NOTE

TARGETING DETACHED CORPORATE INTERMEDIARIES IN THE TERRORIST SUPPLY CHAIN: DIAL 2339/13224 FOR ASSISTANCE?

Lauren C. O'Leary[*]

The United States has for decades faced persistent and evolving threats from highly agile and adaptable terrorist organizations. Recognizing the need for more robust domestic counterterrorism efforts in the early 1990s, the U.S. government has since made significant use of the legal system to disrupt inchoate plots and degrade terrorists' support structures. Among the tools most heavily used on this front have been the material support statutes and the International Emergency Economic Powers Act ("IEEPA"), which aim to deprive terrorists of necessary resources by targeting those who support or do business with them. Though used against hundreds of individuals to date, there has been a dearth of organizational prosecutions in this realm. Recognizing the crucial facilitating role corporate actors often play, the Department of Justice ("DOJ") has long targeted neutral intermediaries to get at underlying crime, from tax evasion to drug trafficking. Recent cases suggest the DOJ is increasingly comfortable pursuing entities that do business with bad actors, including through novel applications of existing laws.

This Note argues that the material support statutes and IEEPA can and should be applied against corporate actors that do business with terrorists, as a means of both disrupting the terrorist "supply chain" and incentivizing greater private sector cooperation. Examining in particular the potential for prosecution of social media and content-hosting companies, encrypted messaging providers, and nontraditional financial intermediaries exploited by terrorists, this Note argues

[*] J.D. Expected 2017, University of Virginia School of Law; B.A. 2006, George Washington University. I would like to thank Professor Ashley Deeks for her invaluable guidance, insight, and feedback on earlier drafts. Many thanks also to the staff of the Virginia Law Review; it takes a village to publish a Note, and I am grateful for the thoughtful comments and suggestions of each and every editor. All opinions are my own.

that a credible and carefully wielded threat of terrorism-related charges would be an important addition to prosecutors' toolkits where appeals to good corporate citizenship fall flat. An effective all-tools counterterrorism strategy requires imagination and adaptation. This Note argues the material support statutes and IEEPA are tools that can be brought to bear against those that play the role of willing supporter or are otherwise indifferent to the harm they facilitate.

INTRODUCTION

IN 2014, federal prosecutors indicted FedEx Corporation and two subsidiaries (collectively, "FedEx"), alleging the shipping behemoth had engaged in a years-long money laundering and drug-trafficking conspiracy.[1] The government alleged FedEx had received multiple warnings that Internet pharmacies engaged in illegal conduct were using its services, yet created dedicated billing codes and policies to deal with these problematic (but lucrative) customers rather than cease doing business with them.[2] Then-U.S. Attorney Melinda Haag described the headline-grabbing case as "highlight[ing] the importance of holding corporations that knowingly enable illegal activity responsible."[3] FedEx took the unusual approach of fighting the case, publicly stressing its past attempts and continued willingness to assist law enforcement.[4] While prosecutors ultimately moved to dismiss remaining charges mid-trial in June 2016 and reportedly undertook an internal review of the charging decision,[5] the facts and theory under which the case was brought in the first place remain significant.

FedEx's hard stance contrasted with those of competitor United Parcel Service ("UPS") and Internet giant Google, each of which had previously entered into nonprosecution agreements ("NPAs") with the Department of Justice ("DOJ") to resolve similar probes.[6] Commentators

[1] Press Release, Dep't of Justice, FedEx Indicted for Its Role in Distributing Controlled Substances and Prescription Drugs (July 18, 2014), 2014 WL 3538921 [hereinafter DOJ FedEx Press Release].

[2] Superseding Indictment at 2–8, United States v. FedEx Corp., No. 14-CR-00380 (N.D. Cal. Aug. 14, 2014).

[3] DOJ FedEx Press Release, supra note 1.

[4] Press Release, FedEx Corp., Updated FedEx Response to Department of Justice Charges (Aug. 15, 2014), http://about.van.fedex.com/newsroom/global-english/updated-fedex-response-to-department-of-justice-charges [https://perma.cc/GR3Q-AAEP] ("We have asked for a list [of Internet pharmacies engaging in illegal activity], and [the Department of Justice] ha[s] sent us indictments.").

[5] Dan Levine & David Ingram, U.S. Prosecutors Launch Review of Failed FedEx Drug Case, Reuters (July 15, 2016, 1:03 AM), http://reut.rs/29XeeNE [https://perma.cc/9DE3-TSCD].

[6] See infra Subsection II.D.3.

characterized the FedEx case as indicative of an emerging "gray collar crime" approach under which the DOJ pursues "novel kind[s] of white collar indictment[s] grounded in blue collar law," such as the Controlled Substances Act ("CSA").[7] FedEx was not accused of violating affirmative statutory duties, but rather of being complicit in drug trafficking by providing the services it markets to the rest of the world to bad actors.[8] Novelty of theory aside, going after bad actors through third parties is hardly a new tactic. Prosecutors have long targeted detached intermediaries in efforts to get at blue collar crime, including illegal gambling and drug trafficking, among many others.[9] Despite concerns over collateral consequences and broader doctrinal discomfort,[10] data on federal prosecution of business entities[11] and the public stance of the DOJ suggest such cases will likely remain a prominent fixture of the legal and business landscape.[12]

Enter, stage right, the specter of terrorism. The old paradigm of state-sponsored attacks on U.S. targets overseas has been largely supplanted by "entrepreneurial" groups and Internet-radicalized "lone wolves" aiming at U.S. soil, often from within.[13] These actors generally lead facially

[7] Michael D. Ricciuti et al., 2014 Saw the Arrival of 'Gray Collar' Crime, Law360 (Jan. 5, 2015, 10:17 AM), http://www.law360.com/corporate/articles/606293 [https://perma.cc/R96Z-SSL4]; see also David Ring & Claire Coleman, The Rise of 'Failure to Prevent' Crimes and CCO Liability, N.Y.L.J., Oct. 27, 2014, at 10 (characterizing the FedEx prosecution as "set[ting] a new high-water mark for the 'failure to prevent' theory of criminal liability").

[8] Superseding Indictment at 9–18, United States v. FedEx Corp., No. 14-CR-00380 (N.D. Cal. Aug. 14, 2014).

[9] See, e.g., Lindsey Gruson, U.S. Accuses Shearson of Money Laundering, N.Y. Times, June 27, 1986, at A1 (illegal bookmaking); Michael Isikoff, U.S. Links Bank to Drug Cartel, Wash. Post, Oct. 12, 1988, at A1 (international cocaine trafficking).

[10] See infra Part II.

[11] Brandon L. Garrett, Corporate Criminal as Scapegoat, 101 Va. L. Rev. 1789, 1802–05 (2015) [hereinafter Garrett, Scapegoat] (reporting that federal prosecutors filed more than 300 deferred prosecution and nonprosecution agreements with entity defendants between 2001 and 2014, and further illustrating year-to-year trends during that period).

[12] See, e.g., Aruna Viswanatha, Justice Department Gets Tougher on Corporate Crime, Wall St. J. (Nov. 16, 2015, 5:28 PM), http://on.wsj.com/1PKLaHR. The 2017 presidential transition and related personnel changes within the DOJ create an open question as to whether the Department will adopt a materially different approach under the new administration. Ben Protess & Matt Apuzzo, Tougher on Corporate Crime. For Now., N.Y. Times, Jan. 13, 2017, at B1.

[13] Nat'l Comm'n on Terrorist Attacks Upon the United States, 9/11 Commission Report 145–50, 153–56 (2004) [hereinafter 9/11 Commission Report]; Lisa O. Monaco, Assistant to the President for Homeland Sec. and Counterterrorism, Address at the Council on Foreign

unremarkable lives in the United States and other Western countries, availing themselves of mainstream financial, communications, and travel networks to facilitate planning, preparation, and execution of their plots.[14] In response, criminal prosecution has increasingly been used as a complement to U.S. military and intelligence activities in the years since the 1993 World Trade Center ("WTC") bombing.[15] Enacted in the mid-1990s but rarely used prior to 9/11, the material support statutes broadly criminalize the provision of goods and services to terrorists and have become a critical facet of U.S. counterterrorism strategy.[16] Similarly, the International Emergency Economic Powers Act ("IEEPA") broadly bars most transactions with countries, individuals, and entities designated as being affiliated with terrorism.[17] To date, IEEPA's criminal provisions (as distinguished from the designation and blocking authority it provides to the President[18]) have primarily been used to enforce country-based sanctions, not terrorism-specific programs.[19] Both IEEPA and the material support statutes are versatile tools that could be used more expansively to combat the threat posed by terrorist groups that target the Unit-

Relations (Mar. 7, 2016), http://www.cfr.org/homeland-security/lisa-o-monaco-homeland-security-counterterrorism/p37621 [https://perma.cc/S6V6-HZ7X].

[14] The 9/11 hijackers are but one illustrative example of this reality. 9/11 Commission Report, supra note 13, at 215–31, 241–43, 247–53.

[15] See, e.g., id. at 71–73 (discussing post-WTC investigations and prosecutions, and finding that, in the mid-1990s, legal processes were "the primary method for responding to . . . early manifestations of a new type of terrorism"); Should 9/11 Trials Be Held at Guantanamo Bay?, PBS NewsHour (Sept. 10, 2016, 2:36 PM) (program transcript), http://to.pbs.org/2iu9L6G [https://perma.cc/4SUC-7SVU] ("[F]ederal prosecutors in New York . . . wrote the book on prosecuting major terrorism cases. The first chapter was the trial for the 1993 World Trade Center truck bombing . . . .") (statement of Phil Hirschkorn); cf. U.S. Dep't of Justice, The Criminal Justice System as a Counterterrorist Tool: A Fact Sheet (Jan. 26, 2010), http://www.justice.gov/opa/blog/criminal-justice-system-counterterrorism-tool-fact-sheet [https://perma.cc/E75E-248J] ("As a counter-terrorism tool, the criminal justice system has proven incredibly effective in both incapacitating terrorists and gathering valuable intelligence from and about terrorists.").

[16] Jeff Breinholt, Material Support: An Indispensable Counterterrorism Tool Turns 20, War on the Rocks (Apr. 19, 2016), http://warontherocks.com/2016/04/material-support-an-indispensable-counterterrorism-tool-turns-20 [https://perma.cc/3YGK-FTGH]. The material support statutes are codified under 18 U.S.C. §§ 2339, 2339A–2339D (2012); this Note focuses primarily on § 2339B.

[17] 50 U.S.C. §§ 1701–1707 (2012).

[18] See infra Subsection I.C.1.

[19] See, e.g., Nicole Hong, Sanctions Law a Powerful Tool for Prosecutors, Wall St. J.: L. Blog (Mar. 25, 2015, 5:04 PM), http://on.wsj.com/1xhbxyM.

ed States and its interests, including in the corporate context where there is likely to be a concern with public perception.

At present, there appears to be a confluence of factors supporting such an expansion. The DOJ's willingness to pursue "gray collar" theories against corporations as well as prosecute individuals for providing increasingly broad types of support to foreign terrorist organizations ("FTOs"), combined with shifts in FTOs' focus from overseas targets to U.S. soil, suggests mainstream companies could well find themselves in the crosshairs of the material support laws and IEEPA. To date, however, only one large, mainstream company has been convicted of criminal charges related to dealings with terrorists.[20] This Note argues that both the doctrinal underpinnings of corporate criminal liability and the DOJ's prior prosecutions of corporate intermediaries to get at underlying bad actors support broader application of IEEPA and the material support statutes in the corporate context than has been observed to date. Where supported by facts and evidence, such as indicia that a potential corporate defendant is aware that it is or very likely may be doing business with FTOs or their associates, the threat of prosecution can and should be used to incentivize greater cooperation in efforts to disrupt terrorist networks when appeals to good corporate citizenship alone are unpersuasive. Charging decisions should of course involve careful consideration of potential collateral impacts, including those on intelligence collection and civil liberties, but private-sector companies should not be absolved of criminal responsibility where they take a hands-off approach with respect to their user or customer base.

Much has been written about the material support statutes and IEEPA; similarly, much has been written about federal corporate criminal liability and its application in practice. To date, there has been little examination in the academic literature of the intersection of the two; this Note seeks to provide a view of that intersection as well as potential hazards and opportunities on the road forward. Part I examines the material support statutes and IEEPA, focusing on text and history, application, and critiques. Part II focuses on doctrinal issues with corporate criminal liability and examines past targeting of corporate intermediaries. Part III illustrates how firms such as social media and content-hosting companies, providers of messaging and communications platforms, and non-

[20] See infra Subsections I.B.2 & I.C.2.

traditional financial intermediaries could be prosecuted under principles discussed in Parts I and II. Focus is placed in Part III on products and services designed to ensure anonymity or to frustrate lawful investigative requests, though these statutes could be applied to a much broader range of corporate actors. Part IV addresses potential critiques and identifies safeguards before concluding.

I. ADDRESSING THREATS TO THE HOMELAND THROUGH LAW: THE MATERIAL SUPPORT STATUTES & IEEPA

This Part will serve as a high-level introduction to the terrorist threat currently faced by the United States, as well as the use of criminal prosecution as part of broader counterterrorism efforts. Section I.A begins by broadly tracing the evolution of threat and response, and is followed by an overview of the text and history, historical application, and critiques of the material support statutes and IEEPA in Sections I.B and I.C, respectively.

A. The Evolution of Modern Terrorist Threats to U.S. Interests

The use of the U.S. legal system against FTOs and their facilitators is a relatively recent development, reflecting the evolving nature of international terrorism (though the foreign/domestic line is increasingly blurred[21]). In the 1970s and 1980s, the prevailing paradigm was one of state-sponsored attacks against U.S. targets overseas.[22] While the DOJ attempted to prosecute some operational leaders, the U.S. response was generally weighted toward military, intelligence, and diplomatic action.[23] The 1990s saw a shift toward "private-sector terrorism," with al

[21] Lorenzo Vidino & Seamus Hughes, Program on Extremism, George Washington Univ., ISIS in America: From Retweets to Raqqa 5–10 (Dec. 2015) [hereinafter Retweets to Raqqa], https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf [https://perma.cc/M6B5-JNLT] (analyzing social media-based recruitment).

[22] Terrorist Attacks on Americans, 1979-1988, PBS: Frontline, http://www.pbs.org/wgbh/pages/frontline/shows/target/etc/cron.html [https://perma.cc/JS23-FRG3] (last visited Aug. 27, 2016).

[23] George Lardner, Jr., 2 Libyans Indicted in Pan Am Blast, Wash. Post, Nov. 15, 1991, at A1 (reporting the indictment of the Pan Am Flight 103 bombers and U.S. lobbying efforts for an international embargo against Libya); Matthew Levitt, 'Fox' Hunt: The Search for Hezbollah's Imad Mughniyeh, The Hill (Feb. 4, 2015, 6:00 AM), http://thehill.com/blogs/pundits-blog/defense/231592-fox-hunt-the-search-for-hezbollahs-imad-mughniyeh

Qaeda as the prototypical entrepreneurial FTO.[24] Though these groups continued to attack targets overseas, striking the homeland became a primary goal.[25] In the aftermath of the 1993 WTC bombing and disruption of other inchoate plots, the DOJ notched several in-court victories, cementing its enlarged role in U.S. counterterrorism efforts.[26] Also emerging in the mid-1990s were the material support statutes, which despite the urgency with which they were enacted, saw little use pre-9/11.[27]

In the days following the 9/11 attacks, President Bush outlined a broad counterterrorism strategy, calling for the use of military, financial, and diplomatic means, as well as "every instrument of law enforcement."[28] One such instrument since put to much greater use has been the material support statutes.[29] While still below the post-9/11 zenith, there has been a recent resurgence in terrorism-related prosecutions tracking the rise of the Islamic State (commonly referred to as "ISIS"),[30] a group simultaneously compared to both General Motors[31] and Uber,[32] at once highly bureaucratic yet also highly "freewheeling" in the latitude it gives to individual operatives.[33] The greater agility and adaptability of ISIS, al

[https://perma.cc/M88M-Z4AU] (noting the indictment of the Hezbollah leader, but emphasizing CIA kill-or-capture efforts).

[24] Lawrence Wright, The Looming Tower: Al-Qaeda and the Road to 9/11, at 318 (2006).

[25] 9/11 Commission Report, supra note 13, at 59–63 (detailing attacks on U.S. government personnel and facilities overseas in the 1990s and early 2000s).

[26] Id. at 71–73.

[27] See infra Section I.B.

[28] President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001), http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html [https://perma.cc/H438-J8S4].

[29] See infra Subsection I.B.2.

[30] Adam Goldman et al., The Islamic State's Suspected Inroads into America, Wash. Post, http://wapo.st/isis-suspects [https://perma.cc/3X36-FFGC] (counting 109 ISIS-related prosecutions as of February 2017) (last visited Feb. 24, 2017).

[31] ISIS and the Corporatization of Terror, NPR (Nov. 29, 2014, 4:57 PM), https://n.pr/1yoShMz.

[32] Canadian Sec. Intelligence Serv., The Foreign Fighters Phenomenon and Related Security Trends in the Middle East 5 (Jan. 2016).

[33] See, e.g., Sebastian Rotella, ISIS via WhatsApp: 'Blow Yourself Up, O Lion,' PBS Frontline (July 11, 2016), http://www.pbs.org/wgbh/frontline/article/isis-via-whatsapp-blow-yourself-up-o-lion [https://perma.cc/L4HJ-UZQE]. Although this Note examines potential prosecution of companies that deal with terrorists generally, al Qaeda and ISIS are used as familiar and illustrative examples.

Qaeda, and other groups relative to the U.S. government necessitates a similarly resourceful, flexible, and creative approach in response.

B. The Material Support Statutes: Modern-Day "Prosecutor's Darlings?"

Broadly, the material support statutes criminalize harboring, concealing, or providing nearly any type of support to terrorists and designated FTOs. Collectively, they have been described as among "the most significant doctrinal developments in the federal criminal law" since the enactment of organized crime, money laundering, and forfeiture statutes in prior "federal criminal 'war[s],'" providing the U.S. government with powerful means of disrupting terrorist supply chains and preventing attacks.[34]

1. Text and History

Though often referred to generically as the "material support statute," there are in reality several distinct provisions comprising the material support framework.[35] The anchoring provision of the broader framework, 18 U.S.C. § 2339A, defines "material support or resources" as:

> *[A]ny* property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, personnel (1 or more individuals who may be or include oneself), and transportation.[36]

[34] Norman Abrams, The Material Support Terrorism Offenses: Perspectives Derived from the (Early) Model Penal Code, 1 J. Nat'l Sec. L. & Pol'y 5, 6–7 (2005) (likening the statutes to conspiracy, the "prosecutor's darling").

