THE ROLE OF INTERNET INTERMEDIARIES IN TACKLING TERRORISM ONLINE

*Raphael Cohen-Almagor**

INTRODUCTION

John took a stool to the street, stood on it, and started shouting in a loud voice: "I want to kill a soldier. Would you join me? I will kill a soldier. Come on with me. Soldiers deserve death."

John's target was not named. The target was generic: a soldier, any soldier. John's intention was nevertheless dangerous. The speech conveyed a violent message and was aimed to recruit support for translating ideas into action. In most countries—the United States included—John would be questioned by police. The threat would not go unnoticed. The speech might well have repercussions. But if John were to say the same words online, he might be able to enjoy free speech protection. Why does the mode of communication make a difference? Why is the mode of communication more important than the content of the speech?

Now consider a second scenario. Lee is a school guard. His role is to ensure that only people who have business in the school are allowed in. One day, a man approaches the gate. Lee asks for the man's identification. In response, the man produces a certificate written in a foreign language. Would Lee still allow the man in? The most likely answer is "no." Lee would insist on seeing some form of identification that he is able to read to make sure that the man is who he claims to be. Responsible gatekeepers are expected to take their role seriously.

Many online gatekeepers, however, do not think they have any responsibility for content. Furthermore, permissive online gatekeepers not only allow speech, they facilitate it. They provide platforms and connect speakers with many other people, sometimes anonymously. Online gatekeepers are enablers and protectors of speakers. Why is online gatekeeping fundamentally different from offline gatekeeping? Is this difference justified?

* Professor and Chair in Politics, University of Hull. I am grateful to Scott Atran, Jack Balkin, Richard Oliver Collin, Paul Giannasi, Ivan Koedjikov, Sam Lehman-Wilzig, Steve Newman, Marc Sageman, Stephanos Stavros, John Trumpbour, Alex Tsesis, Jonathan Vick, and Chris Wolf for their constructive comments. This Article was prepared for the *Fordham Law Review* symposium entitled *Terrorist Incitement on the Internet* held at Fordham University School of Law. For an overview of the symposium, see Alexander Tsesis, *Foreword: Terrorist Incitement on the Internet*, 86 FORDHAM L. REV. 367 (2017).

This Article focuses on the role internet intermediaries play in facilitating and encouraging terror. It also focuses on internet intermediaries' moral and social responsibilities to fight terror. The fight against radicalization and terror requires all pertinent stakeholders to cooperate and share responsibility.

Gatekeeping is defined as the work of third parties "who are able to disrupt misconduct by withholding their cooperation from wrongdoers."[1] Internet intermediaries need to be far more proactive as gatekeepers than they are now. Socially responsible measures can prevent the translation of violent thoughts into violent actions. Designated monitoring mechanisms can potentially prevent such unfortunate events. This Article suggests an approach that harnesses the strengths and capabilities of the public and private sectors in offering practical solutions to pressing problems. It proposes that internet intermediaries should fight stringently against terror and further argues that a responsible gatekeeping approach is good for business.

Part I defines terror. Next, Part II discusses the role of social networking sites in facilitating terror and argues that principles of Corporate Social Responsibility (CSR) should dictate censorship of online terror. Part III shows that the great internet companies are slowly coming to understand that with great power comes great responsibility. Part IV then argues that internet intermediaries have a role to play beyond providing a platform to anyone with something to say. Social responsibility dictates some minimal standards of gatekeeping without which mayhem and destruction will ensue unabated. The policy of "anything goes" is self-defeating and irresponsible. Internet companies are expected to show readiness to work with governments to hinder terror activities. The industry should be encouraged to be proactive.

I. DEFINING TERROR

There is no internationally agreed-upon definition of terrorism.[2] But the majority of definitions include the following components:

(1) Terrorists are nonstate actors, and are state sponsored, or both. The focus here is on individuals. Terrorist states are another matter.[3]

[1] Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 53 (1986).

[2] For a discussion on the complicated task of defining terrorism, see STELLA MARGARITI, DEFINING INTERNATIONAL TERRORISM: BETWEEN STATE SOVEREIGNTY AND COSMOPOLITANISM 2–3 (2017); GUS MARTIN, ESSENTIALS OF TERRORISM: CONCEPTS AND CONTROVERSIES 2–25 (2d ed. 2010); GUS MARTIN, UNDERSTANDING TERRORISM: CHALLENGES, PERSPECTIVES, AND ISSUES 22–45 (5th ed. 2016); Boaz Ganor, *Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?*, 3 POLICE PRAC. & RES. 287 (2002); Alex P. Schmid, *The Definition of Terrorism*, *in* THE ROUTLEDGE HANDBOOK OF TERRORISM RESEARCH 39, 39–157 (Alex P. Schmid ed., 2011).

[3] For a discussion of state terrorism, see HARVEY W. KUSHNER, ENCYCLOPEDIA OF TERRORISM 342–46 (2003); Jonathan Glover, *State Terrorism*, *in* VIOLENCE, TERRORISM, AND JUSTICE 256, 256–75 (Raymond Gillespie Frey & Christopher W. Morris eds., 1991); Igor

(2) The terrorist's *motivation* is customarily devoid of personal gain. It is ordinarily political, religious, or ideological. Acts of terror are usually the work of a small number of committed individuals who strive for what they perceive as the greater good of a larger group with which the terrorists identify.

