U.S. 735 (1979).

[238] California v. Greenwood, 486 U.S. 35 (1988).

[239] The fact that a person is merely using an Internet service probably does not free the government of its First Amendment obligations, just as using the phone company does not mean an individual allows the government to listen in on phone calls. *See* Katz v. United States, 389 U.S. 347, 352 (1967); *see also infra* notes 289–91.

[240] Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2722–32 (2010).

[241] Namely, the Partiya Karkeran Kurdistan (PKK) and Liberation Tigers of Tamil Eelam (LTTE). Both groups engaged in political and humanitarian activities, but also had committed numerous terrorist attacks. *Id.* at 2713.

[242] *Id.* at 2714–16.

[243] *Id.* at 2724–26.

say anything they wish on any topic."[244] The Court differentiated "pure political speech," which is not forbidden by the material support statutes, from "'material support,' which most often does not take the form of speech at all" and is narrowly drawn to cover speech under the direction of or in coordination with FTOs.[245]

Cases like *Holder* that uphold the potential to convict offenders for acts that "in other circumstances might have been understood as protected speech" are evidence "of a global move that seeks to limit speech that supports terrorism, terrorist acts, or terrorist organizations."[246] *U.S. v. Mehanna* is a prime example of the acknowledgement of the potential constitutional First Amendment clash with the efforts to fight terrorism, here described as "an existential threat" and "the modern-day equivalent of the bubonic plague."[247] *Mehanna* affirmed the conviction of an accountant on several counts of material support charges relating to his travel to Yemen in an unfruitful search for a terror training camp as well as his translation of documents from Arabic to English, which he then posted online for a community "for those sympathetic to al-Qaida and Salafi-Jihadi perspectives."[248] Regarding his material support charges, the court noted that 18 U.S.C. § 2339B does not require "[a] specific intent to advance the organization's terrorist activities."[249] The defendant argued that the evidence on the record only showed activity protected by the First Amendment, such as "discussing politics and religion, consuming media related to those topics, and associating with certain individuals and groups."[250] However, the court found that the jury's inference against the categorization of the evidence as mere political speech was permissible, and indeed, that it was "virtually unarguable that rational jurors could find that the defendant and his associates went abroad to enlist in a terrorist training camp."[251]

Moreover, the court completely quashed the defendant's First Amendment arguments, determining that speech made "in coordination with foreign groups

---

[244] *Id.* at 2710.
[245] *Id.* at 2723.
[246] Daphne Barak-Erez & David Scharia, *Freedom of Speech, Support for Terrorism, and the Challenge of Global Constitutional Law*, 2 HARV. NAT'L SEC. J. 1, 3 (2011). We recognize that *Holder* was a case where plaintiffs requested injunctive relief; it was not a criminal prosecution.
[247] United States v. Mehanna, 735 F.3d 32, 40 (2013), *cert. denied*, 135 S.Ct. 49 (2014).
[248] *Id.* at 41.
[249] *Id.* at 42. The court further noted that charges under 18 U.S.C. § 2339A require proof "that the defendant had the specific intent to provide material support, knowing or intending that it would be used in a conspiracy to kill persons abroad." *Id.* at 43. The proposals in this Article are much more akin to a § 2339B charge, which would not require proof of a specific intent to advance a terrorist group's activities.
[250] *Id.* at 44. The evidence against the defendant included co-conspirator testimony that he "persistently stated his belief that engaging in jihad was 'a duty upon a Muslim if he's capable of performing it,'" that he believed America was at war with Islam and that American soldiers were "valid targets," that he expressed interest in receiving military-type training to participate in jihad, and that he "wished to engage in jihad if he 'ever had the chance.'" *Id.*
[251] *Id.*

that the speaker knows to be terrorist organizations" "is not protected" under the Constitution,[252] and that "a direct link [to the foreign terrorist organization] is neither required by statute nor mandated by [*Holder*'s analysis of the material support statutes in light of First Amendment law]."[253] This expounding on the holding in *Holder* suggests an unwillingness to allow a defendant to escape conviction on First Amendment grounds in light of the severity of potential harm in providing support to terrorist organizations. More importantly, the proposal in this Article does not convict individuals or even charge them. In the few instances where a prosecution might be brought, only a jury could find beyond a reasonable doubt that the individual provided material support to an FTO through the defendant's postings.