[35] This Note focuses primarily on § 2339B. For a more granular overview of both provisions, see Charles Doyle, Cong. Research Serv., R41333, Terrorist Material Support: An Overview of 18 U.S.C. 2339A and 2339B (2010).

[36] 18 U.S.C. § 2339A(b)(1) (2012) (emphasis added). This broad definition is in turn incorporated into 18 U.S.C. § 2339B. See id. § 2339B(g)(4). Herein, "material support or resources" will be termed "material support."

Only limited exceptions are drawn for medicine and religious materials.[37] Though the word "including" suggests other forms of support not explicitly mentioned could fall within the scope of § 2339A—and by incorporation, § 2339B—the existing categories ("personnel" in particular) have supported prosecution of a wide range of conduct to date, and the statutes have been characterized by prosecutors as "indispensable" to U.S. counterterrorism efforts.[38]

While § 2339A criminalizes providing or concealing support connected with the actual commission of specific terrorism offenses,[39] § 2339B sweeps more broadly, prescribing criminal penalties against "[w]hoever *knowingly* provides material support or resources to a [FTO], or attempts or conspires to do so, . . . [with] *knowledge* that the organization is a designated [FTO] . . . that the organization has engaged or engages in terrorist activity . . . or that the organization has engaged or engages in terrorism[,]" regardless of how or when the support is used.[40] Provision of indirect support through an FTO affiliate or associate has been found sufficient to support § 2339B charges.[41] Sections covering terrorist financing, receipt of military-type training, and harboring of terrorists largely overlap with the above provisions;[42] these have seen less use to date and are thus not in focus in this Note.

[37] Id. § 2339A(b)(1).

[38] Breinholt, supra note 16. For a sampling of the range of recent material support prosecutions, see Press Release, Dep't of Justice, Former Army National Guard Member Arrested for Attempting to Provide Material Support to ISIL (July 5, 2016), https://www.justice.gov/opa/pr/former-army-national-guard-member-arrested-attempting-provide-material-support-isil [https://perma.cc/DQT4-PLX9]; Press Release, Dep't of Justice, ISIL-Linked Hacker Pleads Guilty to Providing Material Support (June 15, 2016), https://www.justice.gov/opa/pr/isil-linked-hacker-pleads-guilty-providing-material-support [https://perma.cc/2FYK-U4MV]; Press Release, Dep't of Justice, Wife of Dead ISIL Leader Charged in Death of Kayla Jean Mueller (Feb. 8, 2016), https://www.justice.gov/opa/pr/wife-dead-isil-leader-charged-death-kayla-jean-mueller [https://perma.cc/A3T8-XFMR].

[39] 18 U.S.C. § 2339A(a) (incorporating by reference several separately criminalized offenses).

[40] Id. § 2339B(a)(1) (emphasis added). The list of FTOs maintained by the State Department presently encompasses sixty-one such groups. Foreign Terrorist Organizations, Bureau of Counterterrorism, U.S. Dep't of State, http://www.state.gov/j/ct/rls/other/des/123085.htm [https://perma.cc/J6WD-KM79] (last visited Nov. 5, 2016).

[41] See, e.g., United States v. Holy Land Found. for Relief & Dev., No. 3:04-CR-240-G, 2007 WL 1498813, at *2 (N.D. Tex. May 23, 2007).

[42] 18 U.S.C. §§ 2339C (financing), 2339D (military-type training), 2339 (harboring).

There are notable distinctions between these sections that impact their applicability to different fact patterns. Most significant is the difference in mens rea between § 2339B, which requires only *knowledge* that the recipient is an FTO or is otherwise involved in terrorism, and § 2339A, which requires *specific intent* to further terrorist acts or at least knowledge that the support provided will be used to further *specific terrorist acts*.[43] Additionally, § 2339A lacks the explicit and broad extraterritorial jurisdiction provisions of § 2339B (which largely parallel those of §§ 2339C[44] and 2339D[45]); however, amendments that removed the predicate of a defendant's presence within the United States suggest Congress also intended for § 2339A to have a degree of extraterritorial reach.[46]

The current material support framework is the product of evolution in response to gains in institutional knowledge and the identification of gaps. While § 2339A defines material support broadly, the nexus requirement created by the intent provision has limited its utility.[47] By contrast, the 1996 enactment of § 2339B has been referred to as "[*t*]*he* watershed legislative development" in efforts to target terrorist infrastructure.[48] Animated by the principle that support is fungible and that facilitating FTOs' "legitimate" activities frees up resources for terrorist activities, these statutes seek to dry up wells of support by targeting for

[43] Compare 18 U.S.C. § 2339B(a)(1) ("knowingly provides material support"), with 18 U.S.C. § 2339A(a) ("provides material support . . . knowing or intending that they are to be used in preparation for, or in carrying out" specific terrorism offenses). See also 18 U.S.C. § 2339C (requiring proof of intent that funds collected are to be used in carrying out specific terrorist acts).

[44] 18 U.S.C. § 2339C(b)(2).

[45] Id. § 2339D(b).

[46] John De Pue, Extraterritorial Jurisdiction and the Federal Material Support Statutes, 62 United States Attorneys' Bulletin (Terrorist Financing) 5, 16, 19–20 (Sept. 2014) (arguing the "plain implication" of amendments enacted in 2001 is that "Congress intended to eliminate § 2339A's jurisdictional restriction and to expand its scope," but also noting the absence of language as explicit as that found in § 2339B).

[47] Andrew Peterson, Addressing Tomorrow's Terrorists, 2 J. Nat'l Sec. L. & Pol'y 297, 317–18, 348 (2008).

[48] A Review of the Tools to Fight Terrorism Act: Hearing Before the Subcomm. on Terrorism, Tech. & Homeland Sec. of the S. Comm. on the Judiciary, 108th Cong. 9–10 (2004) (statement of Barry Sabin, Chief, Counterterrorism Section, Department of Justice) (emphasis added); see also Robert M. Chesney, The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention, 42 Harv. J. on Legis. 1, 12–18 (2005) (discussing the origins of § 2339A and efforts to close the specific intent "loophole" with § 2339B).

prosecution those who provide it.[49] Since their original enactment, these statutes have been amended to broaden their scope and provide insulation from judicial challenge with tightened mens rea provisions.[50] Over time, Congress (with executive branch input) has built a framework that is both operationally malleable and sufficiently solid to withstand most in-court challenges.[51]

2. Historical Application—Notable Successes, Failures, and Trends

Though both §§ 2339A and 2339B were on the books by the mid-1990s, neither was put to substantial use prior to 9/11.[52] Post 9/11, the DOJ quickly acknowledged the necessity of shifting to a prevention-focused stance.[53] The all-tools strategy adopted by the government and subsequent amendments to the material support statutes spurred heavier use by prosecutors, transforming these once-obscure provisions into powerful weapons.[54] In the years following 9/11, the DOJ brought such charges against a range of defendants, among them individuals who fought for the Taliban in Afghanistan,[55] fundraisers,[56] an attorney who helped a jailed FTO leader convey orders to members of his organization,[57] and individuals who maintained websites on behalf of FTOs.[58]

[49] Albeit in a factually narrow case, the Supreme Court approved of the "fungibility" rationale of § 2339B in *Holder v. Humanitarian Law Project*, 561 U.S. 1, 29–37 (2010).

[50] See, e.g., Peterson, supra note 47, at 311–35 (detailing the statutes' evolution, from pre-2339 legislation in the late 1980s through amendments enacted in 2004).

[51] Doyle, supra note 35, at 4–9, 21.

[52] Chesney, supra note 48, at 18–20; Breinholt, supra note 16. Indeed, the 9/11 Commission Report contains only two explicit references to the material support statutes, buried in endnotes. 9/11 Commission Report, supra note 13, at 501 n.24, 504 n.81.

[53] See, e.g., Chesney, supra note 48, at 26–28; Kelly Moore, The Role of Federal Criminal Prosecutions in the War on Terrorism, 11 Lewis & Clark L. Rev. 837, 838–41 (2007).

[54] Breinholt, supra note 16.

[55] See, e.g., Brooke A. Masters, American Taliban Suspect Appears in Alexandria Court, Wash. Post (Jan. 25, 2002), http://wpo.st/uVDV1 [https://perma.cc/HH98-UEKE] (discussing an American captured with Taliban forces in Afghanistan and noting the rarity of material support charges at that point in time).

[56] See, e.g., Wayne Washington, Charity's Leader Charged in al Qaeda Conspiracy, Bos. Globe, Oct. 10, 2002, at A1 (discussing indictment of the leader of a Chicago-area charity on material support and racketeering conspiracy charges).

[57] See, e.g., Michael Powell & Michelle Garcia, Sheik's U.S. Lawyer Convicted of Aiding Terrorist Activity, Wash. Post, Feb. 11, 2005, at A1 (discussing the material support conviction of a lawyer who smuggled messages for a client).

[58] See, e.g., Eric Lipton & Eric Lichtblau, Online and Even near Home, a New Front is Opening in the Global Terror Battle, N.Y. Times, Sept. 23, 2004, at A12 (discussing an indi-

Though this initial wave produced numerous convictions, the DOJ also suffered notable trial losses that illustrated difficulties inherent in pursuing novel theories and prosecuting organizational defendants in this context.[59] Such setbacks and a decreased sense of emergency may have contributed to a tapering off of material support cases in the mid-2000s.[60]

More recently, the DOJ has made heavy use of these statutes to counter the threat posed by ISIS's decentralized model. The tempo of terrorism-related prosecutions since late 2014 is higher than at any time since the immediate post-9/11 period.[61] The DOJ has wielded § 2339B against numerous individuals seeking to fight for ISIS overseas[62] as well as those who have used social media to recruit adherents, incite attacks, and instruct donors on avoiding detection.[63] Though some of the DOJ's

vidual charged with material support of terrorism for registering websites that hosted terrorist material).

[59] Jimmy Gurulé, Unfunding Terror: The Legal Response to the Global Financing of Terrorism 301–10 (2008); Susan Schmidt, Saudi Acquitted of Internet Terror, Wash. Post, June 11, 2004, at A3.

[60] See, e.g., Ctr. on Law & Sec., N.Y.U. Sch. of Law, Terrorist Trial Report Card: September 11, 2001–September 11, 2011, at 10, 18–21 (2011), http://www.lawandsecurity.org/wp-content/uploads/2011/09/TTRC-Ten-Year-Issue.pdf [https://perma.cc/D6M6-ANYC] (charting the use of material support charges after 2001).

[61] Retweets to Raqqa, supra note 21, at 5–6 (noting more terrorism arrests in 2015 than in any year post-9/11). The recent spike in federal terrorism prosecutions has by no means been limited to suspects connected to or inspired by ISIS; however, ISIS-related cases brought since 2014 have dominated and are used in this Note to illustrate the agility of both modern FTOs and the material support statutes more generally.

[62] Program on Extremism, George Washington Univ., GW Extremism Tracker: Terrorism in the United States (Mar. 2017) [hereinafter Extremism Tracker], https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/March%202017%20Update.pdf [https://perma.cc/XPL4-856Q] (noting 45% of the 117 individuals charged on offenses related to ISIS since March 2014 either attempted to or successfully traveled abroad to support the group); see also Phil Hirschkorn, Conviction in First ISIS Trial in the U.S. Underscores Foreign Fighter Threat, PBS NewsHour (Mar. 12, 2016, 5:21 PM), http://to.pbs.org/1SjQCTU [https://perma.cc/4N6Y-2XKL] (discussing the material support conviction of a U.S. Air Force veteran accused of attempting to travel to Syria to aid ISIS and ISIS-related prosecutions more broadly).

[63] See, e.g., Mark Berman, Mississippi Couple Accused of Using Honeymoon as Cover to Join Islamic State Plead Guilty, Wash. Post (Mar. 30, 2016), http://wpo.st/CHPR2 [https://perma.cc/Q29F-U8ES] (attempting to travel to Syria to enlist in ISIS); Devlin Barrett, U.S. Charges Man in Malaysia with Hacking, Aiding Islamic State, Wall St. J. Online (Oct. 15, 2015, 8:47 PM), http://on.wsj.com/1PkBDs6 (posting addresses of U.S. military personnel); David Kravets, Jihadist US Teen Gets 11 Years for Blog, Tweets About Crypto and Bitcoin, Ars Technica (Aug. 29, 2015, 5:35 PM), http://arstechnica.com/tech-policy/2015/08/jihadist-us-teen-gets-11-years-for-blog-tweets-about-crypto-and-bitcoin

more aggressive applications of § 2339B are as-yet untested in court, government victories in trials of ISIS supporters in 2016 and early 2017 suggest the statute is sufficiently flexible to support creativity.[64]

One significant gap has been in the corporate context. With the exception of a number of cases involving charities post-9/11, there have been relatively few organizational prosecutions to date, and entities charged have generally been alter egos of individual supporters rather than presumably neutral third parties.[65] Further, in other suspected terrorist-financing cases, the DOJ has brought only lesser charges related to reporting and licensing violations.[66] The only large, mainstream company charged with terrorism-related offenses to date is produce giant Chiquita, which in 2007 pleaded guilty to a single IEEPA count and paid a $25 million criminal penalty for willfully making repeated payments to a Colombian FTO; facts detailed by prosecutors in court filings and press releases also met the standard for material support.[67] This dearth of organ-

[https://perma.cc/5JWE-G7XW] (giving advice on the use of Bitcoin and encryption software).

[64] See, e.g., Jack Healy & Matt Furber, 3 Somali-Americans Found Guilty of Trying to Join Islamic State, N.Y. Times (June 3, 2016), http://nyti.ms/1TNOtgF; Hirschkorn, supra note 62; Fernanda Santos, Guilty Verdict for Aiding in Attack on Anti-Islam Cartoon Event in Texas, N.Y. Times (Mar. 17, 2016), http://nyti.ms/1XyzcD0. See also Press Release, U.S. Dep't of Justice, Arizona Man Convicted in Manhattan Federal Court for Material Support to ISIS (Jan. 30, 2017), https://www.justice.gov/usao-sdny/pr/arizona-man-convicted-manhattan-federal-court-material-support-isis [https://perma.cc/6CBE-446N] (providing statement from then-U.S. Attorney Preet Bharara that the material support conviction of an individual accused of recruiting for ISIS "show[s] that terrorists and terrorist enablers can be brought to justice fairly, openly, and swiftly in the crown jewel of our justice system—civilian courts").

[65] See, e.g., Press Release, Dep't of Justice, Two British Nationals Plead Guilty to Terrorism-Related Charges in New Haven Federal Court (Dec. 10, 2013), https://www.justice.gov/sites/default/files/nsd/legacy/2014/07/23/12.10.2013-nsd.pdf [https://perma.cc/45X7-28QR] (detailing support provided to Chechen mujahideen and the Taliban through the entity Azzam Publications); Benjamin Weiser, A Guilty Plea in Providing Satellite TV for Hezbollah, N.Y. Times (Dec. 23, 2008), http://nyti.ms/1XCBxMZ [private] (discussing case against the owner of a small satellite television provider for distributing programming of Hezbollah-run Al Manar).

[66] Michael Freedman, The Invisible Bankers, Forbes (Oct. 17, 2005, 12:00 AM), http://www.forbes.com/global/2005/1017/024A.html [https://perma.cc/968E-YSDF] (discussing difficulties encountered by U.S. authorities in proving ties between money-transfer services and FTOs).

[67] Information at 16–17, United States v. Chiquita Brands Int'l, Inc., No. 1:07-cr-00055-RCL (D.D.C. Mar. 14, 2007); Press Release, Dep't of Justice, Chiquita Brands International Pleads Guilty to Making Payments to a Designated Terrorist Organization and Agrees to Pay

izational prosecutions may reflect several factors, including evidentiary gaps and lessons learned from trial setbacks in the mid-2000s, such as the initial mistrial in the Holy Land Foundation ("HLF") terror-finance prosecution.[68] However, as discussed in Part III, conditions appear ripe for application in the mainstream corporate realm.

3. Challenges and Critiques

To date, the material support statutes have largely withstood judicial scrutiny.[69] This is owed in large part to the broad definitions set forth in § 2339A(b), the nexus requirement of § 2339A(a), and amendments to § 2339B that clarified the required mens rea. Courts have found the statutes sufficiently clear and narrow, and in 2010 the Supreme Court handed the DOJ a notable victory in *Holder v. Humanitarian Law Project*, rejecting pre-enforcement challenges by nonprofits that sought to provide training to the political arms of two FTOs.[70] Though the case did not involve actual prosecution and the Court confined its opinion to narrow facts,[71] its rejection of vagueness and overbreadth challenges even in the First Amendment context appears likely to do some work in support of broad interpretations of the material support statutes in future cases.

Beyond legal challenges, academic critiques of the material support statutes have been persistent. The bulk of these critiques echo constitutional challenges raised by defendants, including nondelegation concerns related to FTO designation, claims of overbreadth and chilling of First Amendment activity, and issues with the lower level of scienter required

$25 Million Fine (Mar. 19, 2007) [hereinafter DOJ Chiquita Press Release], https://www.justice.gov/archive/opa/pr/2007/March/07_nsd_161.html [https://perma.cc/8294-PU9Q]. For additional discussion of the Chiquita case, see infra Subsection I.C.2.

[68] See, e.g., Gurulé, supra note 59, at 305–10; Elizabeth J. Shapiro, The Holy Land Foundation for Relief and Development: A Case Study, 62 U.S. Attorneys' Bulletin (Terrorist Financing) 5, 23, 28–30 (Sept. 2014).

[69] Gurulé, supra note 59, at 281–93 (discussing failed challenges to §§ 2339A and 2339B); Doyle, supra note 35, at 4–9 (same).

[70] Holder v. Humanitarian Law Project, 561 U.S. 1, 7–8 (2010).