(3) The terrorist's aims are twofold: (a) to undermine, hurt, or destroy the enemy and (b) to spread fear widely among the targeted population and beyond.

(4) Terrorists do not follow rules. They are willing to break any rule to promote their ends. International conventions do not apply to them. Breaking all norms and rules is the terrorist's guiding rule.

(5) The means may have no limits.[4] Terrorists are often willing to justify all means to achieve their goals. They often employ violence or threats of violence against targets.

(6) Every person who does not belong to the terrorist group or is not an ally is potentially included in the general category of "the enemy." The targets include noncombatants, innocent civilians, and representatives of the state.

(7) Terrorists can be anywhere. Any location may be regarded as a legitimate locus for destruction. Terrorists wish to surprise, to keep the enemy on its toes, to exhaust, to instill fear, and to stretch the enemy's resources. They attack anywhere they can.[5]

In recent years, terrorism has been a constant presence in our lives. Governments try to curb terror while the global media covers its deadly results. Terrorism is of great public interest. It is impossible to ignore. Elsewhere I have analyzed the relationships between media and terror,[6] how terrorists use the internet,[7] and what can be done to counter their activities.[8] The focus of this Article is the role of social networking sites in assisting and facilitating terror. While this Article focuses on Islamic terrorism, its reasoning applies to other forms of terrorism as well.

Primoratz, *State Terrorism and Counter-Terrorism*, *in* TERRORISM: THE PHILOSOPHICAL ISSUES 113, 113–40 (Igor Primoratz ed., 2005).

[4] In his comments on a draft of this paper, John Trumpbour noted that the IRA on numerous occasions issued warnings or took steps to avoid civilian carnage. Comments by John Trumpbour, Research Director, Labor and Worklife Program, Harvard Law School (Mar. 4, 2017) (on file with author). Indeed, some terrorists are more careful about taking human lives than others. *Id.*

[5] Ivan Koedjikov commented that defining terror is in the program of the Council of Europe's Committee of Experts on Terrorism (CODEXTER). Comments by Ivan Koedjikov, Head of Action Against Crime Department of the Council of Europe (Apr. 4, 2017) (on file with author) [hereinafter Koedjikov Comments]. The committee is expected to complete its work in 2018. *Id.*

[6] *See generally* Raphael Cohen-Almagor, *Media Coverage of Acts of Terrorism: Troubling Episodes and Suggested Guidelines*, 30 CANADIAN J. COMM. 383 (2005); Raphael Cohen-Almagor, *The Terrorists' Best Ally: The Quebec Media Coverage of the FLQ Crisis in October 1970*, 25 CANADIAN J. COMM. 251 (2000).

[7] *See* Raphael Cohen-Almagor, *Jihad Online: How Do Terrorists Use the Internet?*, *in* MEDIA AND METAMEDIA MANAGEMENT 55, 55 (Francisco Campos Freire et al. eds., 2017).

[8] *See* Raphael Cohen-Almagor, *In Internet's Way: Radical, Terrorist Islamists on the Free Highway*, INT'L J. CYBER WARFARE & TERRORISM, Sept. 2012, at 39.

II. THE ROLE OF SOCIAL NETWORKING SITES IN FACILITATING TERROR

Modern terrorism relies heavily on the internet. Both modern terrorism and the internet have common features that promote close relations: they are global and diffusive, they do not require one center, their operation does not require a very large budget, innovation is important to sustain both, and their operation can be carried out through clandestine means.

Terrorists and their collaborators strive to keep their identity, their modes of operation, and their plans secret. They use advanced technological tools to secure their privacy and anonymity. They are quick to adapt to new innovations and to exploit technological advantages as means to nefarious ends. Clandestine modes of operation generate the necessary funding to maintain solvency. Terrorists are working in international cells and rings that contest geographical boundaries. Thus, considerable resources and the close cooperation of law enforcement agencies are required to obstruct terrorist activities.

More than 27,000 foreign fighters have traveled to Iraq and Syria since fighting broke out there in 2011.[9] Approximately 6000 of those fighters came from European countries, most notably France, Germany, and the United Kingdom.[10] Approximately 760 United Kingdom-linked fighters have traveled to Syria and Iraq since the conflicts began in those countries.[11] Some of them have returned to the United Kingdom and could undermine the country's security.[12]

In August 2016, the United Kingdom Home Affairs Committee published a report on terror and political extremism.[13] The report probes the role of the government, communities, media, and technology, aiming to contain radicalization and promote security and peace of mind.[14] The report accentuates the need for responsible conduct. The fight against radicalization and terror requires all pertinent stakeholders to cooperate and share responsibility to prevent violence. The report states that

> [s]ocial media companies are consciously failing to combat the use of their sites to promote terrorism and killings. Networks like Facebook, Twitter and YouTube are the vehicle of choice in spreading propaganda and they have become the recruiting platforms for terrorism. They must accept that the hundreds of millions in revenues generated from billions of people using their products needs to be accompanied by a greater sense of

[9] Ashley Kirk, *Iraq and Syria: How Many Foreign Fighters Are Fighting for ISIL?*, TELEGRAPH (Mar. 24, 2016, 3:45 PM), http://www.telegraph.co.uk/news/2016/03/29/iraq-and-syria-how-many-foreign-fighters-are-fighting-for-isil/ [https://perma.cc/V4YV-MLW7].