More recently, a district court upheld the detention of a man charged under the material support statutes for tweeting support to ISIS "an organization whose brutality is shocking even by the standards of terrorism,"[254] for maintaining "direct communications with persons involved with such organization," and for attempting to travel to join ISIS.[255] The Court held that while the defendant "may enjoy rights under the First Amendment," these rights were not violated by the government's use of his "comments on twitter as evidence of intent or motive" to provide material support to a foreign terrorist organization.[256] The court also further elaborated the mental state required for material support convictions, stating that "only individuals who act entirely independently of a terrorist organization may avoid prosecution" under the material support statutes—"[t]here is no requirement that the recruitment . . . be done at the terrorist organization's direction or control, only that the personnel provided to the organization eventually acts under that organization's direction or control."[257]

Likewise, a court would not find our proposals invalid as impermissibly vague. In *United States v. Farhane*, the Second Circuit upheld the conviction of a New York doctor for his interest in and agreement to meet with terrorists operating in Saudi Arabia to provide medical assistance to any who were wounded.[258] Responding to a challenge that the material support statutes were unconstitutionally vague or overbroad, the Court relied heavily on the language in *Holder v. Humanitarian Law Project*, reiterating that "the statute is carefully drawn to cover only a narrow category of speech to, under the direction of, or in coordination with foreign groups that the speaker knows to be terrorist organizations."[259] Regarding the accusation that the material support statute was overbroad, the Court ruled that proof of "the knowing provision, [whether actual, attempted, or conspiratorial], of material support to a known terrorist organization

---

[252] *Id.* at 49.
[253] *Id.* at 50.
[254] United States v. Ahmed, 107 F. Supp. 3d 1002, 1005 (D. Minn. 2015).
[255] *Id.* at 1007.
[256] *Id.* at 1006–07.
[257] *Id.* at 1006.
[258] United States v. Farhane, 634 F.3d 127, 133 (2d Cir. 2011).
[259] *Id.* at 137 (citing *Holder*).

. . . together with the dual knowledge elements of the statute is sufficient to satisfy the personal guilt requirement of due process."[260] In addition, the Second Circuit determined that when a terror organization's "history for using murderous terrorism" is "so well known that no reasonable person could doubt that [an action] . . . is precisely the sort of material support proscribed by the material support statute," the statute is not vague as applied in the conviction of that activity.[261]

We fully recognize, however, that people may be unwilling or afraid to publicly post communications which turn out not to provide material support to a foreign terrorist organization, but are still flagged by the social media company's compliance program and revealed to government investigators. The possibility of a chilling effect will surely be pushed by those lobbying against our proposals. The difficulty, then, lies in the fact that the line between protected speech and the pledge to support terror may be subjective and difficult to draw. Recently, Israel has begun a string of arrests of people charged with inciting violence, some of them based on the content of their social media posts. Most of these cases involve posts that support the recent upsurge of violence by the Palestinian uprising in the West Bank.[262] While opposition to incitement laws are rooted in a freedom of expression argument, even a prominent legal rights group admits that "some investigations into incitement are justified."[263] It is important to note that the Israeli judicial system does not have a lay jury; those convicted of incitement do not have the trial by jury available in the United States, but are instead tried in military courts.[264] However, in the United States, the jury is an appropriate way of checking for abuse of discretion—indeed, in *Mehanna*, the court often noted its deference to the jury's factual decisions in the trial court.[265] It was, after all, the jury that received the presented evidence, and the jury determining that it was beyond a reasonable doubt that the defendant's behavior was illegal and presented an unacceptable risk. Here, assuming the FBI finds any postings through our proposal that arguably qualify as material support to a FTO, a federal prosecutor

---

[260] *Id.* at 138.
[261] *Id*. at 140.
[262] Tia Goldenberg, *Israel takes on Facebook to stop incitement to violence*, ASSOCIATED PRESS (July 21, 2016), http://bigstory.ap.org/article/e08f5c12f80143f986c02df2e45c1dec/israel-takes-facebook-battle-against-incitement (describing Israel's new "Facebook Law" and discussing the numerous recent arrests for incitement).

While Israel does not have the freedom of speech memorialized in its constitution (and indeed, does not have a constitutional basis for its legal regime), its "law provides for freedom of speech and of the press, and the government generally respected these rights in practice subject to restrictions concerning security issues. The law prohibits hate speech and incitement to violence, and the 1948 Prevention of Terrorism Ordinance prohibits expressing support for illegal or terrorist organizations." *2005 Country Reports on Human Rights Practices: Israel and the occupied territories*, U.S. DEP'T OF STATE, BUREAU of DEMOCRACY, HUMAN RIGHTS, AND LABOR (Mar. 8, 2006), http://www.state.gov/j/drl/rls/hrrpt/2005/61690.htm; Steven J. Colby, *A Jury for Israel?: Determining When a Lay Jury System is Ideal in a Heterogeneous Country*, 47 CORNELL INT'L L.J. 122, 126 (2014).
[263] Goldenberg, *supra* note 262.
[264] Colby, *supra* note 262, at 126–29.
[265] United States v. Mehanna, *supra* note 247.

and a grand jury must then decide that a federal criminal charge is warranted in order to move ahead with a criminal case. Only at that point would the government present the available evidence, including evidence based on the defendant's public activity on social media sites, to a jury. And only after a jury finds beyond a reasonable doubt that a defendant knowingly assisted a FTO can punishment be imposed.