[71] Robert Chesney, The Supreme Court, Material Support, and the Lasting Impact of *Holder v. Humanitarian Law Project*, 1 Wake Forest L. Rev. F. 13, 18–19 (2010) ("[I]t is tempting to treat *Holder v. Humanitarian Law Project* as a sweeping victory for the government . . . . But this would be premature if not foolish.").

under § 2339B.[72] Such concerns have been raised with regard to the DOJ's more novel prosecutions, though it appears even free-speech concerns have yielded somewhat in light of ISIS's affinity for "crowdsourcing" attacks through social media and other online outreach.[73] With many recent defendants pleading guilty rather than facing trial, it remains to be seen whether critiques of the statutes, § 2339B in particular, will see new life in the courts with this latest wave of cases.[74]

Lastly, despite the prevailing assessment that the material support statutes are crucial to U.S. counterterrorism efforts, operational critiques remain. Concerns with the list-based approach of § 2339B, which limits its reach to the provision of support to designated FTOs, are valid and salient. While this approach cabins § 2339B's scope and allays constitutional concerns (at least somewhat), it has been criticized as hampering counterterrorism efforts given designation delays and shifts toward informal allegiances.[75] Unintended consequences of early incapacitation are also worth noting. Counterterrorism efforts are aided significantly by open-source intelligence ("OSINT") on the Internet; aggressive prosecution of recruiters, propagandists, and others may push more communica-

[72] See, e.g., Wadie E. Said, Crimes of Terror: The Legal and Political Implications of Federal Terrorism Prosecutions 51–72 (2015) (criticizing judicial deference and increasingly broad statutory applications); David Cole, Out of the Shadows: Preventive Detention, Suspected Terrorists, and War, 97 Calif. L. Rev. 693, 723–25 (2009) (supporting a specific intent requirement for § 2339B).

[73] See, e.g., Erik Eckholm, ISIS Influence on Web Prompts Second Thoughts on First Amendment, N.Y. Times (Dec. 27, 2015), http://nyti.ms/1mcy2AP.

[74] Extremism Tracker, supra note 62 (noting 58 of 109 individuals charged with ISIS-related offenses as of December 2016 have pleaded guilty or been convicted). For reports noting the dearth of ISIS-related trials and trial convictions thus far, see Hirschkorn, supra note 62; see also Dan Frosch, Arizona Man Sentenced for Planning Islamic State-Inspired Attack in Texas, Wall St. J. Online (Feb. 8, 2017, 7:51 PM), https://www.wsj.com/articles/arizona-man-sentenced-for-planning-islamic-state-inspired-attack-in-texas-1486595045 (describing the trial of an ISIS supporter from Phoenix as a "test case for the government" and noting the low number of similar trials to date).

[75] Peterson, supra note 47, at 343–48; see also Robert M. Chesney, Beyond Conspiracy? Anticipatory Prosecution and the Challenge of Unaffiliated Terrorism, 80 S. Cal. L. Rev. 425, 436–40 (2007) (discussing limitations of the FTO-based approach). The San Bernardino attackers' neighbor was charged under § 2339A for providing guns for the attack, but not under § 2339B. Though one of the shooters pledged allegiance to ISIS on Facebook during the rampage, the DOJ did not allege the neighbor knew either of them were ISIS adherents. Criminal Complaint at 2, 11, 21, United States v. Marquez, No. 15-MJ-00498 (C.D. Cal. Dec. 17, 2015).

tions underground.[76] Early disruption of plots through aggressive application of the material support statutes and other criminal laws may also tip off bad actors or associates not known to the government, and balancing prevention against intelligence gathering remains a challenge.[77]

C. IEEPA

Of a less-recent vintage is IEEPA, which broadly proscribes transactions with countries, individuals, and entities designated by the President through executive order.[78] This Note focuses primarily on the use of IEEPA's criminal provisions to enforce terrorism-related sanctions promulgated through Executive Order 13224 ("E.O. 13224"), enacted in the wake of 9/11.

1. Text and History

IEEPA provides the President with tools to "deal with any unusual and extraordinary threat" originating in substantial part outside of the United States and relating to the U.S. economy, foreign policy, or national security.[79] These powers include the authority to issue further regulations to freeze property and to investigate, block, and prohibit nearly *any* transaction with some nexus to a declared national emergency.[80] Parties subject to sanctions are designated through Executive Order.[81] IEEPA further establishes a penalty regime whereby civil penalties may be imposed on a strict liability basis against anyone who "violate[s], attempt[s] to violate, conspire[s] to violate, or cause[s] a violation of any

[76] See, e.g., Andrew V. Moshirnia, Valuing Speech and Open Source Intelligence in the Face of Judicial Deference, 4 Harv. Nat'l Sec. J. 385, 394, 433–36 (2013) ("In the words of one intelligence official, '[OSINT] is no longer the icing on the cake, it is the cake itself.'" (citation omitted)).

[77] See Chesney, supra note 75, at 433–34 (discussing the "early intervention dilemma" and noting potential negative effects on the ability of authorities to identify associates and obtain cooperation from the community); see also Michael S. Schmidt et al., U.S. Investigators Struggle to Track Homegrown ISIS Suspects, N.Y. Times (Nov. 19, 2015), http://nyti.ms/1X0oOrM (outlining challenges law enforcement faces in monitoring so-called lone wolves).

[78] 50 U.S.C. §§ 1701–1708 (2012).

[79] Id. § 1701(a).

[80] Id. §§ 1702(a)(1), 1704.

[81] See Geoffrey Corn et al., National Security Law: Principles and Policy 374–76 (2015).

license, order, regulation, or prohibition" issued pursuant to the statute.[82] Criminal penalties are prescribed against anyone "who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of" a violation of orders, regulations, or prohibitions issued pursuant to IEEPA.[83]

Since its enactment in 1977, IEEPA has proven itself a powerful tool, enabling the President to block transactions with entire countries as well as individuals and entities. The strategy of applying targeted "smart sanctions" against non-state actors emerged in the mid-1990s and has since been expanded significantly.[84] At present, the United States maintains "an intricate array of lists" of terrorist groups, operatives, and facilitators subject to freezing and blocking under E.O. 13224.[85] Issued shortly after 9/11, the Order imposes sanctions against specific foreign terrorists and any persons supporting "or otherwise associate[d]" with foreign terrorists to attack their financial resources,[86] and the list of Specially Designated Global Terrorists ("SDGTs") designated pursuant to E.O. 13224 has expanded to encompass several hundred individuals and entities.[87] In the present context, the continued growth of the SDGT list increases the potential exposure to prosecution of companies that deal with these parties and their cohorts.

2. Usage of Criminal IEEPA Provisions in the E.O. 13224 Context

One of IEEPA's most significant contributions is the broad asset-freezing and transaction-blocking authorities it grants.[88] The designation

[82] 50 U.S.C. § 1705(a)–(b).

[83] Id. § 1705(c).

[84] See, e.g., R. Richard Newcomb & Mark D. Roberts, An Introduction to Economic Sanctions: A Brief History and the Basic Tools, *in* National Security Law & Policy 1331–34, 1341–47 (John Norton Moore et al. eds., 3d ed. 2015).

[85] Audrey Kurth Cronin, Cong. Research Serv., RL32120, The "FTO List" and Congress: Sanctioning Designated Foreign Terrorist Organizations 5 (2003).

[86] Exec. Order No. 13,224, 31 C.F.R. § 595 (2001).

[87] Office of Foreign Assets Control, U.S. Dep't of the Treasury, What You Need to Know About U.S. Sanctions (last updated Apr. 5, 2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/terror.pdf [https://perma.cc/KPD5-3L56]. Current E.O. 13224 designees range from the unsurprising (FTOs such as ISIS and al-Shabaab) to the amusing (front entities such as Wonderland Amusement Park). Id.

[88] Cf. David D. Aufhauser, Terrorist Financing—The Privatization of Economic Sanctions, 56 Fed. Law. 22, 24 (2009) (noting E.O. 13224's "profound effect on the international financial community").

process and the pressure the United States is able to exert on foreign institutions provide the government with powerful means of drying up terrorists' assets and denying access to financial networks.[89] Though there has been an uptick in high-profile criminal IEEPA cases in recent years, these have thus far primarily involved violations of country-based sanctions.[90] Criminal IEEPA cases involving dealings with SDGTs have largely been limited to the context of direct terrorist finance.[91] The DOJ's relatively limited forays into prosecution in this realm have demonstrated the challenges in proving willful violations of E.O. 13224 sanctions and the complexity of terrorism-support cases generally, factors which may cut against criminal prosecution on the margins or in favor of lesser charges.[92] Such difficulties may be even more pronounced when potential corporate defendants lack a physical presence within the United States, as can arguably be inferred from the DOJ's decision to pursue civil forfeiture, rather than criminal charges, against a Lebanese bank it accused of laundering money for parties tied to the FTO Hezbollah.[93]

The Chiquita case noted above serves as the lone example of a major company that has been charged criminally for E.O. 13224–based IEEPA violations, as distinguished from violations of country-based sanctions. Further, this prosecution was based upon largely indisputable evidence that the company knowingly and willfully violated both IEEPA and § 2339B by making protection payments to a Colombian FTO that con-

[89] See generally Suzanne Katzenstein, Dollar Unilateralism: The New Frontline of National Security, 90 Ind. L.J. 293 (2015) (discussing the "harnessing of foreign banks" through a carrot-and-(mostly)-stick approach).

[90] Hong, supra note 19.

[91] Id.

[92] Gurulé, supra note 59, at 299–301, 303–10 (providing background on IEEPA and E.O. 13224, and outlining "disappointing legal setbacks" in early post-9/11 terrorism trials); Shapiro, supra note 68, at 28–30 (detailing differences in the DOJ's approach between the first and second Holy Land Foundation trials, which included pursuing fewer charges and "repackaging to make the case more digestible to the jury" in the latter trial); see also Freedman, supra note 66 (discussing difficulties in tying individual supporters to FTOs).

[93] Sharon Cohen Levin & Carolina A. Fornos, Using Criminal and Civil Forfeiture to Combat Terrorism and Terrorist Financing, 62 U.S. Attorneys' Bulletin (Terrorist Financing) 5, 42, 45–46 (Sept. 2014) (providing overview of the Lebanese Canadian Bank case and noting the utility of civil forfeiture "[p]articularly where the putative defendant is overseas"); see also Jeffrey Alberts, The Rise of the Civil Money Laundering Prosecution, N.Y. L.J., Feb. 10, 2014, at S4 (detailing an increase in civil forfeiture prosecutions and potential strategy-related explanations for the trend).

trolled areas in which it maintained banana-producing operations.[94] Though the company voluntarily disclosed to DOJ officials that it had made payments to the FTO in an April 2003 meeting, a factor often considered in charging decisions, Chiquita's situation was further complicated by the fact that it continued making illegal payments for nearly a year after this meeting.[95] Notably, a subsequent internal investigation conducted in connection with a shareholder suit found Chiquita's management was firmly against accepting any plea agreement involving material support charges, given the "implication that the offender is 'in bed' with the terrorist organization."[96]

3. Challenges and Critiques

Many of the legal challenges mounted against IEEPA in the E.O. 13224 context have focused on the designation process and have been raised by parties added to the Office of Foreign Assets Control's ("OFAC's") list of SDGTs. Courts have been largely deferential to the government and unreceptive to due process, nondelegation, vagueness, and other constitutional claims raised by designees.[97] In the prosecution context, the higher willfulness requirement of IEEPA's criminal provi-

[94] DOJ Chiquita Press Release, supra note 67. Chiquita became aware in early 2003 that it had been making payments to a Colombian FTO; the company continued to make payments against the "persistent advice of its outside counsel" until early 2004. Id.

[95] Laurie P. Cohen, Chiquita Under the Gun: After Disclosing Payments to Colombian Terrorists, Company Officials Face Legal Jeopardy, Wall St. J., Aug. 2, 2007, at A1 (discussing Chiquita-DOJ meetings and quoting an internal Chiquita memorandum that stated "[w]e appear to [be] committing a felony" (second alteration in original)).

[96] Special Litig. Comm., Report of the Special Litigation Committee: Chiquita Brands International, Inc. 139–40 (Feb. 2009) http://nsarchive.gwu.edu/NSAEBB/NSAEBB340/chiquita-slc-report.pdf [https://perma.cc/E2WP-Y9AX] ("[T]he Company was concerned that a plea under § 2339B could potentially cause devastating global public relations issues . . . .").

[97] Gurulé, supra note 59, at 201–14 (discussing designation challenges); see also Corn et al., supra note 81, at 423 ("U.S. courts have upheld sanctions to serve foreign policy goals. . . . [and] rarely second-guess the substance of sanctions decisions."); see also Humanitarian Law Project v. U.S. Treasury Dep't, 578 F.3d 1133, 1138 (9th Cir. 2009) (rejecting a pre-enforcement challenge and rejecting several constitutional challenges to IEEPA and E.O. 13224). But see Al Haramain Islamic Found. v. U.S. Dep't of Treasury, 686 F.3d 965, 1001 (9th Cir. 2012) (finding specific OFAC restrictions on advocacy-related activities violated the First Amendment).

sions likely does significant work in reducing both as-applied and facial challenges.[98]

Academic critiques of IEEPA and E.O. 13224 echo those made of the material support statutes to a degree, particularly with respect to First Amendment speech and associational freedoms.[99] Critics have also expressed concern regarding the disparate impact of designations on Muslim charities, alleging the U.S. government has unfairly singled out such groups and their donors.[100] The propriety of OFAC's control over designation has also been questioned, characterized as "activit[y] that look[s] a lot like criminal law enforcement . . . without the usual protections of criminal procedure."[101] OFAC has further been portrayed as overburdened and operating outside of its traditional area of expertise with near-absolute discretion.[102] Though designation is not the focus of this Note, it necessarily feeds into the IEEPA penalty regime.

Operationally, IEEPA employs a list-based approach similar to § 2339B (though SDGT and similar lists are far larger than the FTO list), and thus is subject to a similar critique.[103] Concern that early intervention may dry up intelligence is salient here as well.[104] Designation has the immediate effect of freezing a designee's assets and barring nearly all transactions with it, explicitly in the United States and increas-

[98] 50 U.S.C. § 1705(c) (2012). One district court has read a specific intent requirement into IEEPA. Gurulé, supra note 59, at 299–301 (discussing the decision of the U.S. District Court for the Middle District of Florida in *United States v. Al-Arian*, 308 F. Supp. 2d 1322 (M.D. Fla. 2004)). This reading was rejected by the Ninth Circuit and has not been adopted widely. *Humanitarian Law Project*, 578 F.3d at 1152 (9th Cir. 2009); see also, e.g., United States v. Elashyi, 554 F.3d 480, 505 (5th Cir. 2008) ("As other courts have noted, adding a requirement that the defendant have the specific intent to further the terrorists' unlawful activities would effectively rewrite [IEEPA] . . . . We decline to follow *Al-Arian* here." (citations omitted)). It is worth noting that the mens rea of IEEPA's criminal provision still has been criticized as being *too* demanding by supporters of more aggressive use of prosecution in the counterterrorism context. See Gurulé, supra note 59, at 310 (arguing Congress should amend § 1705(c) to bring it in line with § 2339B's "knowing" requirement).

[99] See, e.g., Laura K. Donohue, Constitutional and Legal Challenges to the Anti-Terrorist Finance Regime, 43 Wake Forest L. Rev. 643, 670–73 (2008).

[100] Id. at 673–75.

[101] David Zaring & Elena Baylis, Sending the Bureaucracy to War, 92 Iowa L. Rev. 1359, 1403 (2007).

[102] Id. at 1399–404.

[103] See Chesney, supra note 75, at 436–40; Peterson, supra note 47, at 343–48 (arguing "[t]he FTO approach cannot deal effectively with dynamic networks accelerated by cyber-jihad").

[104] See supra notes 76–77 and accompanying text.

ingly by default overseas.[105] While the importance of depriving terrorists and facilitators of resources and access to financial networks cannot be understated, sanctions also push activity underground to alternative payment systems, a financial blackout that impedes law enforcement and intelligence efforts.[106] Lastly, both advocates and critics of the aggressive use of IEEPA have noted the substantial burden compliance places on the private sector and the potential for alienation of firms through overuse, which may chill proactive cooperation.[107]

II. CORPORATE CRIMINAL LIABILITY

To even casual observers, investigations and prosecutions of large companies have become a fixture of U.S. news.[108] General acceptance of (or resignation to) principles of corporate criminal liability and the DOJ's recent actions suggest no material shift is forthcoming, and that it may actually double down on targeting firms.[109] For present purposes, this arguably cuts in the direction of a heightened risk of prosecution for firms that do business with terrorists, where the DOJ has demonstrated a strong focus on both corporate crime and counterterrorism. This Part first provides background principles of corporate criminal liability, discusses doctrinal issues of proving knowledge and intent, and notes critiques of the American approach to corporate criminal liability. The Part concludes with illustrative examples of how the DOJ has targeted bad

[105] Katzenstein, supra note 89, at 315–21 (discussing "financial sticks" used to give teeth to sanctions outside of the United States).

[106] For an illustration of the difficulties in tracking funds through informal networks, see Giovanni Legorano & Joe Parkinson, Following the Migrant Money Trail, Wall St. J. (Dec. 30, 2015, 1:57 PM), http://on.wsj.com/1mpkVvD.

[107] Juan C. Zarate, Harnessing the Financial Furies: Smart Financial Power and National Security, 32 Wash. Q. 43, 43, 56–57 (Oct. 2009); cf. Zaring & Baylis, supra note 101, at 1405–07, 1417–18 (describing burdens on financial institutions from post-9/11 anti–money laundering and terrorist financing regulations).

[108] See, e.g., Devlin Barrett & Evan Perez, HSBC to Pay Record U.S. Penalty, Wall St. J. (Dec. 11, 2012, 7:04 AM), http://on.wsj.com/W0Psne; Ben Protess & Jessica Silver-Greenberg, Two Giant Banks, Seen as Immune, Become Targets, N.Y. Times: DealBook (Apr. 29, 2014, 8:40 PM), http://nyti.ms/1hbPbAR.

[109] See, e.g., Ricciuti et al., supra note 7 ("As the DOJ has pledged, it is increasingly looking to make white collar cases, and can be expected to harness all of the tools in its formerly blue collar arsenal—and even new ones developed just for white collar cases—in which to do so."); Ring & Coleman, supra note 7 (discussing the "growing trend" of the DOJ pursuing "companies and individuals whose compliance programs fail to prevent others' wrongdoing").

actors through detached (that is, not co-opted) corporate intermediaries in the past to set the stage for discussion in Part III of such an approach in the counterterrorism context.