[10] *Id.*

[11] *Id.*

[12] HOUSE OF COMMONS, HOME AFFAIRS COMMITTEE, RADICALISATION: THE COUNTER-NARRATIVE AND IDENTIFYING THE TIPPING POINT, 2016, HC 135, at 7 (UK) [hereinafter HOUSE OF COMMONS], https://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/135/13502.htm [https://perma.cc/29C7-XYXB].

[13] *See id.*

[14] *See id.*

> responsibility and ownership for the impact that extremist material on their sites is having.[15]

The report calls for a "zero tolerance approach to online extremism, including enticement to join extremist groups" to glorify them or to commit terror attacks.[16] It recommends the removal of terrorist manuals from the internet.[17] Similarly, my book *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway* recommends that there should at the very least be restricted areas on the internet which people should have to register for to access certain forms of speech that are presently shielded under the First Amendment.[18] Thus, if you develop an interest in terrorism, you will need to leave verifiable details.[19] Morally speaking, we cannot be neutral regarding such alarming speech.[20] We must take some precaution. Requiring people to register to access sites where they could view videos advocating bloodthirsty revenge and establishment of the caliphate by the sword would allow scholars to see what is on the internet while somewhat limiting the proliferation of these videos on open platforms. An open and transparent policy is essential to alleviate justified civil liberty concerns when we aim to crack down on these vile propaganda videos and violent messaging.

The United Kingdom Home Affairs Committee report voiced dismay that social media "companies have teams of only a few hundred employees to monitor networks of billions of accounts and that Twitter does not even proactively report extremist content to law enforcement agencies."[21] The report states:

> These companies are hiding behind their supranational legal status to pass the parcel of responsibility and refusing to act responsibly in case they damage their brands. If they continue to fail to tackle this issue and allow their platforms to become the "Wild West" of the internet, then it will erode their reputation as responsible operators.[22]

Indeed, these companies have reputations to preserve and they do not wish to be subjected to legal liability.[23]

During the past decade, I have spoken with dozens of security officers in the United Kingdom, the United States, Canada, Australia, and Israel. They all voiced their growing frustration with the media giants' neutral attitude towards free speech. My own experience in communicating with representatives of internet intermediaries is no different. They stand behind their free speech reasoning with little attention to competing considerations

[15] *Id.* at 34.

[16] *Id.* at 14.

[17] *Id.*

[18] RAPHAEL COHEN-ALMAGOR, CONFRONTING THE INTERNET'S DARK SIDE: MORAL AND SOCIAL RESPONSIBILITY ON THE FREE HIGHWAY 159 (2015).

[19] *Id.* at 159–60.

[20] *Id.* at 160.

[21] HOUSE OF COMMONS, *supra* note 12, at 14.

[22] *Id.*

[23] *See id.*

that would require more sophisticated tools for balancing. The rationales offered by Facebook and other internet intermediaries are of different sorts. There are principled reasons grounded in the free speech principle. There are pragmatic, business-oriented reasons anchored in the need for innovation. And there are technical reasons rooted in the sheer difficulty of monitoring the enormous volume of content introduced onto the internet on a daily basis.

In May 2015, Facebook Director of Policy Simon Milner delivered a speech in Jerusalem.[24] He said that most of the content on Facebook is positive.[25] Facebook wants to provide as much of a voice to as many people as possible.[26] Some people, however, contravene Facebook's community standards.[27] Milner acknowledged that he has to be a guardian of the Facebook community.[28] Content that does not adhere to these standards should be removed. People can complain about problematic speech.[29] Every complaint is reviewed by at least two people to ascertain whether the speech in question is indeed hateful.[30] Facebook informs people of how their complaints were decided.[31] Milner noted that speech flagged as potentially terrorist is a priority.[32] Such speech is singled out and then checked by language experts to see if it violates the standards.[33]

Milner emphasized two issues. First, that threats of violence should be directed to law enforcement. Officers then will contact Facebook and the company will cooperate with them.[34] Facebook trains law enforcement to deal with such content.[35] Second, Milner stressed the importance of counterspeech.[36] Recall the fictitious story about Lee the school guard that opened this Article. It is of the utmost importance that internet gatekeepers employ individuals who have mastered the more popular languages used by terrorists so they can decide whether or not violence is being incited. Tools like Google Translate can be useful as well, but presently they are still quite limited in their usefulness.