Our proposal may also be compared to Israel's proposed "Facebook Law," which would allow authorities to apply for court orders to demand that social media networks remove certain online content upon pain of fines.[266] Allowing for the government to remove social media content is a slightly different approach than what we propose. We do not advocate prior restraint of speech, nor would we fine Internet providers for failing to remove postings. Their role is limited to passing information about potential criminal offenses on to the government. Such information is, as we have emphasized, already made public by the speaker.

Internet pages that support terror activity may well facilitate and encourage violence against groups of people, including American citizens. This reasoning prompted Senator Feinstein's bill, as well as a civil lawsuit by a group of Israelis against Facebook.[267] As briefly mentioned above, speech that involves incitement to imminent lawless action (a category which terror activity would undoubtedly fit into) is not covered by First Amendment protections. The holding in *Mehanna* explicitly notes that speech covered in the material support statutes is not constitutionally protected; arguments against material support convictions that are based in the First Amendment have been rejected. Therefore, even if the proposed reporting requirements are seen as a restriction on the freedom of speech, they are justified by essential national interests in security and procedural prophylactics are appropriately applied in the U.S. judicial system and the jury trial. Likewise, the proposed requirements are further supported by an international trend toward the criminalization of involvement in online terror activity and support.[268]

---

[266] Goldenberg, *supra* note 262.

[267] Harriet Salem, *Facebook Is Being Sued by 20,000 Israelis for Inciting Palestinian Terror*, VICE NEWS (Oct. 27, 2015), https://news.vice.com/article/facebook-is-being-sued-by-20000-israelis-for-inciting-palestinian-terror (discussing a case filed in the Southern District of New York against Facebook for facilitating connections using algorithms for "like-minded people who share common groups or hashtags such as 'Stab' and 'Knife Intifada'" and inciting violence in the "thousands of posts endorsing [terrorist] acts, glorifying it, and encouraging others to follow them").

[268] *See, e.g.*, Flinn, supra note 233 ("A look to notable domestic statutes, such as the anti-bribery and corruption mandates in the FCPA, as well as international law precedents, such as the International Criminal Court's rulings against individuals and companies related to the genocides in Nazi Germany, demonstrates a willingness and precedent towards strict accountability even for minor actors caught within the fringe of the hub of malignant criminal activity.").

B. *The Fourth Amendment is not a Bar to Implementation*

Our specific proposals do not violate any Fourth Amendment prohibitions. Since both proposals target only publicly viewable wall postings and similar shared content, rather than e-mails or other communications between two individuals, they avoid Fourth Amendment inquiries concerns.[269] The Fourth Amendment protects against unreasonable searches and seizures (those done without probable cause and a warrant or a warrant exception) of persons, places, and things.[270] This was famously applied to a case regarding a conversation a defendant had with anther individual from a public telephone booth: the government, even with probable cause, must obtain a warrant before it can listen to and/or record this conversation where neither party to the conversation agreed to the government's intrusion.[271] However, our proposal does not require that social media companies identify, read, or submit e-mails or oral communications between two customers who both wish that conversation to remain private. Our first proposal, the new federal offense of Failure to Institute a Terrorist-Activity Discovery Program, allows a private company and eventually the government to obtain and read communications only where such communications are publicly posted. Likewise, our second proposal, creating FSG Manual section 8B2.2, the Effective Terrorist-Activity Discovery Program, imposes maximum fines upon social media companies after they are found or plead guilty in proceedings conducted with full constitutional protections for their and their users' public speech, only where they failed to disclose public postings.

Even if Fourth Amendment protections extend to the contents of e-mails sent over the Internet, a proposition we discuss below, they clearly do not extend to public websites[272] and file-sharing services.[273] Most lower courts previously confronted with this issue have reached these same conclusions,[274] though the Supreme Court has yet to weigh in on precisely this question.[275] However, related

---

[269] We acknowledge that a statutory definition for "social media," or those otherwise impacted, may be necessary beyond what we provide in our proposal. We intend "publicly viewable" shared content to include posts that can be seen by followers or friends of the user.

[270] U.S. Const., amend. IV.

[271] Katz v. United States, 389 U.S. 347 (1967).

[272] *See, e.g.*, United States v. Forrester, 512 F.3d 500. 509–11 (9th Cir. 2008) (holding that the Fourth Amendment does not limit the monitoring of visited websites, such as Internet Protocol addresses and to/from e-mail information); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (applying third-party disclosure doctrine to records kept by ISPs); United States v. Post, 997 F.Supp.2d 602, 606 (S.D. Tex. 2014) (holding that the metadata embedded in a photograph posted to a website is not protected under the Fourth Amendment); United States v. Gines-Perez, 214 F.Supp.2d 205, 224–25 (D.P.R. 2002) (holding that defendant had no reasonable expectation of privacy in a group portrait of store employees posted on the Internet).