A. Background and Evolution

In a decision with far-reaching impact, the Supreme Court held in 1909 in the case of *New York Central & Hudson River R.R. Co. v. United States* that a corporation could be held *criminally* liable for its agents' acts by extending the tort principle of respondeat superior.[110] Though the Court's opinion only addressed corporate liability under one particular statute, federal courts have since applied the same reasoning expansively and nearly across the board.[111] Broadly, the actions, knowledge, and intent of *any agent* may be imputed to his or her employer, if the agent acts within the scope of employment and at least partly intended to benefit the company.[112]

This sweeping and oft-criticized view of entity liability has been described as necessary to hold business organizations accountable where countless actions are taken far from the view of upper management and responsibility is often diffuse.[113] Broad corporate criminal liability for the acts of agents is further seen as in the public interest given the magnitude of harm that firms may cause in the course of business.[114] Though seemingly a minority view given the volume and vehemence of critiques, scholars have argued persuasively that entity liability is generally consistent with the broader aims of criminal law, including deterrence

[110] 212 U.S. 481, 494–495 (1909).

[111] Brandon L. Garrett, Too Big to Jail: How Prosecutors Compromise with Corporations 33–36 (2014) [hereinafter Garrett, Too Big to Jail]; see also V.S. Khanna, Corporate Criminal Liability: What Purpose Does it Serve? 109 Harv. L. Rev. 1477, 1479–88 (1996) (tracing the evolution of entity liability).

[112] See, e.g., Charles Doyle, Cong. Research Serv., R43293, Corporate Criminal Liability: An Overview of Federal Law 3–4 (2013).

[113] See, e.g., United States v. Bank of New England, N.A., 821 F.2d 844, 856 (1st Cir. 1987) (finding a "collective knowledge" jury instruction "not only proper but necessary" given the bank's compartmentalized operations); United States v. Hilton Hotels Corp., 467 F.2d 1000, 1006 (9th Cir. 1972) (discussing the difficulty in identifying agents responsible for wrongdoing in large firms, and finding corporate prosecution "appropriate and effective").

[114] See, e.g., Sara Sun Beale, A Response to the Critics of Corporate Criminal Liability, 46 Am. Crim. L. Rev. 1481, 1483–85 (2009) ("[C]orporations have the ability to engage in misconduct that dwarfs that which could be accomplished by individuals.").

and retribution, despite the fact that entities themselves are legal fictions.[115] Fundamentally, the specter of *New York Central*–type liability may incentivize companies to undertake efforts to ensure compliance with the law. Where such controls are not implemented or fail, and crimes are committed in the name of the company, the law provides for potentially severe sanctions.

Corporate criminal liability has been described as a "form of American Exceptionalism"[116] whereby both domestic and foreign firms may be subject to harsh or even company-ending penalties, including in some cases for conduct occurring largely outside of the United States.[117] This increasingly credible threat, demonstrated by upticks in corporate prosecutions, is arguably a powerful weapon in the DOJ's arsenal that can be used to socialize firms, particularly non-U.S. firms that may be less regulated at home or less solicitous of U.S. laws.[118] Recent high-profile criminal IEEPA cases, many of which have involved flagrant sanctions-busting by non-U.S. institutions, are illustrative.[119] These cases are also indicative of a broader DOJ priority of prosecuting corporate crime as a means of reinforcing overarching policies and appear to reflect a more strategic approach that has developed in recent years.[120] The DOJ's demonstrated willingness to go after both U.S. and non-U.S. companies,

[115] See, e.g., Samuel W. Buell, The Blaming Function of Entity Criminal Liability, 81 Ind. L.J. 473, 500–10 (2006) (discussing deterrent effects flowing from reputational concerns); Lawrence Friedman, In Defense of Corporate Criminal Liability, 23 Harv. J.L. & Pub. Pol'y 833, 852–53 (2000) (distinguishing corporations from their agents and arguing corporate convictions can be viewed as "the effectuation of expressive retribution").

[116] Brandon L. Garrett, Globalized Corporate Prosecutions, 97 Va. L. Rev. 1775, 1777–78 (2011).

[117] Id. at 1788–93.

[118] Cf. id. at 1849–51 (discussing "globalized deterrence").

[119] Ben Protess, German Bank to Pay $1.5 Billion in U.S. Case, N.Y. Times, March 13, 2015, at B1 (describing IEEPA as "a sore spot for many European banks"); cf. Katzenstein, supra note 89, at 320–21 (discussing sanctions-related fines levied against HSBC, BNP Paribas, and others, and suggesting these institutions may have been insufficiently deterred from violating U.S. sanctions prior to this wave of prosecutions).

[120] See U.S. Dep't of Justice, United States Attorneys' Manual § 9-28.000 [hereinafter USAM], https://www.justice.gov/usam/united-states-attorneys-manual [https://perma.cc/D9ZD-FT3G] (last visited Feb. 11, 2017); see also Garrett, Globalized Corporate Prosecutions, supra note 116, at 1776–77 (noting the DOJ "publicizes its goal to 'root out global corruption' and . . . ensure 'the stability and security of domestic and global markets'" through use of various prosecutorial tools (citation omitted)).

including large firms, weighs in favor of the potential IEEPA and material support applications discussed in Part III.

Though the DOJ brought noteworthy corporate cases prior to the 2000s, it was only in 1999 that it issued formal guidance to prosecutors on corporate charging decisions.[121] Though nonbinding, these guidelines have evolved to address factors that include the seriousness of the alleged offenses, corporate cooperation, the existence and strength of compliance programs, potential collateral effects, and the adequacy of noncriminal sanctions.[122] Continual adjustment of these guidelines alongside charging documents, reports of ongoing investigations, and statements of DOJ officials suggest this latest Golden Age of white collar (and gray collar) prosecutions is not yet near its end, and that the Department is fine-tuning its approach.[123] Further, the embrace of corporate prosecution to combat intermediary-facilitated crime, discussed further below in Part III, suggests this may also be a viable tool in U.S. counterterrorism efforts.

B. Proof of Knowledge/Intent in the Corporate Context

Even if one accepts the premise that entities *should* be subject to criminal liability, there is the matter of proving a company not only committed the bad acts, but that it also had the requisite mens rea.[124] As noted above, the knowledge and intent of a company's agents are gener-

[121] Garrett, Too Big to Jail, supra note 111, at 55–56.

[122] USAM § 9-28.000; see also Brian Cromwell, New DOJ Corporate Prosecution Guidelines, Public Company Growth & Compliance, Parker Poe Adams & Bernstein LLP (Oct. 12, 2015), http://pcgc.parkerpoe.com/new-doj-corporate-prosecution-guidelines [https://perma.cc/T63Z-AUPN] (detailing the evolution of DOJ corporate prosecution guidelines since the 1999 "Holder Memo").

[123] See, e.g., A Mammoth Guilt Trip: Criminalizing the American Company, Economist (Aug. 30, 2014), http://econ.st/VPeyo2 [https://perma.cc/G82G-ZD82] (expressing concern over the aggressiveness of U.S. prosecutors toward corporations); Ricciuti et al., supra note 7 ("The DOJ's 'gray collar' crime approach appears to be here to stay.").

[124] See generally Arthur Leavens, Beyond Blame—*Mens Rea* and Regulatory Crime, 46 U. Louisville L. Rev. 1 (2007–08) (examining strict liability where statutes are silent). Both the material support statutes and IEEPA contain explicit mens rea provisions. 18 U.S.C. § 2339B(a)(1) (2012) (providing for criminal penalties against "[w]hoever *knowingly* provides material support or resources" to an FTO, "or attempts or conspires to do so" (emphasis added)); 50 U.S.C. § 1705(c) (2012) (providing for criminal penalties against "[a] person who *willfully* commits, *willfully* attempts to commit, or *willfully* conspires to commit, or aids or abets in the commission of" acts proscribed by § 1705(a) (emphasis added)).

ally imputed to it.[125] Though fairly straightforward when the bad act and bad intent can be traced to specific employees, this may not be the scenario confronted when prosecutors investigate large, complex entities. Decision and execution authority is often diffuse in such organizations and may only cover parts of the broader conduct at issue; communications may also be siloed, making it difficult or impossible to pinpoint the locus of wrongdoing.[126] Some courts have thus in extreme cases allowed theories of collective knowledge, under which the knowledge and intent of *all* involved agents, none of whom could be found guilty individually, are aggregated and imputed to the entity.[127] Recognizing challenges posed by corporate siloing, the U.S. Court of Appeals for the First Circuit seemingly opened the door to further application of such theories in *United States v. Bank of New England, N.A.*[128] The court's logic regarding collective knowledge in this particular case, while arguably appealing to prosecutors and unfavorable to potential corporate defendants, may ultimately have spurred more debate than application.[129] While still good law in the First Circuit, persuasive arguments have been made that a collective knowledge theory should not be (and in reality is not) applied without clear indicia that management avoided acquiring bad facts in attempts to shield the firm from liability.[130] Indeed, *Bank of New England* itself involved not the aggregation of innocent knowledge of agents, but aggregation where the bank exhibited flagrant organizational indifference and consciously avoided learning legal requirements.[131]

[125] See supra note 112 and accompanying text; see also Irina Kotchach Bleustein et al., Corporate Criminal Liability, 52 Am. Crim. L. Rev. 851, 858–63 (discussing imputed knowledge and intent).

[126] See, e.g., David Ingram, Corporate 'Siloing' an Obstacle to Charging GM Employees: Prosecutor, Reuters (Sep. 17, 2015, 6:13 PM), http://reut.rs/1Mf9G0X [https://perma.cc/P455-WCXZ].

[127] See, e.g., Patricia S. Abril & Ann Morales Olazábal, The Locus of Corporate Scienter, 2006 Colum. Bus. L. Rev. 81, 114–21.

[128] 821 F.2d 844, 856 (1st Cir. 1987) ("It is irrelevant whether employees administering one component of an operation know the specific activities of employees administering another aspect of the operation . . . .").

[129] Garrett, Too Big to Jail, supra note 111, at 270 & n.84; Abril & Olazábal, supra note 127, at 116–17 & n.133, 119–21.

[130] Abril & Olazábal, supra note 127, at 120–21; see generally Thomas A. Hagemann & Joseph Grinstein, The Mythology of Aggregate Corporate Knowledge: A Deconstruction, 65 Geo. Wash. L. Rev. 210 (1997) (arguing collective knowledge is merely a corollary to willful blindness).

[131] Hagemann & Grinstein, supra note 130, at 218–20.

Collective knowledge persists as a potential theory of liability, though its availability may turn on indicia of willfulness and the court in which a case is brought.[132]

That the knowledge and intent of a company's agents is imputed to it is critical for prosecutors; however, this also creates incentives to remain ignorant of bad facts and unaware of wrongdoing. Fittingly, doctrines of conscious avoidance (also known as "willful blindness" or "deliberate ignorance") have evolved and been applied in corporate prosecutions to close this potential loophole, including in *Bank of New England*.[133] Broadly, avoidance must go beyond negligent or reckless ignorance to support a finding of knowledge or willfulness. Willful blindness generally requires proof of a subjective belief that specific facts very likely exist and deliberate actions taken to avoid learning those facts, such that a defendant "can almost be said to have actually known" the information.[134]

Though willful blindness does not suffice on its own to establish purpose or willfulness, it can be used as partial proof to establish that a firm's violation was willful in that agents made deliberate and conscious efforts to avoid learning related facts or law.[135] Willfulness generally requires proof that a defendant acted with knowledge that its conduct was unlawful.[136] The government generally need not prove the defendant knew *which* laws were violated, but only that it knew the conduct was proscribed and continued the same course of action.[137] Though this higher bar relative to crimes requiring only knowing action may pose a challenge in marginal cases and require a fact-intensive inquiry into a firm's awareness of or indifference to illegality, company servers are not infrequently veritable caches of smoking-gun evidence in an age of ubiqui-

[132] Cf. Doyle, supra note 112, at 4 & n.21 (collecting cases).

[133] 821 F.2d at 857 (finding a jury could conclude the bank's failure to inquire about the reportability of suspect transactions "constituted flagrant indifference" sufficient to support a finding of willfulness).

[134] Cf. Global-Tech Appliances v. SEB S.A., 563 U.S. 754, 766–70 (2011) (discussing the rationale behind willful blindness in criminal law).

[135] See, e.g., Abril & Olazábal, supra note 127, at 118–21; see also Julie R. O'Sullivan, Federal White Collar Crime 119–20 (5th ed. 2012) (discussing willful blindness as part of specific intent and collecting cases).

[136] John Shepard Wiley, Jr., Not Guilty by Reason of Blamelessness: Culpability in Federal Criminal Interpretation, 85 Va. L. Rev. 1021, 1133–36 (1999) (discussing the construction of "willfully" in *Bryan v. United States*, 524 U.S. 184 (1998)).

[137] *Bryan*, 524 U.S. at 194–96.

tous electronic communication.[138] Further, even moderately sophisticated firms will presumably have in-house counsel or consultants to advise on legal and compliance risks, potentially undermining claims of benign ignorance. In the context of potential corporate prosecutions under IEEPA and the material support statutes, the potential viability of willful blindness and collective knowledge theories could be of significant assistance to prosecutors, particularly in cases where intermediaries are not subject to affirmative statutory mandates to know their customers and monitor user activity. One qualifier, however, is the fact that very few criminal prosecutions of large companies ever reach trial, as is discussed below. FedEx's decision to challenge the DOJ's accusations in court is very much an exception to the general rule that companies settle as a matter of practice.[139] As such, there may be relatively little or even no precedent to illuminate whether theories of organizational culpability fit the facts of a particular case.[140]

C. Challenges and Critiques

Given the small number of corporate prosecutions that go to trial[141] and the acceptance of broad theories of corporate criminal liability by the federal bench, it is unsurprising to find a relative dearth of recent judicial challenges to convictions in this realm.[142] There is, however, no corresponding dearth of criticism. Doctrinal objections read as particu-

[138] See, e.g., Greg Farrell, Deutsche Bank E-Mails Showed 'Tricks' That Led to U.S. Pact, Bloomberg (Nov. 4, 2015, 1:01 PM), http://bloom.bg/1MIaX4l [https://perma.cc/KB5P-GSD6] (reporting that a "string of e-mails showed employees discuss[ing] the 'tricks' used" to evade U.S. sanctions); Matt Levine, BNP Compliance Officers Were Fine With Some Non-Compliance, Bloomberg View (July 1, 2014, 11:07 AM), http://bv.ms/V7LeZY (discussing examples of internal emails and memoranda cited within DOJ charging documents in the 2014 BNP sanctions prosecution).

[139] Ross Todd, Feds Face Fight in Trials Against PG&E, FedEx, Recorder, May 2, 2016, at 1 (characterizing the fact that FedEx and utility Pacific Gas & Electric both faced mid-2016 federal criminal trials in the same district as "the white collar equivalent of a double rainbow").

[140] Cf. id. (quoting experts who assert cases such as those brought against FedEx and PG&E "take the legal fiction of corporate personhood to its extreme" and argue that this can cut both ways before a jury).

[141] Federal sentencing data indicates that over 90% of firms charged plead guilty, and a mere 8% contest charges at trial. Garrett, Too Big to Jail, supra note 111, at 162.

[142] The Arthur Andersen case is a notable exception. In a short and unanimous opinion, the Supreme Court reversed the firm's obstruction conviction. Arthur Andersen LLP v. United States, 544 U.S. 696, 698 (2005).

larly strident, with critics arguing that the imposition of criminal liability onto entities neither comports with principles of criminal law nor serves its aims.[143] Such concerns often center on the imputation of agent actions and intent to the firm, which cannot itself have a culpable mind.[144] Similarly, entity liability may enable prosecutors to secure settlements from corporations on the basis of evidence that would not suffice to sustain an individual conviction.[145] That entities have fewer or otherwise weaker constitutional rights than individuals is pointed to as a further irregularity.[146]

Critics also raise crosscutting fairness arguments against the criminal prosecution of businesses. Under one paradigm, the threat of an indictment is a tool of coercion used to get at corporate misbehavior more easily.[147] Even well-resourced firms are portrayed as exceedingly vulnerable, a depiction informed by the increasingly disputed, but persistent, conventional wisdom that an indictment would sound the death knell of many companies.[148] Critics also point to the collateral effects of prosecu-

[143] See, e.g., Khanna, supra note 111, at 1532 (arguing "the question has become whether corporate criminal liability serves any purpose now" given expanded civil enforcement).

[144] See, e.g., John Hasnas, The Centenary of a Mistake: One Hundred Years of Corporate Criminal Liability, 46 Am. Crim. L. Rev. 1329, 1330–33 (2009) ("No theory . . . can justify punishing an entity that is not capable of morally blameworthy behavior."); cf. Gregory M. Gilchrist, Condemnation Without Basis: An Expressive Failure of Corporate Prosecutions, 64 Hastings L.J. 1121, 1148–49 (2013) (arguing prosecutions of entities based on "[m]ere respondeat superior liability" may be characterized by a lack of "meaningful condemnation," and further arguing that "[a] legal system that blames the non-blameworthy will be deemed less legitimate").

[145] See, e.g., Garrett, Scapegoat, supra note 11, at 1831–37 (positing that prosecutors' ability to pursue corporations without effectively proving mens rea could be a reason why many corporate cases settle and why few prosecutions are brought against agents).

[146] Doyle, supra note 112, at 13–20; see also Garrett, Too Big to Jail, supra note 111, at 196–215 (discussing the constitutional rights of corporations).

[147] For a particularly harsh critique, see Hasnas, supra note 144, at 1340–41 (arguing "corporate criminal punishment is a form of collective punishment in which the innocent are intentionally targeted for punishment along with, *and sometimes in place of*, the guilty in order to discourage wrongdoing by individuals," and further arguing the *New York Central* standard does not advance legitimate purposes of criminal punishment (emphasis added)).