Later in 2015, I met with Milner in London. We discussed whether Facebook should adopt a proactive policy regarding online content.[37] I spoke of the need to adopt a proactive business approach in inspecting and removing violent and dangerous content.[38] Milner explained that Facebook

[24] Israel's Ministry of Foreign Affairs, *Facebook's Simon Milner—The Oldest Hatred in the Newest Vessels: Toward Solutions*, YOUTUBE (May 14, 2015), https://youtu.be/t2M4VJY99w4 [https://perma.cc/EZR8-3RXY].

[25] *Id.*

[26] *See id.*

[27] *See id.*

[28] *Id.*

[29] *See id.*

[30] *See id.*

[31] *See id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] Interview with Simon Milner, Facebook Dir. of Policy for U.K., Middle E., & Afr., Facebook, in London, U.K. (July 22, 2015) [hereinafter Milner Interview].

[38] *Id.*

has no intention to be more proactive in inspecting content on its server.[39] Milner espoused several arguments to explain why passivity is a good business model for Facebook and why it is wrong to expect social networking companies to change to a proactive monitoring policy.[40]

The first argument is that freedom of expression is of crucial importance. Milner stressed the liberal concept of fighting opinions with opinions and argued that Facebook's officers are not equipped with the ability and knowledge to identify "bad speech" as distinct from "good speech."[41]

Second, the internet business model is based on innovation. Innovation requires freedom of expression and freedom to have ideas and promote them in the marketplace of ideas. Milner uttered the same words he used in Jerusalem, emphasizing the importance of counterspeech.[42] Facebook wants to provide as much of a voice as possible to as many people as possible.[43] This argument is well known in the literature.[44] While free speech advocates recognize the internet's dangers, they argue that free speech should shield all but the most immediately threatening expression. For them, the substantive danger is censorship. Freedom of expression is perceived as a fundamental human right and censorship should not be allowed to inhibit the internet's free flow of information.

In 1996, the U.S. Congress enacted the Communications Decency Act (CDA).[45] The CDA provides strong, wide-reaching protections for internet intermediaries from attempts to (1) impose liability on them for content posted by others or (2) force them to police the content posted online.[46] By protecting online providers from intermediary liability, Congress enabled a range of innovative new websites to offer social networking, video sharing, and other "Web 2.0" services that have transformed how we do business and socialize online.[47] In his testimony before the House Committee on Homeland Security, John Morris of the Center for Democracy and

[39] *Id.*

[40] *Id.*

[41] *See id.*

[42] *Id.*

[43] *See supra* note 26 and accompanying text.

[44] *See, e.g.*, *Internet Terror Recruitment and Tradecraft: How Can We Address an Evolving Tool While Protecting Free Speech?: Hearing Before the Subcomm. on Intelligence, Info. Sharing, & Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 111th Cong. 29–30, 33–35 (2010) [hereinafter *Morris Hearings*] (statement of John B. Morris, General Counsel, Center for Democracy and Technology); YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 355 (2006); MANUEL CASTELLS, COMMUNICATION POWER 190–91 (2009); MANUEL CASTELLS, THE INTERNET GALAXY: REFLECTIONS ON THE INTERNET, BUSINESS, AND SOCIETY 24–25, 46–47, 54–55 (2001); LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 238–39 (2001); TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 122–23 (1st ed. 2010); Leonard Kleinrock, *History of the Internet and Its Flexible Future*, IEEE WIRELESS COMM., Feb. 2008, at 8, 15.

[45] Pub. L. No. 104-104, §§ 501–509, 110 Stat. 56, 133–39 (1996) (codified at 47 U.S.C. § 230 (2012)).

[46] *See* 47 U.S.C. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

[47] *See Morris Hearings*, *supra* note 44, at 30.

Technology argued, "A decision by Congress to step back from such protections and to impose obligations on service providers to police on-line content—even in the effort to fight terrorism—would have serious and harmful implications both for free speech on-line and for innovation and competition in on-line services."[48]

John Morris and others are seriously concerned that obligations to police content will have a chilling effect on speech.[49] Internet intermediaries will be preoccupied with monitoring at the expense of innovating. The demand for proactivity would have profound chilling effects on internet intermediaries' willingness or ability to host content created by others. They might not publish at all rather than risk publishing problematic speech, or they might waste resources dedicating teams to monitor their servers.

Morris further argues that the demand for proactivity would also chill internet users' freedom of expression.[50] Because they would know that internet intermediaries monitor speech, users would screen "content before it is posted on-line, creating an indirect prior restraint on speech and inevitably leading to less user-generated content overall."[51] "In some instances," Morris warned, "entire platforms for expression simply could not exist because the sheer volume of content would make it impossible or economically unviable for the company to screen all user-generated content."[52]

Another argument in support of the passivity voiced by Facebook, the Center for Democracy and Technology, and others, is that large internet intermediaries simply are unable to screen all information. For example, YouTube has over one billion users.[53] Every second, one hour of video is uploaded to YouTube.[54] If liability concerns compelled YouTube to examine each video before allowing it to be posted, YouTube could not continue to operate as an open forum for user expression. The same is true for Facebook and other social networking sites where internet users post hundreds or thousands of comments every hour.