[273] United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (holding that files made available over a file-sharing network are not protected by the Fourth Amendment).

[274] *See* cases cited in notes 272 and 273, *supra*.

[275] The Court has twice looked at the similar issue of cell phone text messages. In City of Ontario v. Quon, 560 U.S. 746, 760–61 (2010), a civil case, the Court assumed that officer Quon had a reasonable expectation of privacy in the "text messages sent on the pager provided to him by the city" but concluded that the search was constitutional "because there were 'reasonable grounds for

Supreme Court doctrine supports our position on these issues. The Court has held on numerous occasions that persons have no reasonable expectation of privacy in oral or written messages voluntarily revealed to third parties who then decide to share the message with the government. Though not all scholars agree, it seems to us that this third-party doctrine supports the proposition that the act of publicly posting a message using an ISP waives any reasonable expectation of privacy in its contents.[276] For example, should a person orally or in writing make incriminating statements to a recipient who happens to be an undercover government agent, she has no reasonable expectation of privacy in those statements.[277] As the Court stated in *United States v. White*, "however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities."[278]

Similarly, when one reveals personal business records to a third party, such as a bank or accountant, that data no longer receives Fourth Amendment

---

suspecting that the search [was] necessary for a non-investigatory work-related purpose.'" The Court did not discuss the third-party doctrine. In Riley v. California, 134 S.Ct. 2473, 2480 (2014), the Court held that law enforcement generally may not "without a warrant, search digital information on a cell phone seized from an individual who has been arrested." Again, the Court did not discuss the third-party doctrine. However, the Court appeared to view the content of cell phone calls and text as protected by the Fourth Amendment when not voluntarily revealed.

[276] Not all scholars agree with a strict application of the third-party doctrine to IPS' treatment of web sites, e-mail, and stored communications, especially when treating the Internet service provider as the third party. For example, as discussed in note 292, *infra*, Professor Henderson would disallow treating an ISP as a third party where the user's intent was for the message to remain private between the two of them. For examples of various positions taken on this issue, *see, e.g.*, Steven M. Bellovin, Matt Blaze, Susan Landau & Stephanie K. Pell, *It's Too Complicated: The Technological Implications of IP-Based Communications on Content/Non--Content Distinctions and the Third Party Doctrine*, 30 HARV. J.L. & TECH (forthcoming 2016) (arguing that "the once-stable distinction between content and non-content has steadily eroded to the point of collapse, destroying in its wake any meaningful application of the third party doctrine"); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n. 5 (2009) (collecting lists of scholarship that has criticized the third-party doctrine); STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 124 (2012) (criticizing the third-party doctrine because of the "artificial assumption of voluntary choice"); David A. Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CAL. L. REV. 1069 (2014) (arguing that commonly accepted definitions of privacy are imperfect); David McPhie, *Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin*, 2005 STAN. TECH. L. REV. 1 (2005); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2105 (2009) (suggesting that any "electronic information that can reveal the underlying text or subject matter of an Internet communication must be classified as content").

[277] United States v. White, 401 U.S. 745, 1122 (1971) (holding that the Fourth Amendment did not bar testimony of government agent who overheard and taped a conversation with the defendant through electronic monitoring); Hoffa v. United States, 385 U.S. 293 (1966). *See also* Illinois v. Perkins, 496 U.S. 292 (1990) (holding that *Miranda* warnings are not required when a jail plant is placed in a cell with a suspect and the suspect is unaware that he is speaking to an undercover law enforcement officer).

[278] White, *supra* note 277 (Justice Powell writing for the plurality and quoting *Hoffa*, *supra* note 277).

protection.[279] As the Court stated in *United States v. Miller*, "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. . . . This analysis is not changed by the mandate of the Bank Secrecy Act that records of depositors' transactions be maintained by banks."[280] Finally, lower courts regularly hold that when a person speaks in public such that more than one other person hears him, or speaks loudly enough to be overheard, the government does not conduct a search when it listens to that speech.[281]

Given this settled law concerning the third-party doctrine, it seems to us clearly correct that postings held out for public viewing are not protected by the Fourth Amendment. At least one state court has applied the third-party doctrine to public messages communicated over Twitter.[282] Moreover, as one federal judge reasoned when admitting evidence obtained when law enforcement viewed Facebook postings that were visible only to select "friends" through the cooperation of a witness on the defendant's "friends list": "Where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment. . . . While [defendant] Colon undoubtedly believed that his Facebook profile would not be shared with law enforcement, he had no justifiable expectation that his 'friends' would keep his profile private."[283]

The strength and scope of these doctrines, however, may actually give scholars and policymakers pause about whether the Court should place some limits on the third-party when it comes to social media. If the third-party doctrine can be used to permit the government to mandate that social media companies turn over public postings by their users, might the same reasoning be used to permit the government to mandate that social media companies turn over private e-mails, at least where they have some reason to believe that such communications discuss criminal activities? In both cases, arguably the users have voluntarily offered their communications to third parties, who are then free to share them with the government. While we take no firm position on this point, we will lay out the basic arguments on each side. We address this broader issue because it seems to us possible that at some point legislators might call for an