[148] Preet Bharara, Corporations Cry Uncle and Their Employees Cry Foul: Rethinking Prosecutorial Pressure on Corporate Defendants, 44 Am. Crim. L. Rev. 53, 73–76, 86–87 (2007) (describing companies as "eggshell defendants" and discussing the "mercilessness of the applicable legal doctrines"). Notably, the author of this article went on to serve as U.S. Attorney for the Southern District of New York, a role in which he brought high-profile cases against a number of corporate defendants. See Roger Parloff, USA v. SAC: A Simply Unanswerable Indictment, Fortune (July 26, 2013, 10:08 PM), http://for.tn/1ttBxkl

tion on innocent third parties such as shareholders and employees, although the effects of civil penalties are also borne by third parties.[149] The inverse view is that prosecutors should be *more* aggressive and pursue actual indictments against companies, rather than enter into deferred prosecution and nonprosecution agreements that are subject to less judicial scrutiny. Though the DOJ has exacted billions of dollars in penalties through such deals, there is a popular view that this does not adequately punish the often-egregious conduct detailed in accompanying factual statements, and may be dismissed as a cost of business.[150] Such critiques often reject or gloss over the indictment-as-death-penalty concept and minimize the collateral consequences of convictions.[151]

D. Targeting Bad Actors Through Detached Third-Party Intermediaries

Though the FedEx prosecution, discussed further below, reflected a novel theory and an aggressive approach by prosecutors, it fits into a longer narrative of the DOJ's strategic use of new law and new applications of existing law in various criminal "wars." The examples below are by no means exhaustive, but they are illustrative of past targeting of bad actors through detached third-party intermediaries. These and other examples form the basis for the theoretical application in the counterterrorism context discussed in Part III, which seeks to both disrupt FTO activities and incentivize intermediaries to provide much-needed assistance in the fight.

[https://perma.cc/Y58N-RSWA] (noting Bharara's authorship of the above law review article in the context of the indictment of hedge fund SAC Capital); see generally Jeffrey Toobin, The Showman: How U.S. Attorney Preet Bharara Struck Fear Into Wall Street and Albany, New Yorker (May 9, 2016), http://www.newyorker.com/magazine/2016/05/09/the-man-who-terrifies-wall-street (chronicling Bharara's career and tenure in the Southern District) [https://perma.cc/B3JJ-ESS3].

[149] Hasnas, supra note 144, at 1339–40.

[150] See, e.g., Peter J. Henning, In Bank Settlements, Fines but No Accountability, N.Y. Times: DealBook (Dec. 12, 2012, 8:22 AM), http://nyti.ms/1wVmaoc; Matt Taibbi, Gangster Bankers: Too Big to Jail, Rolling Stone (Feb. 14, 2013), http://rol.st/UiVY5a [https://perma.cc/HPM3-975H].

[151] See, e.g., Gabriel Markoff, Arthur Andersen and the Myth of the Corporate Death Penalty: Corporate Criminal Convictions in the Twenty-First Century, 15 U. Pa. J. Bus. L. 797, 827–30 (2013) (arguing there is no empirical support for the so-called "Andersen Effect" and suggesting reasons why corporate convictions appear less fatal than assumed by the conventional wisdom).

1. Sanctions and Tax Evasion

Among the most straightforward examples of this intermediary-focused approach are "sanctions-busting" cases. Here, though the ultimate targets are rogue regimes, terrorists, and associates designated by the executive branch, sanctions are largely enforced through IEEPA's penalty provisions (and the compliance they "inspire").[152] The DOJ has recently brought a raft of high-profile criminal IEEPA cases against European banks in efforts to "give teeth" to U.S. sanctions overseas, leveling billions of dollars in penalties against institutions that facilitated illegal U.S. dollar transactions.[153] Similarly, the federal tax-evasion crackdown that began in the late 2000s, though aimed at U.S. taxpayers hiding assets and income offshore, targeted the banks that catered to such clients. In various phases of this initiative, the DOJ entered into NPAs with dozens of overseas banks that were conditioned on their provision of account information and continued cooperation with record requests.[154] The pressure exerted by U.S. officials on overseas banks has in turn pushed thousands of tax scofflaws out of the shadows and has made classic secrecy havens increasingly inhospitable.[155]

2. Prostitution and Human Trafficking

Federal authorities have also recently stepped up efforts against online facilitators of prostitution and human trafficking. In late 2014, prosecutors in San Francisco hailed the "first federal conviction of a website operator for facilitation of prostitution."[156] The DOJ has brought

[152] See supra discussion in Subsections I.C.1–2.

[153] See, e.g., Ben Protess & Chad Bray, French Bank to Settle Inquiries in U.S., N.Y. Times, Oct. 21, 2015, at B5 (detailing the broader DOJ initiative).

[154] Swiss Bank Program, Dep't of Justice, https://www.justice.gov/tax/swiss-bank-program [https://perma.cc/P6YU-HDPR] (last visited Nov. 5, 2016) (detailing program and providing settlement-related documents).

[155] Caroline D. Ciraolo, Principal Deputy Assistant Attorney Gen., Dep't of Justice, Remarks at the Cambridge International Symposium on Economic Crime (Sept. 5, 2016), https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-caroline-d-ciraolo-delivers-remarks-cambridge [https://perma.cc/TJ2W-BVD9] ("Those who . . . use secret foreign financial accounts are running out of places to hide . . . .").

[156] Press Release, Dep't of Justice, California Operator of MyRedBook.com Website Pleads Guilty to Facilitating Prostitution (Dec. 11, 2014), https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/california-operator-of-myredbook.com-website-pleads-guilty-to-facilitating-prostitution [https://perma.cc/2PQN-R793].

similar cases in Pennsylvania and New York, also involving seizure of offending sites and charges against corporate entities.[157] It remains to be seen whether the DOJ will pursue criminal charges against general-purpose sites, that is, those not specifically tailored to the commercial sex trade but that also significantly facilitate such transactions. Classified-ad forum Craigslist eliminated its "adult services" section in 2010 amid pressure from authorities related to alleged facilitation of sex trafficking and related violence.[158] Ad-site Backpage took similar actions in early 2017, on the eve of Senate subcommittee hearings held in conjunction with the release of an investigative report alleging it knowingly facilitated sex trafficking of minors.[159] Members of Congress have further cited the DOJ's success in the San Francisco case in calls for a criminal investigation of the company.[160] For its part, Backpage raised a pre-enforcement challenge to a new federal antitrafficking statute that targets third-party advertisers. This action was dismissed by the district court in October 2016 on standing grounds, and potential federal prosecution of the company does not appear beyond the realm of possibility.[161]

Still more controversial is the issue of potential Internet service provider ("ISP") liability for criminal activity conducted through their networks. While immunity of ISPs and content hosts from *civil* liability is a generally settled matter under the Communications Decency Act of 1996 ("CDA"),[162] potential *criminal* liability remains an open question

[157] Nathan Gorenstein, 2 Firms With Prostitution Ties Fined, Phila. Inquirer, Mar. 20, 2012, at B2; Rebecca Davis O'Brien, Rentboy.com CEO, Business Indicted; Gay-Escort Service and its Leader Charged with Prostitution and Money-Laundering, Wall St. J. (Jan. 27, 2016, 8:47 PM), http://on.wsj.com/1Phqzqu.

[158] Claire Cain Miller, Some See a Ploy as Craigslist Blocks Sex Ads, N.Y. Times, Sept. 6, 2010, at B1 (detailing efforts of state attorneys-general against the company); Cecilia Kang, Adult Ads Permanently off U.S. Sites, Craigslist Says, Wash. Post, Sept. 16, 2010, at A22 (discussing pressure from law enforcement and advocacy groups).

[159] Janelle Nanos, Backpage Pilloried in Senate Hearing, Bos. Globe, Jan. 11, 2017, at C1.

[160] Sen. Dianne Feinstein, Letter to the Editor, Human Trafficking, N.Y. Times (Mar. 15, 2016), http://nyti.ms/1UwVyFy (repeating calls for DOJ investigation).

[161] Memorandum Opinion at 20–21, Backpage.com, LLC v. Lynch, No. 15-cv-02155-RBW (D.D.C. Oct. 24, 2016). Notably, three Backpage executives were arrested on state pimping-related charges in October 2016 in connection with the operation of the website. See, e.g., Camila Domonoske, CEO of Backpage.com Arrested, Charged with Pimping, NPR (Oct. 7, 2016, 11:17 AM), https://n.pr/2dxDWLM.

[162] Indeed, Backpage has routinely availed itself of the CDA's civil immunity provisions to have lawsuits brought against it dismissed. Further, the Supreme Court denied cert in Jan-

given CDA provisions that exclude from immunity enforcement of federal criminal statutes.[163] The 2001 state conviction of an ISP for providing access to child pornography sent shockwaves through the industry, but there have been no analogous federal prosecutions to date and this case remains an outlier.[164]

3. The War on Drugs—and More

Facilitator-focused efforts in the drug wars have similarly aimed to target traffickers' assets and tap into private-sector intelligence through intermediaries. The Bank Secrecy Act ("BSA") and related anti–money laundering/counter-terrorism finance statutes have imposed significant monitoring, reporting, and compliance requirements on financial institutions and other businesses.[165] Covered institutions are subject to criminal liability not only for substantive money laundering but also for inadequate BSA compliance programs and controls. Likely due in part to concerns over collateral regulatory consequences, most recent DOJ actions against financial intermediaries in this realm allege compliance failures, not substantive violations or direct facilitation of money laundering or terrorist financing.[166] BSA-related prosecutions have been brought against numerous institutions for violating reporting requirements and, since the late 1970s, for acting "in league with" bad actors; the continued expansion of its statutory reach and enforcement efforts has had a

uary 2017 in a case brought against Backpage by three victims of trafficking allegedly facilitated through the site. See Nanos, supra note 159.

[163] See 47 U.S.C. § 230(e)(1) (2012). For a helpful discussion of civil and criminal liability for user-generated content under the CDA, see Lawrence G. Walters, Shooting the Messenger: An Analysis of Theories of Criminal Liability Used Against Adult-Themed Online Service Providers, 23 Stan. L. & Pol'y Rev. 172 (2012).

[164] Walters, supra note 163, at 174–75, 208–11.

[165] History of Anti-Money Laundering Laws, Fin. Crimes Enf't Network, Dep't of the Treasury, https://www.fincen.gov/history-anti-money-laundering-laws [https://perma.cc/68E7-NWAW] (last visited Nov. 4, 2016).

[166] Garrett, Too Big to Jail, supra note 111, at 100–01 (discussing BSA "systems failures"); see also Betty Santangelo & Matthew P. Truax, Schulte Roth & Zabel LLP, Ten Years After 9/11: A Retrospective on How We Got Here (Feb. 29, 2012), http://www.sifma.org/uploadedfiles/events/2012/anti-money_laundering_and_financial_crimes_conference/sifma-feb292012-tenyearsafter%20911-a-retrospective-on-how-we-got-here-outline.pdf [https://perma.cc/HLH7-TB9B] (outlining notable BSA developments and cases).

marked impact on the financial-services industry.[167] Some have questioned whether authorities have been aggressive enough, pointing to settlements that have allowed banks to continue operating despite evidence of widespread dealings with unsavory actors and direct facilitation of criminal activity.[168] Nevertheless, the willingness of the DOJ and industry regulators to pursue presumably neutral intermediaries under the BSA has arguably had a socializing effect, manifested in greater focus on compliance and "de-risking."[169] The (incentivized) assistance of the financial sector provides authorities with valuable intelligence on drug traffickers, terrorist financiers, and other bad actors, and further assists in disrupting flows of illicit or ill-intentioned funds.[170]

BSA-based bank prosecutions can be distinguished from the drug cases against FedEx, UPS, and Google in that the latter firms had no analogous, affirmative statutory duties related to their dealings with online pharmacies; further, as common carriers, FedEx and UPS are actually *exempt* from core requirements of the CSA.[171] The accomplice

[167] See Santangelo & Truax, supra note 166; Joseph Adler, How Sept. 11 Transformed AML Efforts, Am. Banker, Sept. 12, 2011, at 2; see also Dick Thornburgh, U.S. Attorney Gen., Remarks on Money Laundering Before the City Club Forum Luncheon at 4 (May 11, 1990), https://www.justice.gov/sites/default/files/ag/legacy/2011/08/23/05-11-90.pdf [https://perma.cc/25F3-6VJ4] (stating "the most vulnerable point for any drug operation is . . . the doorway to the bank" and noting increased assistance from banks "coincident with a number of [bank] prosecutions during the mid-80s").

[168] See, e.g., Taibbi, supra note 150. Though a scathing Senate report tied HSBC to terrorist financing, the bank's 2012 DOJ settlement covered only country-based IEEPA violations and BSA control failures. Ben Protess & Jessica Silver-Greenberg, HSBC to Pay $1.92 Billion to Settle Charges of Money Laundering, N.Y. Times: DealBook, (Dec. 10, 2012, 4:10 PM), http://nyti.ms/1kz0LcB.

[169] Cf. Rachel Louise Ensign et al., U.S. Banks Cut Mexico Ties, Wall St. J., Jan. 25, 2016, at C1 (quoting James Dimon, J.P. Morgan Chase's CEO, as saying, "We do move $6 trillion a day and I am terrified if $100 goes to the wrong place").

[170] See generally Patrick T. O'Brien, Tracking Narco-Dollars: The Evolution of a Potent Weapon in the Drug War, 21 U. Miami Inter-Am. L. Rev. 637 (1990) (discussing the early history of U.S. anti–money laundering laws and their importance in the War on Drugs); History of Anti-Money Laundering Laws, supra note 165 (providing overview of the goals and evolution of U.S. money laundering laws); see also John A. Cassara, Hide & Seek: Intelligence, Law Enforcement, and the Stalled War on Terrorist Finance 63–64, 70 (2006) (noting the value of BSA-mandated reporting and financial-industry assistance to criminal investigators).

[171] 21 U.S.C. § 822(c)(2) (2014) (exempting common carriers from CSA registration requirements). The Google investigation centered on violations of the Food, Drug, and Cosmetic Act. See Peter J. Henning, Behind Google's $500 Million Settlement With U.S., N.Y. Times: DealBook (Aug. 30, 2011, 9:30 AM), http://nyti.ms/1UjoeTi.

theory pursued in all three cases is largely the same—that these firms were on notice of illegal activity by online pharmacies yet continued to service them, thus furthering the pharmacies' illegal activity.[172] While the Google and UPS NPAs precluded real testing of the DOJ's "gray collar" theory and charges against FedEx were ultimately dropped mid-trial, that there was a trial at all is still significant.[173] A win against FedEx could have emboldened the DOJ to pursue similarly aggressive theories elsewhere, but it is not yet clear that the forfeiture will substantially chill intermediary prosecutions, or conversely, that it will embolden more corporate defendants to opt for trial rather than settlement.

The lack of similar prosecutions of airlines in the height of the drug wars further suggests that the cases above may represent an increasingly aggressive strategy. Despite frequent discoveries of drugs cached aboard planes and arrests of dozens of employees, authorities stopped short of charging any airline criminally even where illegal activity was pervasive and involved airline personnel, instead levying civil fines and seizing airliners under forfeiture provisions.[174] The novelty of the DOJ's theory against FedEx did not go unnoticed by the judge presiding over the case, who twice denied motions to dismiss[175] but also twice ordered prosecutors to identify cases previously brought against shippers on similar facts.[176] The court's probing interest in the prosecutors' theory and the ultimate turn of events underscore the need for rigorous ex ante evalua-

[172] Mary Schlangenstein & Karen Gullo, FedEx Fights U.S. in Online-Pharmacy Probe After UPS Deal, Bloomberg (June 13, 2013, 5:12 PM), http://www.bloomberg.com/news/articles/2013-06-13/fedex-fights-u-s-in-online-pharmacy-probe-after-ups-deal [https://perma.cc/FP4M-ZTKL].

[173] Though noting the lack of precedent for such a prosecution, the district court rejected FedEx's broad reading of the common-carrier exemption and denied motions to dismiss the case. Laura Stevens, FedEx Loses Motion to Dismiss DOJ Drug-Shipping Charges, Wall St. J. (May 14, 2015, 7:34 PM), http://on.wsj.com/1PjkXpO.

[174] See, e.g., Peter Kerr, Employees of 3 Airlines Charged in Cocaine Smuggling at Kennedy, N.Y. Times (Mar. 11, 1987), http://nyti.ms/1Ug0saB; Bob Wiedrich, Airlines Taking the Rap for Drug Smugglers, Chi. Trib., July 25, 1988, at D1.

[175] Order Denying Motion to Dismiss the Indictment Based on Grand Jury Instructions, United States v. FedEx Corp., No. 14-CR-00380 (N.D. Cal. Apr. 18, 2016); Transcript of Proceedings at 21, United States v. FedEx Corp., No. 14-CR-00380 (N.D. Cal. May 14, 2015) (denying FedEx's first motion to dismiss).

[176] Order Directing the Government to File a Submission Regarding Similar Prosecutions, United States v. FedEx Corp., No. 14-CR-00380 (N.D. Cal. Apr. 21, 2016); United States' Submission in Response to Court's Request, United States v. FedEx Corp., No. 14-CR-00380 (N.D. Cal. Sept. 30, 2015).

tion of novel applications against corporate intermediaries, particularly firms that have made substantive efforts to assist law enforcement.[177]

III. TARGETING LINKS IN THE TERRORIST SUPPLY CHAIN

Similar to challenges faced in other federal anticrime campaigns, there is a need to take an all-tools approach to counterterrorism. IEEPA and the material support statutes have had a significant impact, but both could be put to even greater use through application in the corporate context. The volume of information possessed by firms and the criticality of their products and services to terrorists makes their assistance crucial, in both denying access to resources and providing intelligence. The goal here is not to create a de facto strict liability regime, but to incentivize firms to provide proactive assistance and thorough cooperation to government. Such an approach would be consistent with DOJ efforts in other contexts, and while actual charges may remain rare, a credible threat of criminal liability could go a long way in pushing companies to better monitor distribution channels and avoid being co-opted into the terrorist supply chain.