Milner voiced a strong objection to monitoring.[55] For him, monitoring is far too intrusive.[56] Facebook does not adopt such a proactive policy just as British Telecom (BT) does not monitor phone conversations to detect

[48] *Id.*

[49] *Id.* at 34; *H.R. 5777, the 'Best Practices Act,' and H.R.—, a Discussion Draft to Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to That Individual: Hearing on H.R. 5777 and H.R.— Before the Subcomm. on Commerce, Trade, & Consumer Prot. of the H. Comm. on Energy & Commerce*, 111th Cong. 123 (2010) [hereinafter *Harris Hearings*] (statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy and Technology).

[50] *Morris Hearings*, *supra* note 44, at 34.

[51] *Id.*

[52] *Id.*

[53] *YouTube for Press*, YOUTUBE, https://www.youtube.com/yt/about/press/ [https://perma.cc/Z4VX-6KL5] (last visited Oct. 16, 2017).

[54] *One Hour per Second*, YOUTUBE, http://www.onehourpersecond.com/ [https://perma.cc/LQ8F-D5RX] (last visited Oct. 16, 2017).

[55] Milner Interview, *supra* note 37.

[56] *See id.*

terrorist activity.[57] Intelligence—that is, acting upon the advice of others who bring such activity to the attention of Facebook—is the key. Facebook has adopted a policy of continued passivity on the whole, mitigated by activity when a request is made. This policy, according to Milner, is far more effective than monitoring vast amounts of content.[58] There is no need to monitor many millions of posts when only a small number of these posts are problematic.[59] According to Milner, the police do not try to monitor all information because they do not have enough manpower to do so.[60] This prompted Facebook's policy director to bring economic considerations to the fore. At present, Facebook is reluctant to allocate funding for this task; important as it might seem to be, it is not *that* important.

Of course, we all support freedom of expression. But freedom of expression surely has boundaries to prevent escalation to lawlessness.[61] Fighting radical speech with more speech is certainly a welcome reaction, but it might be insufficient. Flagging radical, violent speech is not rocket science. Given that terror organizations like ISIS have made heavy use of social media and other digital platforms to recruit, fundraise, and communicate, the Trump administration is examining what it would take to scan social media accounts and cell phone contacts of all visitors to the United States, making "social media screening" a part of the screening process to enter the country.[62] By the same logic, internet intermediaries might be expected to screen users before allowing terrorists to use their networks.[63]

I suggest that a group of talented Facebook software engineers devise a search algorithm that would flag out a string of words that may indicate that a person is engaged in antisocial and dangerous expression. By "antisocial," I refer to (1) terrorists, those who support holy war against the West, infidels, and those who defy Islam, and (2) jihadists, those who wish to expand Islam in the world. Jihadists believe in a perpetual struggle to defend Islam utilizing violence and force, if necessary.[64] But jihadists do not necessarily

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *See* JEREMY WALDRON, THE HARM IN HATE SPEECH 13–14 (2012). *See generally* RAPHAEL COHEN-ALMAGOR, THE BOUNDARIES OF LIBERTY AND TOLERANCE: THE STRUGGLE AGAINST KAHANISM IN ISRAEL (1994) (arguing that there are grounds for boundaries to expression under the harm and offense principles); JOHN STUART MILL, UTILITARIANISM, LIBERTY, AND REPRESENTATIVE GOVERNMENT (1950) (arguing that under the harm principle, speech can be limited to prevent harm).

[62] Kalev Leetaru, *We Already Screen Cell Phones at the Border, Will Social Media Be Any Different?*, FORBES (Jan. 29, 2017), https://www.forbes.com/sites/kalevleetaru/2017/01/29/we-already-screen-cell-phones-at-the-border-will-social-media-be-any-different [https://perma.cc/W4Q4-5GC2].

[63] In his comments, Chris Wolf notes that there are anecdotal reports that platforms use algorithms to screen for terrorists. Comments by Chris Wolf, Attorney, Hogan Lovells (Mar. 7, 2017) (on file with author). Social network platforms are asked to provide some degree of transparency about algorithmic screening for content.

[64] *See* Alexei Malashenko, Stephen R. Bowers & Valeria Ciobanu, *Encyclopedia of Jihad: Islamic Jihad*, CTR. FOR SECURITY & SCI. 4 (2001), http://www.c4ss.net/website/

take part in acts of terror. They provide legitimacy and encouragement to the terrorists.

Facebook takes issues less pressing than terrorism very seriously. For example, it has a team of specialists to deal with suspected fake identities.[65] Because human lives—precisely what is at stake in terrorism—are not less significant than fake identities, Facebook should adopt a similar attitude to combat radical, extremist expressions. After flagging a string of violent words, a team of people who monitor Facebook would then look at the context and, if they believe that terrorism is taking place, they would swiftly intervene, remove the dangerous content, and block the extremist from continuing the dangerous activity. Through such proactivity, Facebook could save many lives.

I am well aware of the problems of my proposal. Liberals might rightly be worried that any program written to detect a string of words indicative of terrorism might be hugely overinclusive, capturing academic writing that quotes jihadists, satirical pieces that mock radical Islamists, serious literary works that feature a terrorist character, and, of course, radical political speech that calls for revolution (say, Marx's *The Communist Manifesto*).