---

[279] United States v. Miller, 425 U.S. 435, 443 (1976) (holding that customer had no reasonable expectation of privacy in bank records he stored with third-party banks, and therefore could not challenge the grand jury subpoena for those records on Fourth Amendment grounds).
[280] *Id.*
[281] *See, e.g.*, United States v. Mankani, 738 F.2d 538 (2d Cir. 1984) (holding that Fourth Amendment is not implicated where conversations in an adjoining motel room were overheard by law enforcement).
[282] People v. Harris, 949 N.Y.S.2d 590, 594 (N.Y. Crim. Ct. 2012).
[283] United States v. Meregildo, 883 F.Supp.2d 523, 526 (S.D.N.Y. 2012).

expansion of our proposals to include e-mail messages between two individuals sent through an Internet service provider. Moreover, scholars and policymakers may anticipate such an extension as a good reason to reject our proposals outright.

The disagreement regarding whether the Fourth Amendment protects e-mails sent between two private individuals on public servers, or whether instead the third-party exception applies, is as follows. Those in favor of broader government enforcement of anti-terrorism provisions will argue that since the ISP already has access to (and could read) things like private e-mail communications solely between two individuals and the attachments to such e-mails, the customer sending or receiving such an e-mail has no reasonable expectation of privacy in its content. Once the ISP has access to the message, it can deliver the message to the government. Such a position would be sturdily bolstered in those instances where, as is currently the case, the email provider requires that its users agree to a Terms of Service (TOS) contract that allows the private company to take action whenever a user posts content or sends messages that contain child pornography or is otherwise threatening, libelous, deceptive, or fraudulent.[284] An ISP could add to its list of prohibitions user posts that potentially violate the material support statute to such TOS contract. Many ISPs, such as Sprint, Verizon, and other telephone service providers, require customers to sign TOS contracts allowing company eavesdropping where necessary to avoid violations of federal law.[285] Most courts have not yet decided the "complex, difficult, and 'far-reaching' legal issues" surrounding whether a sender of an e-mail has a reasonable expectation of privacy in the context of a message voluntarily committed to the custody of an ISP.[286] In those cases, however, it may be that the sender loses her reasonable expectation of privacy regarding the contents of these e-mails, as well as her privacy interest on any embedded or attached files. Quite plausibly the user in

---

[284] AOL current offers free e-mail service to users who agree to its Terms of Service (TOS), which state that a user must: "[c]omply with applicable laws and regulations and not participate in, facilitate, or further illegal activities" and "[n]ot post content that contains explicit or graphic descriptions or accounts of sexual acts or is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, or tortious" and that "[t]o prevent violations and enforce this TOS and remediate any violations, we can take any technical, legal, and other action that we deem, in our sole discretion, necessary and appropriate without notice to you." AOL TOS, last updated July 19, 2016, http://legal.aol.com/terms-of-service/full-terms/. *See also* Ackerman, *supra* note 149, at *1.

[285] *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007) (holding that the defendant-student did not lose his objectively reasonable expectation of privacy in his computer and his e-mails merely by attaching his computer to the university of Wisconsin network, but noting that "privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user"); *but see* United States v. King, 509 F.3d 1338 (11th Cir. 2007) (holding that civilian contractor working at a U.S. Air Force base who connected to the base network using his personal laptop computer had a subjective but not a reasonable expectation of privacy because "[his] files were 'shared' over the entire based network and everyone on the network . . . had access to all of [his] files and could observe them in exactly the same manner as did the computer specialist").

[286] United States v. Keith, 980 F.Supp.2d 33, 39 (2013). *See also* Rehberg v. Paulk, 611 F.3d 828, 846 (11th Cir. 2010) (collecting cases), *aff'd*, 132 S.Ct. 1497 (2012).

such a case has given consent to a private search, and that the company doing the private search might then consent to share the information with the government.[287] Anyone wishing to extend the third-party exception to ISPs might also analogize about Court holdings that when a person voluntarily discloses non-content information, such as telephone numbers, to a third party, that person loses his expectation of privacy on such information.[288]

On the other hand, civil libertarians might suggest that in the modern age sending an e-mail to a single individual is precisely the same thing as making a private telephone call, and the Supreme Court has already held that a call between only two non-governmental agents is protected by the Fourth Amendment from government eavesdropping.[289] A number of lower courts have reached similar holdings.[290] As one judge stated, "we have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user 'seeks to preserve as private,' and therefore 'may be constitutionally protected.'"[291] Just as a caller should not lose his reasonable expectation of privacy from government intrusion merely because the telephone company might decide to listen to her conversation, the e-mail sender should not lose her privacy rights should her ISP decide to snoop. One answer to the Term of Service charge eliminating a users' reasonable expectation of privacy might be to point out that most ISP require that users agree to such contracts before they can use the service, and one might seriously question whether such users have the bargaining strength to obtain service without the terms. One might also question whether an IPS' voluntary decision to turn over messages to the government has the same Fourth Amendment implications as would the ISP's decision to share after the government enacted a mandatory sharing statute (perhaps one similar to our first proposal but extended to all messages).