The aim of this Part is not to provide a blueprint for prosecution, but to realistically evaluate the potential for applying these statutes against corporate actors.[178] Application in the contexts discussed below raises tough and often unresolved follow-on questions, including about the limits of free speech and the currently raging "Going Dark" debate[179] on encryption and government access to private information. This Part addresses considerations specific to the corporate categories examined, while Part IV discusses overarching concerns and safeguards. Refer-

[177] See, e.g., Ross Todd, Behind the Scenes of the Surprise FedEx Dismissal, Law.com (June 20, 2016), http://at.law.com/iDbpEa (discussing evidence that FedEx consistently cooperated with the DEA); infra notes 265–268 and accompanying text. The lack of criminal prosecutions of airlines in the 1980s and 1990s is also likely attributable in part to airlines' efforts to step up detection efforts and assist law enforcement in investigating drug rings. Cf. Wiedrich, supra note 174 (discussing "intensive pressure" placed on airlines by U.S. law enforcement); Christopher S. Wren, Big Cocaine Cache Is Found Stashed in Airliner Cockpit, N.Y. Times, Mar. 23, 1996, at 6 (discussing a U.S. Customs Service "super-carrier initiative[]" that was designed to increase industry cooperation with antidrug efforts).

[178] For purposes of this Part, § 2339B is the focus of the material support discussion given its less-demanding mens rea and the lower probability of a fact pattern in which a mainstream company *actively* seeks to further specific terrorist acts. IEEPA discussion is limited herein to the E.O. 13224 context.

[179] See infra notes 208–216 and accompanying text.

ences to specific companies are included purely for illustrative purposes, and not to suggest that these companies should necessarily face prosecution on present facts.

A. Social Media and Public Content Hosting

Much as the Internet and social networking have been game-changers writ large, they also provide FTOs with new means to recruit, fundraise, transact business, and distribute propaganda, enabling the groups' expansion and amplifying their presence on the world stage.[180] Franchise-like groups have capitalized on these tools,[181] and the world saw the first live-tweeted terrorist attack in 2013 as al-Shabaab militants provided real-time commentary via Twitter.[182] Formerly exclusive al Qaeda affiliates have come to embrace open online engagement,[183] and consumption of the online musings of since-deceased cleric Anwar al-Awlaki has appeared as a common denominator in a large number of "lone wolf" cases.[184] ISIS has been especially prolific on social media, using it to post execution videos, claim responsibility for attacks, and recruit followers.[185] Long gone are the days in which Osama bin Laden relied upon mainstream media outlets and satellite broadcasters to air statements videotaped in the mountains of Afghanistan; we are presently living in The Age of Selfie Jihad, in which anyone with a smartphone

[180] See, e.g., U.N. Office on Drugs & Crime, The Use of the Internet for Terrorist Purposes, ¶¶ 1–25 (Sept. 2012), http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [https://perma.cc/53G4-N6ZV] (discussing means for which terrorists have used the Internet, including propaganda, radicalization, fundraising, and in operational planning); C.J. Chivers, Facebook Groups Act as Weapons Bazaars for Militias, N.Y. Times (Apr. 6, 2016), http://nyti.ms/25LN9Dj.

[181] Retweets to Raqqa, supra note 21, at 15–26; Scott Shane, Matt Apuzzo & Eric Schmitt, Americans Attracted to ISIS Find an 'Echo Chamber' on Social Media, N.Y. Times (Dec. 8, 2015), http://nyti.ms/1XUCkh3.

[182] Scott Higham & Ellen Nakashima, Why the Islamic State Leaves Tech Companies Torn Between Free Speech and Security, Wash. Post (July 16, 2015), http://wpo.st/k_DV1 [https://perma.cc/2APM-CUT3].

[183] Id.

[184] Scott Shane, Objective Troy: A Terrorist, a President, and the Rise of the Drone 176–80, 190 (1st paperback ed. 2016).

[185] Higham & Nakashima, supra note 182.

can live-stream acts committed at the direction of—or even merely inspired by—their FTO of choice.[186]

Online platforms are significant force multipliers, enabling decentralized FTOs to crowdsource terrorism[187] and retain greater narrative control through de facto state media.[188] The upside is that these groups are heavily reliant upon third-party hosts and networks such as Twitter and Facebook, given inadequate in-house capabilities and the appeal of platforms that already boast large, geographically dispersed user bases.[189] At the outset, it is important to distinguish unaffiliated, detached intermediaries from those controlled by or operated primarily for the benefit of FTOs or SDGTs. The latter group provides an easy case for criminal liability, while application to the former raises far tougher questions.

Conviction for providing material support to an FTO under § 2339B requires that a defendant (1) knowingly provided, or attempted or conspired to provide, material support or resources to an FTO; and (2) did so with knowledge of the recipient's FTO designation or engagement in terrorist activity.[190] A literal reading suggests third-party platforms could plausibly be prosecuted under this provision, given the broad and nonexclusive categories of support that appear in the text.[191] There are col-

[186] See Jason Burke, The Age of Selfie Jihad: How Evolving Media Technology Is Changing Terrorism, CTC Sentinel, Nov./Dec. 2016, at 16, 16–20 (detailing the impact of the digital and mobile revolutions on terrorism).

[187] Id.; see also Scott Shane, A Homemade Style of Terror: Jihadists Push New Tactics, N.Y. Times (May 5, 2013), http://nyti.ms/1zZf2FJ (discussing use of online resources posted by FTOs).

[188] See, e.g., Rukmini Callimachi, A News Agency with Scoops Directly from ISIS, and a Veneer of Objectivity, N.Y. Times (Jan. 14, 2016), http://nyti.ms/1TYSDmZ.

[189] Twitter and Facebook claimed 313 million and 1.86 billion active monthly users, respectively, in figures available as of March 2017. Company, Twitter, https://about.twitter.com/company [https://perma.cc/7LCN-TRHJ] (last visited Mar. 17, 2017); Company Info, Facebook, http://newsroom.fb.com/company-info [https://perma.cc/C5HJ-X42K] (last visited Mar. 17, 2017).

[190] 18 U.S.C. § 2339B(a)(1) (2012).

[191] Others have reached similar conclusions as to the facial plausibility of such a scenario. See, e.g., Emily Goldberg Knox, Note, The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists, 66 Hastings L.J. 295, 318 (2014) (discussing uncertainty as to the degree of coordination required by the Court's decision in *Humanitarian Law Project* and conceding "it is plausible that social media companies are providing a service prohibited by the material support statute"); Benjamin Wittes & Zoe Bedell, Tweeting Terrorists, Part II: Does it Violate the Law to Let Terrorist Groups Have Accounts?, Lawfare (Feb. 14, 2016, 6:35 PM), https://www.lawfareblog.com/tweeting-terrorists-part-ii-does-it-violate-law-twitter-let-terrorist-groups-have-accounts [https://perma.cc/CM3L-WMTG] (finding

orable arguments that such companies provide at least *use* of "communications equipment" in the form of platform access, or even "expert assistance." Further, they certainly provide "services" under the common meaning of the term, as Terms of Service agreements commonly posted online by these companies or incorporated into the account-creation process would seem to concede.

As to knowledge, many of the larger firms in the industry have *actual* knowledge of terrorists' use of their platforms given the openness with which many FTOs use social media.[192] Those that deliberately avoid acquiring direct knowledge (for example, by continuing not to obtain users' actual identities, failing to monitor content, or disabling third-party content flagging) could be argued to be on notice based on the extent of media coverage devoted of late to terrorists' online savvy, and potentially subject to liability under a willful blindness theory. While questions have been raised as to the degree of coordination with FTOs required to support § 2339B charges in the social media context following *Holder v. Humanitarian Law Project*,[193] the Court's opinion in that case was limited to *advocacy* as a service, not provision of access to an online platform or services more generally.[194] Internet intermediary liability for providing material support to FTOs is currently being tested in the civil context in a raft of cases filed by family members of terror victims. None of these cases had reached the merits stage as of early 2017, and both Section 230 of the CDA and challenges in establishing causation under civil-suit provisions of the Anti-Terrorism Act ("ATA") appear likely to be formidable obstacles for plaintiffs.[195] Regardless of whether

"Twitter is facing a daunting landscape . . . on a number of fronts" in light of statutory language, the Court's holding in *Humanitarian Law Project*, and its apparent provision of services to actual FTOs).

[192] See, e.g., Natalie Andrews & Deepa Seetharaman, Facebook Moves to Find, Block Terrorist Content, Wall St. J., Feb. 12, 2016, at B1 (also discussing similar efforts by Twitter); Wittes & Bedell, supra note 191.

[193] See, e.g., Knox, supra note 191, at 313–18.

[194] 561 U.S. 1, 26, 39 (2010) (distinguishing speech and advocacy from "services" generally).

[195] For overview and analysis of the legal issues posed by civil material support suits filed against social media and Internet companies, see Alison Frankel, Can Islamic State Victim's Widow Win Suit Against Twitter?, Reuters: On the Case (Jan. 14, 2016), http://reut.rs/1JN9aKm [https://perma.cc/JN2T-BLR7]; Benjamin Wittes, Another Day, Another Material Support Suit Against a Social Media Company, Lawfare (Jan. 10, 2017, 4:55 PM), https://www.lawfareblog.com/another-day-another-material-support-suit-against-social-

plaintiffs are able to recover damages or even merely survive motions for dismissal or summary judgment, the theories advanced in civil cases filed against Twitter, Facebook, and others could potentially be a preview of things to come on the criminal side, given the ATA's incorporation of a civil liability standard similar to that of § 2339B.[196] Though the knowledge requirement of § 2339B and potential applicability of willful blindness seem to set a low bar on criminal liability, particularly where FTO use of a platform is open and notorious, broader policy concerns noted below may cut against expansive application.

Though IEEPA's civil provisions operate on a strict-liability basis, criminal conviction requires that a defendant (1) commits, attempts or conspires to commit, or aids or abets in the violation of a license, order, or regulation issued under IEEPA; and (2) does so willfully.[197] In the context of E.O. 13224, "violations" include making "any contribution of funds, goods, or *services to* or *for the benefit of*" an SDGT without OFAC authorization.[198] In most circuits, the DOJ would need to prove only that a company acted with knowledge that its conduct was unlawful in providing services to SDGTs; it would not generally be required to prove the company was aware of specific provisions that made its conduct illegal.[199] While maintaining social media accounts or hosting content would plainly appear to fall under E.O. 13224's prohibition on providing "services" to SDGTs, it could be more difficult to establish that such a firm acted with knowledge of unlawfulness in serving discrete parties (as opposed to users from countries subject to broad sanc-

media-company [https://perma.cc/B6RL-SDL4]; see also Walters, supra note 163, at 175–77 (discussing CDA Section 230 and open questions as to potential liability of online service providers for user-generated content).

[196] See Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852 (codified as 18 U.S.C. § 2333(d)(2) (2016)) (providing for liability against "any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed . . . an act of international terrorism"). Enacted in 2016, the Justice Against Sponsors of Terrorism Act ("JASTA") amended the Anti-Terrorism Act ("ATA") in aspects largely not relevant to the focus of this Note. Id.

[197] 50 U.S.C. § 1705(c) (2012).

[198] Exec. Order No. 13,224, 31 C.F.R. § 595 (2001) (emphasis added).

[199] See, e.g., United States v. Mousavi, 604 F.3d 1084, 1092–94 (9th Cir. 2010) (discussing willfulness under IEEPA and collecting cases); Mary Carter Andrues et al., Update on Intent Standard for Criminal Export Violations, Law360 (Feb. 28, 2014, 1:39 PM), http://www.law360.com/aerospace/articles/514358 [https://perma.cc/BT82-TTY6] (same).

tions), particularly where many platforms do not obtain or verify users' actual names.

Reports that some tech companies screen for SDGTs suggests they see IEEPA liability (civil or criminal) as a real risk.[200] Willful blindness, if premised on the idea that failing to obtain and screen users' actual names is conscious avoidance of knowledge of IEEPA violations, could potentially be applied against a large swath of the industry; however, this may not support a finding of willfulness without more evidence of a company's disregard for the law and awareness of *some* relevant facts, such as the popularity of a particular platform with FTOs. Reports suggest there has been a lack of IEEPA enforcement against Internet companies to date due to insufficient resources, free-speech concerns, and the potential impact on OSINT collection.[201] Strict-liability civil enforcement could serve as a warning shot to the industry; criminal charges could be reserved for egregious cases where firms fail to act despite clear indicia of terrorist usage.

Under either the material support or the IEEPA rubric, application of criminal liability to mainstream, third-party Internet intermediaries may be inadvisable other than in extreme cases. While imposing criminal liability here would place other firms on notice and likely spur greater efforts to make the Internet less hospitable for extremists, this approach raises thorny issues. First, prosecuting or conditioning nonprosecution on heeding content-takedown requests raises First Amendment concerns.[202] Indeed, a primary argument raised by Backpage against an antitrafficking statute that targets advertisers is that it creates a regime under which hosts are forced to heed government and third-party flagging of suspect content or otherwise face criminal liability, in turn chilling

[200] Rachel Pick, Why Is Epic Games Checking Names Against a Watchlist When It Doesn't Have To?, Motherboard (Jan. 12, 2016, 11:21 AM), http://motherboard.vice.com/read/why-is-epic-games-checking-names-against-a-watchlist-when-it-doesnt-have-to [https://perma.cc/2GY6-3SCZ] (reporting blocking of a gamer's account due to a (false) name match).

[201] Christopher S. Stewart & Rob Barry, Blacklisted Terrorism Financiers Still Active on Social Media, Wall St. J. (Apr. 25, 2016, 12:01 AM), http://on.wsj.com/1ShaTot.

[202] See, e.g., Seth F. Kreimer, Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link, 155 U. Pa. L. Rev. 11, 91–94 (2006) (identifying Internet intermediaries as "obvious targets" for government conscription); Knox, supra note 191, at 325 (warning of potential chilling of speech).

online speech.[203] While *Humanitarian Law Project* arguably only imposes a clear coordination requirement on pro-FTO *advocacy*, and not on the provision of platform access or services generally, there is sufficient uncertainty as to the implication of speech to perhaps counsel caution pending further guidance from the Court. Reserving prosecution for extreme cases, such as that of a platform that hosts virtual arms bazaars[204] or facilitates activity beyond the spread of propaganda, may mitigate speech-related concerns.

There are also practical reasons to tread lightly. Many intermediaries have begun to take on the Sisyphean task of blocking and removing terrorist content, an endeavor resembling an endless game of online Whac-a-Mole.[205] These good-faith efforts may cut against allegations of knowing or willful dealings,[206] and prosecution of firms making substantial, if imperfect, efforts to block terrorist content would seemingly create near–strict liability. Lastly, coercing hosts to take down material or block access in high-risk locations to avoid criminal liability has the potential to dry up valuable information on FTO operations.[207] All of this is not to say charges should *never* be pursued against platforms used by terrorists, but rather that potential fallout should be weighed carefully ex ante. Many such companies are already undertaking significant efforts to police content and assist authorities. But where firms have adopted a hands-off approach despite knowledge of terrorists' presence (or of a high probability of such) in their user base, effectively allowing their platforms to be co-opted, use of the material support statutes and IEEPA should not be taken off of the table. Potentially critical reception of such a prosecution should not create carte blanche for hosts to do nothing.

[203] Complaint for Declaratory and Injunctive Relief at 3, Backpage.com, LLC v. Lynch, (D.D.C. Dec. 11, 2015) (No. 15-cv-02155-RBW), 2016 WL 6208368 ("[C]riminal liability cannot constitutionally be imposed on a website merely for providing a forum for speech that some . . . misuse . . . .").

[204] Chivers, supra note 180. This is not to say Facebook should be charged here, but rather that the option should remain open where a firm has knowledge of such use of its platform and fails or refuses to act.

[205] Christopher S. Stewart & Mark Maremont, Twitter and Islamic State Deadlock on Social Media Battlefield, Wall St. J. (Apr. 13, 2016, 10:17 AM), http://on.wsj.com/1qR9ZcX.

[206] J.M. Berger, Can Twitter Materially Support ISIS While Actively Working to Defeat It?, Lawfare (Feb. 19, 2016, 3:35 PM), https://www.lawfareblog.com/can-twitter-materially-support-isis-while-actively-working-defeat-it [https://perma.cc/CX3B-WE5W].

[207] Moshirnia, supra note 76, at 433–34.

B. Encrypted Communications Platforms

Terrorists have also capitalized on the increasing ubiquity of encrypted communications platforms to facilitate remote recruitment and operational planning.[208] Though terrorist use of encryption is not a new phenomenon,[209] the recent proliferation of platforms and devices geared to the consumer market has been a windfall. Reports increasingly point to FTOs' use of encrypted communications and storage to evade government surveillance ex ante and stymie investigations ex post.[210] Whereas use of unsecure phone lines or messaging may expose the activities of would-be attackers in time to prevent attacks, widely available encrypted platforms such as WhatsApp, Surespot, and Telegram, among many others, often drastically reduce what can be gleaned from intercepted communications.[211] Many firms have begun to aggressively roll out end-to-end ("E2E") encryption as a feature of their products, which in a nutshell prevents anyone other than the parties to a message to view its content, including law enforcement and even the provider itself.[212]

Without technical assistance from platform owners, who have increasingly designed products in ways that reduce their own access to user content, encrypted messaging is a growing blind spot and has been

[208] See, e.g., Rotella, supra note 33 (discussing ISIS's use of encrypted apps).

[209] 9/11 Commission Report, supra note 13, at 88 (noting in 2004 the accessibility of "global, instantaneous, complex, and encrypted" communications to terrorists); Neal Kumar Katyal, Criminal Law in Cyberspace, 149 U. Pa. L. Rev. 1003, 1048–49 (2001) (discussing terrorist use of encryption in the 1990s).

[210] See, e.g., Margaret Coker et al., How Islamic State Teaches Tech Savvy to Evade Detection, Wall St. J. (Nov. 16, 2015, 9:41 PM), http://on.wsj.com/1OcycRr.

[211] Id. (quoting current and former intelligence officials); Rotella, supra note 33 (same). The above-listed apps represent a small sample of those known to be used by ISIS devotees; further, analysts have noted there appears to be little consensus among members and followers of the group as to which are the most (and least) effective from a security standpoint. See, e.g., Rita Katz, Almost Any Messaging App Will Do—If You're ISIS, Motherboard (July 14, 2016, 1:00 PM), https://motherboard.vice.com/en_us/article/isis-messaging-apps [https://perma.cc/Y3ZU-XZDQ] ("Despite the group's strict enforcement of uniform activity on social media, there is a starkly contrasting lack of consistency in its choices regarding [messaging] apps. . . . [W]hen it comes to IS[IS] attackers and coordinators' use of encrypted messaging programs, things suddenly get chaotic.").