In a piece of writing, the presence of certain words alone does not tell the whole story. One needs to see words in context to determine whether or not they amount to incitement to commit violence. Present available software cannot reliably understand the text it screens; only a person can do that. It might be the case that the sheer volume of suspicious content picked up by the software will be unmanageable. The volume could very well prove overwhelming for even a large team of scrutineers. However, as is evident from Milner's argument, Facebook is reluctant to commit to the struggle against online terror and other social ills (such as cyberbullying). If internet intermediaries are willing to start actively monitoring content, they could no longer claim simply to be carriers. The loss of "carrier" status or the artifice of being a carrier would potentially open them to liability for content and inevitable lawsuits. Thus, their current insistence on passivity. I presume that if and when they see the need for such monitoring, they will recognize the public utility that stems from a successful struggle against the perils of terror. Innovative technology will become a reality and there will be less need for human agents.

Web_site/RESEARCH/Islamic_Jihad.pdf [https://perma.cc/W5GJ-DLTJ]. "Jihad al-kufar" (struggle against the infidel) and "jihad al-munafikin" (struggle against hypocrites) are distinctly militant and coercive. *See id.* at 5. They are concerned with the struggle to build a good Muslim society, which may involve the right and the duty to check upon fellow Muslims and to bring them back into line when necessary. *See id.*; *Jihad*, BBC (Mar. 8, 2009), http://www.bbc.co.uk/religion/religions/islam/beliefs/jihad_1.shtml [https://perma.cc/F86U-67BK].

[65] Milner Interview, *supra* note 37.

The chilling effect is certainly a concern.[66] Monitoring requires resources and not all are willing to dedicate those resources.[67] Several publishers have closed down their comment sections.[68] They grew weary of all the nasty trolling and the savage commentary from the readers.[69] This is certainly a price to pay but any option exacts a price. Each internet intermediary needs to decide its priorities. A balance needs to be struck between freedom of speech and providing avenues for abusing this freedom. And each internet intermediary needs to decide what resources it is willing to commit to promote a safe environment. When it comes to the dangers of terrorism, they should be willing to commit resources as the price of limitless tolerance could be exceedingly high.

Milner's analogy between Facebook and BT[70] made it clear that there is a wide gulf between those who wish to see internet intermediaries' proactivity and passive companies like Facebook. Surely Milner knows that Facebook is doing much more than BT does. To start, BT does not integrate video and audio platforms, and it does not run advertisements in the background while people speak. Indeed, BT's commercial model is very different from Facebook's and BT could only dream to have Facebook's reach. More than two billion people use Facebook every month.[71] Five hundred million Instagram users use the Facebook app each month.[72] It is estimated that Americans spend 20 percent of the total time spent on their cell phones using Facebook or Instagram.[73] Facebook enables advertisers to choose their audiences based on demographics, behaviors, or contact information.[74] Facebook advertisement formats are eye-catching, flexible, and work on every device and connection speed.[75] Milner's comparison to BT is most flattering to BT. But it is also misplaced; it is designed to ward off demands for proactivity and responsible conduct.

Indeed, the major internet companies and search engines are engaged in online profiling designed to target individual online conduct so as to direct them to relevant advertisements. Technology and social media companies serve the interests of big business.[76] Facebook invests in such profiling for

[66] *See Morris Hearings*, *supra* note 44, at 34; *see also Harris Hearings*, *supra* note 49, at 123.

[67] Justin Ellis, *What Happened After 7 News Sites Got Rid of Reader Comments*, NEIMANLAB (Sept. 16, 2015, 1:48 PM), http://www.niemanlab.org/2015/09/what-happened-after-7-news-sites-got-rid-of-reader-comments/ [https://perma.cc/3UW5-6BB8].

[68] *See id.*

[69] *See id.*

[70] *See supra* note 57 and accompanying text.

[71] *Facebook Ads*, FACEBOOK, https://www.facebook.com/business/products/ads [https://perma.cc/VQS3-RTJ7] (last visited Oct. 16, 2017).

[72] *Id.*

[73] *See id.*

[74] *See id.*

[75] *Id.*

[76] Paul Bernal, *Web Spies*, INDEX ON CENSORSHIP, June 2011, at 109 (noting that the technology and social media companies tracking online conduct do so for commercial purposes).

each of its more than one billion daily users.[77] Facebook members receive constant information about products and activities tailored to their interests. Given the size of this undertaking, it is clear that Facebook's failure to monitor is not a question of ability, but a question of will. Facebook invests in profitable activities and does not invest in unprofitable activities. With this attitude, Facebook fails to respect its own community standards, which state that "[w]e don't allow any organizations or individuals that are engaged in the following to have a presence on Facebook: Terrorist activity, or [o]rganized violent or criminal activity . . . ."[78] The standards go on to state:

> We also remove content that expresses support for groups that are involved in the violent or criminal behavior mentioned above. Supporting or praising leaders of those same organizations, or condoning their violent activities, is not allowed.
>
> We welcome broad discussion and social commentary on these general subjects, but ask that people show sensitivity towards victims of violence and discrimination.[79]

It is possible to influence Facebook from below. Facebook users have a voice. They have the power to influence policy and bring about change. Facebook is interested in growing its community, and thus Facebook has shown some willingness to listen to its members.[80] While CSR on its own is the right business model to adopt, pressure from users to change, accommodate, monitor, and censor can be effective in supplementing CSR.