---

[287] Though if statute requires a company to share certain e-mail with the government, then the company might become a government actor for Fourth Amendment purposes. *See* Ackerman, *supra* note 149.

[288] Smith v. Maryland, 442 U.S. 735 (1979) (finding that pen register device does not disclose the content of any communications and is voluntarily revealed to the telephone company).

[289] Katz v. United States, 389 U.S. 347 (1967) (defendant had "reasonable expectation of privacy" in telephone call made from a public telephone booth); Berger v. New York, 388 U.S. 41 (1967) (invalidating New York wiretapping law on the ground that it violated the Fourth Amendment).

[290] *See* United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010) (finding that the content of e-mails are protected under the Fourth Amendment); United States v. Ali, 870 F.Supp.2d 10, 39 (D.D.C. 2012); In re Applications for Search Warrants for Information Associated with Target Email Address, No. 12-MJ-8119-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012); In re Applications of U.S. for An Order Authorizing the Release of Historical Cell-Site, No. 10-MC-0897(JO), 2010 WL 5437209, at *3 (E.D.N.Y. Dec. 23, 2010). Additionally, two federal courts have applied the Fourth Amendment to the content of private Facebook messages. R.S. ex rel. S.S. v. Minnewaska Area School Dist. No. 2149, 894 F.Supp.2d 1128, 1142 (D. Minn. 2012); Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965, 991 (C.D. Ca. 2010).

[291] Warshak v. United States, 490 F.3d 455 (6th Cir. 2007).

We are able to avoid this issue through careful drafting and implementation of our proposals. Our proposals would pass constitutional muster even if the Court were to embrace the subtler reasoning of some scholars that an ISP provider does not fit within the third-party exception when it acts merely as a "conduit or bailee."[292] In that case, social media providers who turn over postings made to the public would still be covered by the less expansive third-party doctrine. So long as our proposals remain limited to public postings, it will not matter whether the third-party doctrine permits ISP to read every private e-mail, and it will not matter what kind of service contract the ISP signed with their user.

Finally, we believe that our proposals avoid the current Fourth Amendment controversy in the child pornography area regarding private versus public actors. Our proposal creating a new federal offense codified at 18 U.S.C. § 2339E is in some respects similar to the Missing Children's Assistance Act of 1984,[293] the subject of a current Fourth Amendment split among the circuit courts. Since our proposal, unlike that Act, covers only postings that are public, not private, it should not be relevant under the Fourth Amendment whether these postings are seized and searched by the government or a private actor. A description of this issue is warranted, however, for the same reasons that we delve into the Fourth Amendment issue of private versus public messaging (the third-party doctrine). It may be that a future version of our proposal will apply to individual e-mails in addition to public postings. In that case, it would matter deeply whether the social media company doing the search represented the government.

In *United States v. Ackerman*, a district judge held that AOL's deployment of its Image Detection and Filtering Process (ODFP) and tip to the National Center for Missing and Exploited Children (NCMEC") containing evidence of child pornography possession by its user did not implicate the Fourth Amendment, even when such evidence was turned over to local law enforcement officials.[294] A search by a private person becomes a government search in the Tenth Circuit depending upon a two-part inquiry: "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his

---

[292] *See, e.g.*, Stephen Henderson, *After United States v. Jones*, 14 N.C. J.L. & TECH. 431, 437 (2013) (arguing that the third-party doctrine should not apply where an ISP is acting merely as a conduit to allow a private message to get from one party to another); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data,* 14 J.L. & POL'Y 211, 257 (2006) (arguing that the third-party doctrine incorrectly assumes that disclosure to a trusted third party is identical to indiscriminate disclosure to the public). Some scholars call for an empirical inquiry into whether society views information disclosed to third parties, notably ISPs, is reasonably private. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 4 (2007); Christine S. Scott-Hayward, Henry F. Fradella, and Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19 (2015).

[293] *See supra* note 145 and the discussion of this Act in Section II(A)(2).

[294] Ackerman, *supra* note 149.

own ends." Neither AOL nor the NCMEC were state actors, despite the enactment of 18 U.S.C. § 2258A requiring Internet service providers to report known child pornography to the government, because the statute specifically states that the private company is not required to monitor its users or affirmatively seek child pornography transmitted by its users. The district court found that AOL did not act with government involvement, and that it employed the IDFP to protect its own business interest and reputation, rather than to assist the government. NCMEC, even if a governmental entity or agent, did not conduct a Fourth Amendment search when it merely repeated an investigation already conducted by AOL.