[212] Cade Metz, Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People, Wired (Apr. 5, 2016, 11:00 AM), http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people [https://perma.cc/H6DQ-7K9Z] (briefly explaining E2E encryption).

described by officials as a "huge feature of terrorist tradecraft."[213] Further, the current iteration of the Going Dark debate between those that favor mandating provision of exceptional access or technical assistance to authorities and those favoring strong encryption can be described as polarized at best, with sparse middle ground.[214] Law enforcement is often able to at least obtain metadata such as IP addresses, cellphone numbers, and email addresses linked with messaging accounts used by known or suspected terrorists.[215] While this data is also an important source of investigative leads, the quest for message *content* is increasingly hitting a dead end, depriving authorities of often-critical information.[216]

As explained in Section III.A, criminal liability under § 2339B requires proving the defendant knowingly provided resources to an FTO.[217] It appears material support charges could be brought against providers of messaging platforms, under both literal and less-conventional applications of the statutes. Literal applications of the statutory text, which would entail arguing that these companies provide "services" or *use* of "communications equipment" to FTOs, appear not to be hard sells, similar to in the social media context. Somewhat less literally, these platforms and apps could be conceived of as a form of

[213] Kate O'Keeffe, American ISIS Recruits Down, but Encryption Is Helping Terrorists' Online Efforts, Says FBI Director, Wall St. J. (May 11, 2016, 8:54 PM), http://on.wsj.com/1seWAMI.

[214] Compare The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Comm. on the Judiciary, 114th Cong., at 12 (2016) [hereinafter Encryption Tightrope] (prepared statement of James B. Comey, Director, FBI) ("[T]he Going Dark problem is . . . one of technological choices and capability.") with Berkman Ctr. for Internet & Soc'y, Harvard Univ., Don't Panic: Making Progress on the "Going Dark" Debate 2 (2016) ("[W]e question whether the 'going dark' metaphor accurately describes the state of affairs.").

[215] Encryption Tightrope, supra note 214, at 50.

[216] Id. at 134–39 (prepared statement of Cyrus R. Vance, District Attorney, New York County) (discussing the impact of smartphone encryption on law enforcement investigations). While the first salvo in the Apple-DOJ litigation of early 2016 involved encrypted data "at rest" on a device, the issue of data "in motion" is also salient to the broader debate. Id. at 2 ("Encryption in securing data in motion, and in storage, is a valuable technological tool . . . [n]evertheless . . . a national debate has arisen concerning the positive and negative implications for public safety and national security."). For a high-level overview of the "Renewed Crypto Wars" and what information law enforcement is (and is not) regularly able to obtain, see Kristin Finklea, Cong. Research Serv., R44481, Encryption and the "Going Dark" Debate 5–10 (2016).

[217] See supra note 190 and accompanying text.

"expert assistance," or even virtual "safehouses." Again, this presupposes a firm has knowledge that its services are being used by FTOs. While the founder of the app Telegram acknowledged the encrypted platform was being used by ISIS and has at times maintained that the firm would take no action to combat terrorist usage or assist governments,[218] proving corporate knowledge and intent will likely be more difficult in the typical case, particularly with more companies taking a see-no-evil approach to system design that puts message content out of their reach. Combined with this E2E-created content blackout, the fact that many apps do not collect or verify user information leaves firms blissfully in the dark as to who their users are.[219] Facing this reality, prosecutors pursuing such firms could be reliant upon theories of willful blindness to meet § 2339B's knowledge requirement. However, this would in turn raise a quandary as to whether blindness as a *byproduct* of system or platform design would support such a theory unless design choices were spurred specifically by belief of usage by terrorists or bad actors generally.[220]

Applying a willful blindness–type theory where firms refuse to or otherwise do not maintain the capability to decrypt content seems to require taking a probabilistic approach we may not generally embrace—essentially, that the notoriety of terrorist use of encrypted messaging is such that terrorist use of *any* platform can be assumed. From this assumption, implementation of E2E encryption or other measures precluding access to content is the act of avoidance. Restricting the threat of charges to firms that are unwilling or have deliberately rendered themselves unable to assist in decrypting content and that continue to provide services to suspect users when given some form of government notice may be more palatable.[221] While this approach would still be aggressive,

[218] Natasha Lomas, Telegram Now Seeing 12BN Daily Messages, Up from 1BN in February, TechCrunch (Sept. 21, 2015), http://tcrn.ch/1FbElwS (detailing founder Pavel Durov's public comments on ISIS usage of Telegram).

[219] See, e.g., How Anonymous Am I on Wickr?, Wickr, https://wickr.desk.com/customer/en/portal/articles/2342383-how-anonymous-am-i-on-wickr- [https://perma.cc/72PB-FR6Q] (last visited Jan. 14, 2017) ("[E]ven we cannot determine the actual [user and device] information. . . ."); Law Enforcement Guidelines, Surespot, https://www.surespot.me/documents/surespotLawEnforcementGuidlines.pdf [https://perma.cc/4M9X-89P5] (last visited Jan. 14, 2017) (stating that the firm collects no personal information and has "no ability to view, decipher or see plain text" of messages).

[220] See supra notes 134–135 and accompanying text.

[221] There do not appear to be any reported material support cases related to the provision of encrypted platforms or devices in arm's-length transactions. Encryption-related prosecu-

the investigative challenges posed by increasingly pervasive encryption are likely only to deepen in the absence of a legislative solution mandating companies to provide technical assistance, and keeping the option of prosecution open could serve to incentivize greater cooperation.

Similar to points raised in Section III.A, criminal prosecution of mainstream messaging providers under IEEPA, where establishing that a corporate defendant acted with knowledge of the unlawfulness of its conduct would be required, could be challenging.[222] It is difficult to argue that even ardent supporters of strong encryption are *willfully* providing services to terrorists based on probability alone.[223] Partial or nonexistent verification procedures also give these firms plausible deniability in that they often collect little to no personal information on their users.[224] Somewhat ironically, potential civil or criminal liability under IEEPA for failure to *effectively* screen against OFAC lists may serve as an incentive against obtaining and verifying users' true identities in the first place where not explicitly required by statute, as it is in the financial services industry. However, indicia of awareness of IEEPA's broad requirements (namely, to not do business with terrorists) and a firm's efforts to avoid acquiring knowledge about its user base or failure to act on credible information that its services are being exploited by SDGTs could be used to make such a case.[225] Given the high-profile nature of recent country-based sanctions-busting prosecutions and the steady stream of media coverage detailing terrorists' use of specific messaging platforms, sophisticated firms may be hard-pressed to show true ignorance.[226]

tions have been limited to date, involving provision of equipment or advice to FTOs by direct supporters. See, e.g., Antonio Antenucci & Rich Calder, Al Qaeda "Tech-Geek" Gets 15 Years for Plotting Attack on NYSE, N.Y. Post (Jan. 20, 2015, 2:09 PM), http://nyp.st/1yGTyk9 [https://perma.cc/H8NZ-9EY2]; Nora Ellingsen, Not Quite Making It to Syria: A Tale of Two Failed ISIS Recruits, Lawfare (May 26, 2016, 7:28 AM), https://www.lawfareblog.com/not-quite-making-it-syria-tale-two-failed-isis-recruits [https://perma.cc/YY5L-7UYW].

[222] See supra notes 197–199 and accompanying text.

[223] There are exceptions to every rule; however, these appear more likely to come in the form of apps or providers controlled by FTO supporters, not unaffiliated firms such as WhatsApp or even Telegram.

[224] See supra note 219 and accompanying text.

[225] See supra Section III.A.

[226] See, e.g., Coker et al., supra note 210 (discussing ISIS use of encrypted apps); Rotella, supra note 33 (same).

While prosecution appears facially plausible in this context, evaluating its advisability requires taking stock of the broader Going Dark debate and an appreciation of potential fallout. Though a full treatment of Going Dark is beyond the scope of this Note, threatening prosecution for refusing or failing to maintain capacity to decrypt content would raise a number of far-from-settled legal issues, several of which were previewed in the ultimately abandoned DOJ/Apple litigation of early 2016. Apple's argument that forcing it to decrypt a terrorist's iPhone would have amounted to compelled speech[227] could resurface in the context of criminal prosecution. Forced decryption could also raise potential due process concerns; Apple argued that any such order would effectively conscript it as a state agent and arbitrarily deprive it of the liberty to design products as it sees fit.[228] Further, online anonymity and access to encryption are increasingly framed as human rights and as necessary protections against antidemocratic and authoritarian regimes, and nearly any government action that implicates encryption—even pursuant to judicial order—is, at present, viewed with suspicion.[229] Concerns with undermining security by mandating decryption and exceptional access capabilities also merit serious consideration, particularly given valid concerns with respect to hacking, though it is debatable that the choice between government access and data security is strictly binary.[230] Succinctly, it's complicated.

Any criminal prosecution here (or the threat thereof) would also likely be met with the refrain that unlike traditional telecom carriers, companies such as WhatsApp, Signal, and their peers currently have no statutory duty to decrypt content or maintain interception capabilities.[231] Such arguments are unlikely to carry the day in terms of criminal liability; the lack of an affirmative duty or the existence of a common carrier–type

[227] Steve Lohr, Analyzing Apple's Argument that First Amendment Applies to Its Code, N.Y. Times (Feb. 25, 2016), http://nyti.ms/20YffGr.

[228] Camila Domonoske & Alina Selyukh, Why Apple Says It Won't Help Unlock that iPhone, *in* 5 Key Quotes, NPR: The Two-Way (Feb. 25, 2016, 6:07 PM), http://n.pr/1oDkpez.

[229] UN Human Rights Chief Backs Apple in FBI Encryption Row, BBC (Mar. 4, 2016), http://www.bbc.com/news/technology-35725859 [https://perma.cc/929R-SZ2M].

[230] Matt Tait, An Approach to James Comey's Technical Challenge, Lawfare (Apr. 27, 2016, 7:00 AM), https://www.lawfareblog.com/approach-james-comeys-technical-challenge [https://perma.cc/X46F-AP46].

[231] Finklea, supra note 216, at 2–3 (discussing significant gaps in the Communications Assistance for Law Enforcement Act ("CALEA"), including explicit exceptions for information services).

immunity from liability for the crimes of users would not grant messaging providers themselves license to aid or do business with terrorists.[232] However, reactions to even *suggestions* that providers should be obligated to decrypt content or provide technical assistance have largely been reflexive and harsh.[233] In this climate, charging a provider that is not objectively co-opted by terrorists could be seen as the nuclear option.[234] While not a sufficient justification for inaction, the interplay with Going Dark and the risk that providers will shut down rather than cooperate with the government, as email provider Lavabit chose to in 2013 after authorities investigating leaks of classified information by former NSA contractor Edward Snowden sought the service's encryption keys, merits caution given potential collateral effects.[235] Finally, the lasting operational impact of prosecuting any one provider may be limited or even negative. Encrypted apps have proliferated, and where one is shut down or deemed unsafe by terrorists, hundreds more stand ready to fill the gap, often offshore where acquisition of even metadata could be more difficult.[236]

[232] Cf. Gabe Rottman, Hamas, Twitter and the First Amendment, ACLU (Nov. 21, 2012, 3:25 PM), https://www.aclu.org/blog/hamas-twitter-and-first-amendment [https://perma.cc/2KPE-CWQT] (noting common carrier liability would not extend to crimes committed by the carrier itself, in the context of a hypothetical material support prosecution of Twitter).

[233] See, e.g., Jean-Louis Gassée, The Dumb, Delusional US Senate Encryption Bill Is Everything Wrong with Tech Politics, Quartz (Apr. 19, 2016), http://qz.com/664104 [https://perma.cc/WY2R-29YE] (describing draft legislation that would require companies to decrypt user communications upon receipt of a court order as an "unrealistic, ignorant, and poorly thought-through piece of legislative saber rattling").

[234] Cf. Benjamin Wittes & Zoe Bedell, In Defense of Our "Braindead Jihad Against Encryption," Lawfare (July 30, 2015, 6:57 PM), https://www.lawfareblog.com/defense-our-braindead-jihad-against-encryption [https://perma.cc/RU84-GEJA] (responding to criticism of an earlier article that evaluated Apple's potential civil liability for providing encrypted messaging services).

[235] Lavabit shut down after being held in contempt for failing to comply with a pen-register order related to the Snowden investigation. Prosecutors also attempted to obtain encryption keys through a subpoena and finally a search warrant. See Kim Zetter, Long Before the Apple-FBI Battle, Lavabit Sounded a Warning, Wired (Mar. 18, 2016, 2:18 PM), http://www.wired.com/2016/03/lavabit-apple-fbi [https://perma.cc/4J43-JDE5]. The shutdown affected only 410,000 users, but a similar decision by another firm could have a much more significant impact, perhaps by design. Id.

[236] See generally Bruce Schneier et al., A Worldwide Survey of Encryption Products (2016), https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf [https://perma.cc/JMZ7-XRKU] (analyzing the quality and "jurisdictional agility" of encryption products).

As in the social media context, prosecution here should not be categorically ruled out and a careful cost-benefit analysis should not necessarily be fatal. Going Dark raises difficult questions about the responsibilities of private companies and the scope of government surveillance, but it would be a bridge too far to effectively grant immunity to an entire industry on the basis of its members' own system-design and marketing choices. That these firms provide valuable services with personal-liberty implications should not absolve them of responsibility when these services become widely and notoriously used as tools of terror.

C. Non-Traditional Financial Intermediaries

Beefed-up regulations imposed post-9/11 have been credited with largely driving terrorist finance out of the formal financial sector, as covered entities have stepped up monitoring and adopted more risk-averse postures.[237] Terrorists are still able to use traditional intermediaries to some degree, but the level of scrutiny now applied by at least Western institutions to customer activity writ large makes them increasingly inhospitable for bad actors. Legal and reputational risks have proven highly effective at motivating institutions to assist law enforcement; though a success in one sense, this has also pushed transactions to less-governed channels, including virtual currencies ("VCs").[238]

The degree to which VCs such as Bitcoin, Darkcoin, and others are presently used by FTOs and their supporters is unclear, but the relative anonymity and difficulty involved in tracing make them a potentially attractive means of transferring and storing funds.[239] The material support prosecution of a teenager who posted guides on how to donate Bitcoin to ISIS, along with media reports that hackers have located large virtual "wallets" linked to the group, may be leading indicators of greater use.[240] Supporters of nontraditional currencies dispute the degree of anonymity actually provided, pointing to public ledgers and successful, high-profile

[237] U.S. Dep't of the Treasury, National Terrorist Financing Risk Assessment 2015, at 2–3, 22 (2015).

[238] Id. at 47–57.

[239] Id. at 57–58.

[240] See, e.g., Kravets, supra note 63; Lewis Sanders IV, Bitcoin: Islamic State's Online Currency Venture, Deutsche Welle (Sept. 20, 2015), http://dw.com/p/1GZBo?tw [https://perma.cc/KE7K-A8SN].

prosecutions that have hinged on VC activity.[241] Regardless, investigative challenges posed by VCs are generally greater at present than those associated with the formal financial sector.[242] Furthering this appeal are "mixers" that quite literally offer VC laundering as a service, obfuscating the origin of assets through otherwise-purposeless exchanges with other users. Many mixers make scarce effort to conceal their intended use, making them interesting potential targets for prosecution.[243] As with social media and communications platforms, the nontraditional financial sector is rapidly evolving, and additional types of intermediaries are likely to emerge as VCs gain greater mainstream acceptance.

In addition to other potential grounds for criminal liability,[244] it is not a stretch to argue that VC mixers and other anonymizing services could be conceived of as providing "financial services" or "expert assistance" to FTOs under the material support statutes, or "services" more generally. These services could easily be used to conceal donations and make the task of tracing asset flows more difficult, as openly touted by their developers.[245] As with the other sectors examined in Sections III.A–B, the most significant challenge for prosecutors in this space would be proving a company had the requisite mens rea to support conviction. While legitimate intermediaries may heed new regulatory requirements, on the whole this is still very much a Wild West–type atmosphere relative to the formal financial sector.[246] Mixers often do not collect any personally identifying information on users or maintain transaction rec-

[241] See, e.g., Robert McMillan, Sure, You Can Steal Bitcoins. But Good Luck Laundering Them, Wired (Aug. 27, 2013, 6:30 AM), http://www.wired.com/2013/08/bitocoin_anonymity [https://perma.cc/223V-YVSP] (suggesting Bitcoin is a poor vehicle for large-scale money laundering); Lawrence Trautman, Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?, 20 Rich. J.L. & Tech. 13, 85–98 (2014) (discussing VC-related prosecutions).

[242] Trautman, supra note 241, at 39–41.

[243] See, e.g., Andy Greenberg, 'Dark Wallet' is About to Make Bitcoin Money Laundering Easier Than Ever, Wired (Apr. 29, 2014, 6:11 PM), https://www.wired.com/2014/04/dark-wallet [https://perma.cc/9783-T6S4] ("Wilson states plainly that he intends Dark Wallet to be used for anonymous online black markets like the Silk Road . . . .").

[244] Cf. Trautman, supra note 241, at 24 (discussing the availability of criminal penalties against VC intermediaries under money transmitter licensing and registration statutes, as well as general anti–money laundering statutes).

[245] Greenberg, supra note 243.

[246] See generally Trautman, supra note 241 (discussing VC-enabled illicit activity and attempts at regulation).

ords.[247] Such practices would appear to create a thick cloak of plausible deniability; if a mixer has no real view into who is using its platform and how they are using it, presumably it is not *knowingly* providing support to FTOs. As discussed below, however, willful blindness could do significant work in the context of VC intermediaries specifically designed to facilitate illegal activity.

From a plain reading of the statutory text, VC mixers and other intermediaries could also be candidates for prosecution under IEEPA for willful violations of E.O. 13224.[248] Mixing and transfer services appear to fit plainly within the E.O.'s prohibition on provision of services to SDGTs. Where VC intermediaries are not yet subject to or have otherwise not fallen in line with emerging regulatory mandates and do not maintain user information, it could be difficult to prove *willful* provision of services to SDGTs, unlike in the context of recent IEEPA prosecutions of highly regulated, mainstream banks.[249] Proving willfulness here would require showing an intermediary either acted with knowledge of the unlawfulness of its conduct or was otherwise willfully blind to such. Here, however, the nature of some VC intermediaries' business models may cut in favor of prosecution.