III. SOCIAL RESPONSIBILITY ON THE INTERNET

When the free speech arguments fade out, we are left with one major consideration: the economy. Responsible conduct requires resources, and many internet intermediaries are reluctant to invest resources if it is neither profitable nor demanded of them. In this context, I wish to promote the concept of Corporate Social Responsibility (CSR).

The concept of CSR emerged during the 1950s from a recognition that adopting social responsibility norms could be beneficial for business.[81] "CSR is defined broadly to encompass the economic, legal, ethical and philanthropic expectations placed on businesses by society."[82] These

[77] *Company Info*, FACEBOOK, http://newsroom.fb.com/company-info/ [https://perma.cc/C5HN-C28V] (last visited Oct. 16, 2017). As of June 30, 2017, Facebook has over two billion monthly active users. *Id.*

[78] *Community Standards: Dangerous Organizations*, FACEBOOK, https://www.facebook.com/communitystandards#dangerousorganizations [https://perma.cc/VNP9-LKZY] (last visited Oct. 16, 2017).

[79] *Id.*

[80] *See* Monika Bickert & Brian Fishman, *Hard Questions: How We Counter Terrorism*, FACEBOOK (June 15, 2017), https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/ [https://perma.cc/X2JF-LGM7].

[81] GABRIEL ABEND, THE MORAL BACKGROUND: AN INQUIRY INTO THE HISTORY OF BUSINESS ETHICS 332–33 (2014); Archie B. Carroll, *Corporate Social Responsibility: Evolution of a Definitional Construct*, 38 BUS. & SOC'Y 268, 269–70 (1999).

[82] Archie B. Carroll, *Corporate Social Responsibility (CSR) Is on a Sustainable Trajectory*, J. DEF. MGMT., Dec. 2015, at 1.

expectations include recognition that business integrity and ethical conduct go beyond mere compliance with laws and regulations. Businesses are expected not only to be responsive to the letter of the law but also to the "spirit" of the law and social and ethical norms underlying them.[83]

The arguments for CSR are strong. CSR ensures a company's long-term viability.[84] Responsible planning, including anticipating and initiating policies, is more practical and less costly than reacting to social problems.[85] Furthermore, ethical practice enhances the firm's reputation and marketing and wards off government regulation.[86] A business can forestall government intervention if it applies responsible standards and fulfills society's expectations.[87] However, to successfully implement CSR, a company must take into account CSR's core principles, which

> dictate (a) integrated, sustainable decision making that takes into consideration the positive and negative potential consequences of decisions; (b) obligation on the part of corporations not only to consider different stakeholders . . . and interests but also to incorporate them into the decision-making processes; (c) transparency, which is vital for ensuring accountability; (d) consistent respect for societal and environmental ground rules . . . ; (e) precautionary steps to be taken before implementing agreed-upon decisions; (f) liability for decisions and enactment of remedial measures to redress harm inflicted as a result of conduct; and (g) investment in the community to benefit the public good.[88]

Social responsibility is needed because internet intermediaries have become major actors in shaping the informational environment and in influencing users' experiences and interactions within it.[89] Internet intermediaries provide open infrastructure and applications that facilitate digital expression, interaction, and the communication of information.[90] A survey of the literature regarding internet intermediaries' responsibilities reveals that three topics are salient in the debate: (1) the organization and management of access to information, (2) censorship and freedom of speech, and (3) users' privacy.[91] This survey reflected on internet intermediaries' gatekeeping role, arguing that because gatekeeping "impacts both users'

[83] Archie B. Carroll, *Carroll's Pyramid of CSR: Taking Another Look*, INT'L J. CORP. SOC. RESP., July 2016, at 3; *see also* BRYAN HORRIGAN, CORPORATE SOCIAL RESPONSIBILITY IN THE 21ST CENTURY: DEBATES, MODELS AND PRACTICES ACROSS GOVERNMENT, LAW AND BUSINESS vi (2010); THE OXFORD HANDBOOK OF BUSINESS ETHICS 289 (George G. Brenkert & Tom L. Beauchamp eds., 2010).

[84] Archie B. Carroll & Kareem M. Shabana, *The Business Case for Corporate Social Responsibility: A Review of Concepts, Research and Practice*, 12 INT'L J. MGMT. REVIEWS 85, 88–89 (2010).

[85] *Id.* at 89.

[86] *See id.*

[87] *See id.*

[88] COHEN-ALMAGOR, *supra* note 18, at 149; *see also* Stefan Tengblad & Claes Ohlsson, *The Framing of Corporate Social Responsibility and the Globalization of National Business Systems: A Longitudinal Case Study*, 93 J. BUS. ETHICS 653, 653–57 (2010).