However, the district judge's opinion in *Ackerman* was reversed by the Tenth Circuit, which held that the NCMEC was a government entity for purposes of determining whether its search of defendant's e-mail violated the Fourth Amendment.[295] NCMEC is a government entity because its two primary authorizing statutes, 18 U.S.C. § 2258A and 42 U.S.C. § 5773(b), mandate its collaboration with federal, state, and local law enforcement in a myriad of ways, such as operating an official national clearinghouse for information and helping local law enforcement recover missing and exploited children. ISPs must report known child pornography violations to NCMEC, not to any other governmental agency, when NCMEC confirms a report it must preserve evidence, and NCMEC is authorized to receive contraband and review its contents. While it is true that the federal statutes do not require AOL to develop programs to discover child pornography, nor do they require the NCMEC to open and view e-mail and attachments like Mr. Ackerman's, "everyone accepts that Congress has authorized and funded NCMEC to do just that."[296]

Shortly before the first *Ackerman* decision by the district judge, a second federal district judge came to just the opposite result. In *U.S. v. Keith*, Judge O'Toole held that the NCMEC's conduct constituted a government search under the First Circuit's three factor test: "(1) the extent of the government's role in instigating or participating in the search; (2) the government's intent and the degree of control it exercises over the search and the private party; and (3) the extent of which the private party aims primarily to help the government or to serve its own interests."[297] The facts in *Keith* are very similar to the facts in

---

[295] United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016).

[296] *Id.* at 1302. Having determined that the NCMEC is a governmental agency, the Court considered the open question of "whether the Supreme Court's so-called 'third party doctrine' might undermine any claim to Fourth Amendment protections when someone (like Mr. Ackerman) engages a private agency (like AOL) to deliver his correspondence." *Id.* at 1304. However, the Tenth Circuit was able to completely punt this issue by noting that the district court had not relied upon the third-party doctrine in ruling against Mr. Ackerman, and to the contrary assumed that Mr. Ackerman had a reasonable expectation of privacy in his e-mail. Thus, this case sheds no light on one of the initial issues we discussed in Part III(A), whether senders of e-mails enjoy a reasonable expectation of privacy in their content.

[297] U.S. v. Keith, 980 F.Supp.2d 33 (D. Mass. 2013).

Ackerman. Both involved AOL using its IDFP to find child pornography on an e-mail from one of its users, which it passed on to the NCMEC tip line.[298] However, the *Keith* court found that the NCMEC is a government agent under its three factor test, as it receives government funding and has a "partnership" with local law enforcement. Moreover, the NCMEC analyst's viewing of the contents of the file was an expansion of the AOL's private search, so it constituted a separate search that invaded additional expectations of privacy.[299] Mr. Keith pled guilty after losing his suppression motion, so his case will not be appealed.

Now that the Tenth Circuit and the *Keith* court agree, however, there still remains a circuit split on this issue. Most circuits agree with earlier the district court decision in *Ackerman*, not in the Tenth Circuit's reversal nor in the district judge in *Keith*. For example, in *United States v. Stevenson*,[300] the Eighth Circuit found no Fourth Amendment violation because the ISP was not a government agent, and the provider had no affirmative duty to discover child pornography (only to report such pornography if it was already "known."). The court held that 18 U.S.C. § 2258A's reporting requirements did "not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography."[301] The First and Fourth circuits held similarly when addressing 18 U.S.C. § 2258A's predecessor statute, 42 U.S.C. § 13032(b)(1).[302] Thus, it appears to us at least possible that if our proposals are extended to the content of e-mails containing material support to foreign terrorist organizations, some circuits may hold that the social media company or internet provider service is a private actor, and therefore such a search (even if the results are shared with the federal government) does not implicate the Fourth Amendment. However, we are not at this time suggesting that our proposals apply to individual e-mails, only to public postings. Therefore, the proposal is constitutional whether or not social media companies are acting as private companies or as agents of the government.

We conclude with a thought about postings by foreign lone-wolf terrorists. We believe the Fourth Amendment does protect public postings regardless of

---

[298] We note here that ISPs like AOL use a database of hash values of files to conclude that an e-mail contains child pornography. No employee at AOL actually opens the file or looks at the offending image. This may make these cases distinguishable for our proposal, even applied to e-mails. Under our proposal, it may be that an employee of the private social media company reads the offending message before deciding to pass it along to the FBI. On the other hand, the social media company may also develop a key word program that does not mandate that a person review the posting or e-mail.

[299] Keith, *supra* note 297, at 43 (citing United States v. Jacobsen, 466 U.S. 109 (1984)).

[300] 727 F.3d 826, 830 (8th Cir. 2013).

[301] *Id.* at 829–30.