One could argue in both the material support and IEEPA contexts that a probability-based theory of willful blindness is more agreeable here than with encrypted messaging platforms. There is no fundamental right to financial privacy when dealing with third parties,[250] and there is certainly no fundamental right to launder money or finance terrorism. The privacy/security split on VCs is similar to that seen in Going Dark, and both can be seen as part of the broader debate on surveillance.[251] Arguments for shielding VC transactions from the government's view, however, are weaker in light of existing regulation of traditional financial

[247] BitLaunder appears particularly committed to anonymity; it only collects email addresses of users, and it states: "We will NOT comply with any court order for information pertaining to our clients, nor will we comply with any government request (of any country) for information about our clients." Privacy Policy, BitLaunder, https://bitlaunder.com/privacy_policy [https://perma.cc/86GZ-JW7W] (last visited Jan. 14, 2017).

[248] See supra notes 197–199 and accompanying text.

[249] Cf. sources cited supra note 138 (discussing emails showing banks' awareness of illegality).

[250] United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that there is no reasonable expectation of privacy in banking records).

[251] Cf. Greenberg, supra note 243 (conveying a Going Dark analogy between encrypted messaging and Bitcoin mixers).

services. Should evidence emerge that terrorists are making significant use of specific intermediaries, it would not appear wholly unreasonable to consider these outfits on notice and at risk of criminal liability for failing to police their platforms or otherwise provide assistance.[252]

Given that terrorist use of VC intermediaries is not well quantified at present, the potential operational impact of prosecution is unclear. However, the very nature of the services provided makes these firms ripe for exploitation by bad actors, a reality apparently contemplated or even welcomed in many cases.[253] The apparent bad faith of certain firms makes them easier targets for prosecution. Moreover, there are fewer concerns with respect to individual freedoms here than in the social media or messaging contexts, the threat of prosecution can and should be used more extensively to bring firms seeking to enter the mainstream into line.

D. Other Categories, and Three Hypothetical Targets

The material support statutes and IEEPA were designed to sweep broadly and address a range of evolving threats. These statutes could also conceivably be applied to a range of other intermediaries, including other financial-services providers, professional-services firms, or even an airline infiltrated by FTO operatives. ISIS's control of oil facilities in parts of Iraq, Syria, and elsewhere suggests energy firms operating in the region should tread carefully,[254] and the Treasury Department reportedly made inquiries to Toyota after propaganda videos featuring fleets of apparently-new trucks driven by ISIS fighters surfaced.[255] Given the poten-

[252] Cf. Knox, supra note 191, at 320–21 (discussing potential "notoriety theory" liability for social media).

[253] See Greenberg, supra note 243; Jake Halpern, Bank of the Underworld, Atlantic (May 2015), http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555 [https://perma.cc/CZ4N-DRCH].

[254] Terrorist Financing and the Islamic State: Hearing Before the H. Comm. on Fin. Servs., 113th Cong. 74–77 (2014) (statement of Jimmy Gurulé, Professor, Notre Dame Law School) (discussing E.O. 13224 and sales of black-market oil). Alternatively, one could imagine a Chiquita-type scenario where protection money is paid to FTOs to secure the safety of local workers. See supra notes 94–96 and accompanying text.

[255] See, e.g., Annika Fredrikson, Where Did ISIS Get All Those Toyotas? US Treasury Investigates, Christian Sci. Monitor (Oct. 7, 2015), http://fw.to/K7R6UPE [https://perma.cc/FL86-6LR7]. Though it is unclear whether the government's investigation into Toyota is ongoing or has been closed, no enforcement actions have been filed as of early 2017.

tial difficulties in proving knowledge or willfulness and collateral risks of prosecution, charges in the corporate realm may remain rare. The need for caution, however, must be weighed against signaling effects and the potential for even marginal disruption of terrorist logistics. Targeting corporate facilitators has been part of the DOJ's approach in addressing numerous other types of crime and threats, and taking a similar tack in the counterterrorism context is a reasonable and logical extension of this tactic.

By way of highly simplified and generic illustration, consider the hypothetical potential for bringing material support or IEEPA charges against each of three companies that are in the business of making and selling widely used widgets that also happen to be of use to terrorists. For the sake of the exercise, assume said widgets would fall into one of the broad statutory categories of material support and that dealings between the companies and their customers would qualify as transactions subject to IEEPA.

- Company A sells its widgets all over the world. One of its employees notices a large number of orders are going to Country X, which has been in the news frequently due to its ongoing civil war and the rise of a group that has been designated by the U.S. government as an FTO and an SDGT. The company investigates further and determines it has been doing business with members of the terrorist group. It immediately halts sales to Country X, implements monitoring systems and procedures to screen its customer base and reduce the risk of unwittingly supplying such groups with widgets, and reports the prior sales to the DOJ. Additionally, it assists law enforcement going forward by providing information on potentially suspicious orders and in response to investigative requests.

- Company B also sells its widgets all over the world, including in Country X. One of its employees has similar suspicions, and the company discovers it has also been selling widgets to the same terrorist group. Rather than cutting off this business, taking steps to ensure future compliance, or notifying law enforcement, the company proceeds as normal and continues do-

ing business with the terrorist group, even after employees explain to management that selling to the group is against federal law. A similar, alternative scenario could entail a decision by Company B to not investigate its employee's suspicions regarding shipments to Country X, which would enable it to avoid acquiring actual knowledge of dealings with the terrorist group.

- Company C likewise sells widgets worldwide. Unlike Companies A and B, it has catered its business model to address its customers' desire for privacy in their use of said widgets. The company collects little to no identifying information on its customers, and furthermore keeps few if any readable records of its transactions, standing by its promise to guard customers' privacy. In so doing, Company C may be aware that growing numbers of its widgets are going to Country X, but it is effectively unable to determine who it does business with and is incapable of providing any meaningful response to law enforcement requests for information.

While these scenarios are magnitudes of order less complex than those likely to face prosecutors in reality, they can still in a rudimentary way illustrate the spectrum of potential corporate targets. Company A, though it failed to prevent initial sales to the FTO, conducted an investigation in response to employee concerns, implemented measures to ensure future compliance, and provided assistance to the government. Thus, it would have an argument that it did not *knowingly or willfully* do business with the FTO, and that it at least took steps to investigate, remediate, and cooperate once transactions were identified.[256] Company B falls on the opposite side of the spectrum given its confirmation of (or willful blindness to) the fact of illegal transactions and its decision to maintain business as usual; it would face a much greater challenge in arguing for leniency if the government later discovered the violations. Company C falls in the middle of the spectrum and seems to pose a

[256] As alluded to earlier, Company A could still face enforcement action under IEEPA's civil provisions, which provide for strict liability. 50 U.S.C. § 1705(a) (2012) ("It shall be unlawful for a person to violate, . . . any license, order, regulation, or prohibition issued under [50 U.S.C. §§ 1701 et seq.].").

more difficult case to resolve one way or the other, given its lack of affirmative monitoring and the fact that it has designed its business in such a way as to acquire little to no useable information about its customers and their activities.

It seems reasonable to assume that more of the cases confronted by prosecutors will look like Companies A or C than will look like Company B, and that all scenarios, even those closer to the one posed by Company B, will require weighing a panoply of factors prior to arriving at a decision to charge a company. That said, IEEPA and the material support statutes are invaluable components of the DOJ's counterterrorism arsenal, and could have an even greater impact if employed in the corporate context.

IV. OVERARCHING CONCERNS AND SAFEGUARDS

Beyond sector-specific critiques, the approach discussed in Part III may raise broader concerns irrespective of the type of company targeted. Pursuit of non-U.S. companies could be seen as having a low potential return on investment given the challenges often encountered in cross border investigations.[257] This critique, while valid, gives short shrift to prior successes in international prosecutions. Moreover, the difficulty of investigation or presence of competing priorities should not be used to justify inaction broadly at the outset. There is also an argument that the threat of terrorism-related prosecution under IEEPA or the material support statutes places undue burdens on intermediaries by creating BSA-like compliance obligations without affirmative statutory mandates. For many companies, implementing controls to meaningfully monitor customer bases and platform activity could require making significant compliance expenditures or even redesigning technological infrastructure, potentially at the expense of data security. There may be related concerns as to appropriate expectations of private industry and the conscription of companies as de facto deputies of law enforcement; the DOJ's apparent "failure to prevent" theory of corporate criminal liability was was the subject of sharp criticism in light of the FedEx prosecution, both

[257] Cf. Devlin Barrett et al., In Europe's Terror Fight, Police Push to Access American Tech Firms' Data, Wall St. J. (May 1, 2016), http://on.wsj.com/1rJIT81 (discussing information-sharing issues in cross border investigations).

initially and in the aftermath of prosecutors' mid-trial decision to drop the case.[258]

Those embracing deputization-related critiques are largely unmoved by appeals to good corporate citizenship and the reality that firms are critical, if largely unwitting, enablers of a range of threats, finding the public-private distinction unsettlingly blurry.[259] However, the assistance of private industry has proven invaluable in the law enforcement and national security contexts. While perhaps not *embracing* deputization, financial-services firms, telecom carriers, and others have come to accept it as part of doing business.[260] Given the threat posed and the unique position many firms occupy vis-à-vis modern FTOs, it is not unreasonable to hold corporations accountable for how their products and services are used when these services are widely exploited by terrorists and these same companies fail to act. While affirmative statutory mandates may be preferable, the threat of terrorism-related prosecution, wielded carefully, could also prod holdouts to pitch in.

The lack of a specific intent requirement under § 2339B has been a persistent source of criticism.[261] Amending the statute to require intent to further the *terrorist* activities of an FTO would ignore the fungibility principle recognized by the Court in *Holder v. Humanitarian Law Pro-*

[258] See, e.g., Ring & Coleman, supra note 7; A Mammoth Guilt Trip, supra note 123 ("[The FedEx prosecution] raises a lot of questions about what a company can and should know about [its] customers."); see also Press Release, FedEx, FedEx Announces Successful Conclusion of Internet Pharmacy Case (June 17, 2016), http://about.van.fedex.com/newsroom/global-english/fedex-announces-successful-conclusion-internet-pharmacy-case [https://perma.cc/5M5D-KX89] ("The case never should have been brought. . . . Many companies would not have had the courage or the resources to defend themselves against false charges." (internal quotation marks omitted)).

[259] See Jon D. Michaels, Deputizing Homeland Security, 88 Tex. L. Rev. 1435, 1452–66 (2010) (discussing challenges posed by the deputization of private actors, including market distortion, denial of services, and potential expansion of the scope of de facto state action).

[260] Though banks and phone companies have affirmative statutory duties to provide information and assistance to law enforcement, the IEEPA regime for one does not impose similarly explicit requirements. Nevertheless, IEEPA effectively imposes duties that firms ignore at their peril. Cf. Hong, supra note 19 (providing background on IEEPA and discussing recent prosecutions); Pick, supra note 200 (noting the lack of an affirmative obligation to maintain an IEEPA compliance program, but adding banks (and by extension, other companies) "sort of just *have* to" given potentially severe consequences of being found in violation of U.S. sanctions).

[261] See, e.g., Cole, supra note 72, at 724–25 (arguing the material support statutes effectively impose "guilt by association" and arguing in favor of amending the statutes to require intent to further an FTO's *illegal* acts).

ject and undermine the entire material support framework as it stands today, enabling adherents to frame contributions as support for "neutral" activities.[262] This could in turn drastically reduce the incentives that detached intermediaries have to monitor their customer bases and employees, as the government would likely be hard-pressed to prove that a mainstream intermediary provided material support with the intent to further actual terrorist activities. Though cooperation is explicitly incorporated in DOJ guidelines for corporate charging decisions,[263] an argument can be made for statutory safe harbors for firms that make good-faith efforts to assist authorities, perhaps along the lines of suspicious-activity reporting mandates under the BSA. Although this could assuage concerns of well-meaning intermediaries, safe harbors could also have the effect of overwhelming law enforcement with a flood of unvetted reports and unnecessary "defensive filings" made more out of a desire for insulation from prosecution rather than genuine or even reasonable suspicions as to the underlying activity.[264] Moreover, codifying exemptions that could be exploited by firms that do business with terrorists for an extended period and then have a change of heart (or new appreciation of legal exposure) is at least somewhat unattractive.

At the same time, prosecuting firms that have provided substantial assistance to authorities may be inadvisable, as was arguably shown in the FedEx case.[265] DOJ guidelines on prosecuting business organizations, while not formally binding on prosecutors, outline a number of factors to be considered in addition to the sufficiency of evidence and likely effects of charges, among them: timely and voluntary disclosure of wrongdoing; the willingness to cooperate in the investigation of its agents; the pervasiveness of wrongdoing within the organization, including complicity by senior management; and remedial actions taken, including efforts to implement or improve compliance programs and co-

[262] Holder v. Humanitarian Law Project, 561 U.S. 1, 29–34 (2010).

[263] See, e.g., Michael Volkov, The Real Impact of Aggressive AML/BSA Enforcement, VolkovLaw: Corruption, Crime & Compliance (Jan. 19, 2015), http://blog.volkovlaw.com/2015/01/real-impact-aggressive-amlbsa-enforcement [https://perma.cc/P2G4-H3BG] (noting and questioning value of significant increases in Suspicious Activity Report filings).

[264] Id.

[265] Todd, supra note 177 (outlining FedEx's planned defense of focusing on assistance provided to authorities).

operation provided to relevant agencies.[266] While there is no absolute compliance defense, demonstration of meaningful and substantial efforts to prevent violations of law, remediate compliance gaps, and cooperate with investigations of both the company itself and its customers or users may cut in favor of a firm potentially facing charges. The flip side of such discretion is that prosecutors are also instructed to consider the nature and seriousness of the alleged violations, including the "risk of harm to the public" and the intersection with federal law enforcement priorities, which would arguably cut against a firm that has knowingly or willfully provided services to terrorists.[267] Like any good multifactor balancing test, corporate charging decisions are fact- and circumstance-intensive. Factors may be weighed differently across the range of cases, and ultimately the decision is one of "thoughtful and pragmatic judgment" by prosecutors.[268]

In the context of a potential corporate material support or E.O. 13224-related IEEPA case, it would seem to behoove a targeted company to be able to demonstrate actual, good-faith effort to prevent or otherwise report terrorist usage of its products or services. Such compliance efforts could take many forms depending upon the industry. For example, a social media firm may point to efforts to block or remove terrorist content and accounts, outreach to authorities about potential threats, and cooperation with lawful requests for user information. Messaging platforms and nontraditional financial intermediaries acting in good faith could point to efforts to obtain know-your-customer information and to maintain access to useable data in such a manner so as not to frustrate investigative requests. By contrast, a firm that has made little such effort and is demonstrably aware of its (actual or highly likely) exploitation by FTOs could find arguing for leniency an uphill battle given the gravity of terrorism-related charges and implication of national security concerns.

Those unsatisfied by plain-vanilla prosecutorial discretion should draw additional comfort from DOJ policies that cover investigations of potential material support and E.O. 13224-related IEEPA violations.[269]

[266] USAM, supra note 120, § 9-28.300 (discussing relevant considerations in corporate charging decisions).
[267] Id. §§ 9-28.300, 9-28.400.
[268] Id. § 9-28.300 cmt.
[269] Id. § 9-2.136.

In contrast to the broad control that prosecutors and individual U.S. Attorneys' Offices have generally, the DOJ currently requires consultation with its National Security Division *prior to* initiation and *throughout* any international terrorism investigation. Aimed at avoiding conflicts between intelligence and law enforcement activities, such policies appear to place a meaningful check on investigations and acknowledge the varied interests implicated in such cases.[270] While these policies are not codified in law and are subject to change both across and during administrations, there appears to be pragmatic appeal in leaving speed bumps in place for terrorism prosecutions due to the range of interests at stake.

Given the potentially significant penalties and the stigma of charges connoting endorsement of terrorist aims or indifference in the face of the "see something, say something" ethos, the approach proposed in this Note may draw critiques. As should be evident from the foregoing discussion, however, the risk of unsupported corporate prosecution is minimized by existing statutory provisions, structural protections, and DOJ charging policies. The desirability of a more aggressive approach to investigating and prosecuting terrorism-related violations in the corporate realm presumes good faith and depends in part on "[dedication] to the spirit of fair play and decency" that then-Attorney General Robert Jackson decades ago argued "should animate the federal prosecutor."[271] The threat of prosecution must only be brought to bear where supported by evidence and law, and where such a prosecution would serve the aims of criminal law as well as national security-related interests in this context. But where so supported, such cases can and should be pursued.

CONCLUSION

More than fifteen years post-9/11, the United States faces a continued, persistent threat of terrorist attacks at home and abroad by increasingly decentralized groups. Conventional military and intelligence operations will continue to be important parts of U.S. counterterrorism strategy, but these provide incomplete coverage. To more fully protect U.S. nationals and U.S. interests, the government must continue to adapt and employ the all-tools approach it embraced after 9/11, including the aggressive

[270] Id. §§ 9-2.136(D), 9-2.136(H), 9-90.000.

[271] Robert H. Jackson, Att'y Gen., Address at the Second Annual Conference of United States Attorneys: The Federal Prosecutor 3 (Apr. 1, 1940).

and even creative use of existing criminal statutes. Targeted and appropriately cautious use of the material support statutes and IEEPA against detached intermediaries that provide terrorists with logistical support could pay dividends in terms of more robust assistance to law enforcement and disruption of terrorist supply chains. The DOJ has embraced similar targeting of intermediaries in other contexts, including where such an approach may previously have seemed unimaginable. It is not unreasonable in the context of counterterrorism to target companies that knowingly facilitate terrorist activities or otherwise take a see-no-evil approach to business that exposes the public to significant risk.

The aim of this proposal is not to ensnare companies acting in good faith or to rack up fines, but rather to provide additional incentive for firms to assist law enforcement. A clearer threat of prosecution would serve to encourage firms not already on board to step up cooperation. Application of IEEPA or the material support statutes in this context would raise tough and unresolved subsidiary questions, but novelty is not a sufficient reason to employ a strict wait-and-see approach to the other issues that are implicated. Actual prosecution should not be pursued where not supported by facts or where probable collateral effects outweigh likely gains, but it is an avenue that should be considered and pursued where firms exploited by terrorists take the stance that this is strictly a problem for the government to solve. An effective all-tools strategy requires imagination and adaptation, and the material support statutes and IEEPA are tools the DOJ can and must continue to sharpen.