[302] *See, e.g.*, United States v. Cameron, 699 F.3d 621, 637–38 (1st Cir. 2012) (holding that although 42 U.S.C. § 13032(b)(1) required Yahoo! to report child pornography, there was no obligation to search for it and therefore the government did not exercise control over Yahoo!'s actions); United States v. Richardson, 607 F.3d 357, 364–67 (4th Cir. 2010) (holding that "the statutory provision pursuant to which AOL reported [defendant's] activities did not effectively convert AOL into an agent of the Government for Fourth Amendment purposes").

whether the persons, companies, data and computers are physically located inside or outside the United States.[303] There is no reasonable expectation of privacy because the user is sharing her message publicly; whether such users are based in the United States, or are predominantly foreign customers, as may be more likely,[304] is not determinative.[305] Prosecuting users residing in jurisdictions without extradition treaties will be quite difficult, but at least those users who enter the United States, perhaps with the intent of committing a terrorist act, can be more easily arrested once our proposal is implemented. Whenever communications cross an international border, whether they are public postings or private e-mails, they might be considered searchable under the border search exception to the Fourth Amendment.[306]

Conclusion

If it is true that "Facebook's policy is to pass on information to law enforcement as soon as it becomes aware of any planned attack or threat of imminent harm,"[307] then the legislation proposed here should not cause vocal denunciations from social media companies and their lobbyists. However, as with the protests we have seen with respect to Senator Feinstein's much weaker proposal, we expect both of our proposals to generate controversy and intense lobbying efforts by the social media industry. At some point, we believe in the very near future, the public's demand for safety from domestic lone-wolf terrorist attacks will trump even these tech companies' well-funded and sophisticated efforts to stave off federal legislation of any kind. As demonstrated above, our proposals carry the biggest impact in terms of their potential to identify terrorist threats and prevent attacks without violating constitutional protections. While our proposals do reach significantly further than current law, clear precedents in the First and Fourth Amendment areas from the Supreme Court and lower courts

---

[303] *But see* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015).

[304] Today, 83 percent of Facebook's users are located outside of U.S. soil. *See Population and Telecom Reports for the Americas,* INTERNET WORLD STATS (June 30, 2016) http://www.internetworldstats.com/stats2.htm. At the end of 2014, less than 10 percent of the world's Internet use was attributable to users within the United States. *Id.*

[305] Of course, a foreign person with no connection to the United States does not enjoy any Fourth Amendment rights. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 274 (1990) (refusing to suppress evidence obtained during searches by U.S. law enforcement personnel of houses in Mexico owned by a Mexican drug kingpin because the Fourth Amendment is implicated only when the subject has contacts with the United States via either lawful presence or some substantial connection). While posting messages that are received in the United States may give a person sufficient voluntary connection to the United States to trigger Fourth Amendment protections, under our proposals only public messages are covered, and thus the Fourth Amendment is inapplicable to any poster.

[306] *See, e.g.*, Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) (holding that routine border searches are permissible under the Fourth Amendment at the international border and its functional equivalents); United States v. Flores-Montano, 541 U.S. 149, 152 (2004) (holding that searches at the international border are permitted without reasonable suspicion).

[307] David Jones, *Social Media Firms Face Quandary Over Terror Prevention*, TECH NEWS WORLD (Dec. 8, 2015), http://www.technewsworld.com/story/82845.html.

support their legality. Neither of our proposals impinge upon social media users' reasonable expectation of privacy, nor impermissible restrict their freedom of speech.

We applaud Senator Feinstein's bill to mandate that all social media companies report known violations of the federal material support statutes to federal authorities, but the current proposal remains insufficient. "Terrorism is the modern day equivalent of the bubonic plague: it is an existential threat."[308] Our first proposal, the new federal offense of Failure to Institute a Terrorist Activity Discovery Program, in violation of 18 U.S.C. § 2339E, will criminalize social media companies' failure to police their public websites for threats that may violate material support or other anti-terror statutes. Our second proposal, amending to Federal Sentencing Guidelines to add § 8B2.2, the Effective Terrorist-Activity Discovery Program, will encourage social media companies to institute compliance programs to ensure that their own agents do not violate any anti-terror provisions. Though far from a panacea, our proposals offer a solid framework for catching foreign and domestic individuals intent on assisting foreign terrorist organizations or attacking themselves before they strike, by enlisting the support of those companies making money off their global media activities. These proposals also properly shift the decision-making regarding how to react to posts offering material support to terrorists from private companies to government experts. While these proposals represent a significant change from current policy, they follow a long domestic history in the areas of fraud, corruption, and banking, and they are consistent with more recent precedent under international copyright law. Unfortunately, without government intervention using tools such as the ones we offer here, the prevalence of domestic terrorist activity, which heavily rely on the Internet and mobile applications for recruitment, planning, and implementation of attacks, will continue to rise.

[308] United States v. Mehanna, *supra* note 132, at 40.