[89] Mariarosaria Taddeo & Luciano Floridi, *The Debate on the Moral Responsibilities of Online Service Providers*, 22 SCI. & ENGINEERING ETHICS 1575, 1576 (2016).

[90] *See id.*

[91] *Id.* at 1579.

access to information and the dynamics of the informational environment, any ethical framework that defines such principles should account for the rights of both users and the environment."[92] The survey emphasize the concepts of "care" and "respect," the flourishing of the environment as a function of its diversity, and the responsibility of human agents to care for the design and management of the informational environment to ensure its well-being as fundamental ethical principles that may guide internet intermediaries' conduct.[93]

Two bones of contention are (1) whether internet intermediaries have any moral responsibilities beyond the professional responsibility to carry and disseminate information, and (2) whether internet intermediaries should monitor and filter the content circulating on their platforms to prevent the dissemination of harmful material. I answer both questions in the affirmative. These questions relate to technological abilities and the expectations we may have regarding the conduct of internet gatekeepers. In *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway*, I argue that internet intermediaries should proactively combat antisocial and violent content.[94] Those who control access to the information highway have certain gatekeeping responsibilities. They should assume an obligation as trustees of the public good. Internet intermediaries cannot be neutral towards antisocial and violent content. Absolute content net neutrality constitutes inexcusable, irresponsible conduct. Terrorism and its relationship to crime are among the prime troubling antisocial and violent activities that have significant presence on the internet.[95]

As for ability, it is a contested issue among laypersons whether it is technologically possible to monitor websites, especially very large and voluminous websites with heavy traffic. The issue is far less contested among experts. Marc Rotenberg, president of the Electronic Privacy Information Center, said that the capability to monitor the internet is greater than most people assume.[96] It is a question of will, not of ability.[97] Edward Snowden's revelations about the National Security Agency (NSA) surveillance program opened our eyes to the growing technological capabilities and the rapid expansion of security surveillance over the past decade.[98]

[92] *Id.* at 1597.

[93] *Id.* at 1598; *see also* Mariarosaria Taddeo & Luciano Floridi, *The Moral Responsibilities of Online Service Providers*, *in* THE RESPONSIBILITIES OF ONLINE SERVICE PROVIDERS 13, 34 (Mariarosaria Taddeo & Luciano Floridi eds., 2017).

[94] COHEN-ALMAGOR, *supra* note 18, at 224–27.

[95] *Id.* at 311–12. In my book I also discuss terrorist manuals and learning tools that are also aimed to instigate violence. *Id.* at 184–86.

[96] Interview with Marc Rotenberg, President of the Elec. Privacy Info. Ctr., in Washington, D.C. (May 2, 2008).

[97] *Id.*

[98] *See* *Citizenfour*, IMDB, http://www.imdb.com/title/tt4044364/ [https://perma.cc/P8MZ-SK9Q] (last visited Oct. 16, 2017); *see also* Ewan Macaskill & Gabriel Dance, *NSA Files: Decoded*, GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [https://perma.cc/F54K-R8X9].

Companies and programs that patrol online content have recently emerged. Companies like Check Point Enterprise, Symantec Gateway Security, Allot, and Packeteer provide traffic management facilities and security management tools. David Corchia founded Concileo, a company "which develops and manages community and participatory strategies by providing community platforms forums and internal teams for moderating user content submitted to its clients' user participation areas."[99] Concileo's clients include major French newspapers and magazines, such as *Figaro* and *Elle*.[100] Corchia's team of thirty people monitors some 100,000 text-based media a day.[101] Further, "[n]ational security organizations have developed mechanisms to scrutinize large parts of the Internet susceptible to criminal activity."[102] The University of Florida created ICARUS, a software tool "that monitors traffic over its network, identifies traffic that appears to be characteristic of peer-to-peer file sharing, and then suspends network service to the computer generating the traffic for 30 minutes. Users may regain network access only if they complete a 10-minute interactive presentation on copyright law."[103]

Microsoft created a system to help monitor and track down online child pornography.[104] YouTube, Facebook, and other companies use this system, known as PhotoDNA, to find and delete child pornography.[105] PhotoDNA is an image-matching technology designed to help find, report, and eliminate images of child pornography.[106] "PhotoDNA enables the creation of a unique digital signature of an image which can then be used to compare against signatures of other photos to find copies of the same image."[107] Similar methods are used to take down copyrighted material.

Based on the existence of these companies and programs, it is possible to monitor traffic on large websites.[108] It is a question of allocating resources for monitoring.[109] Presently, many internet intermediaries are reluctant to commit resources unless they are pressured to do so.[110] They relieve

[99] COHEN-ALMAGOR, *supra* note 18, at 226.

[100] *Id.*

[101] Discussion with David Corchia, Chief Exec. Officer of Concileo, in Paris, Fr. (Oct. 10, 2011).

[102] COHEN-ALMAGOR, *supra* note 18, at 226.

[103] Eric Evans, Note, *From the Cluetrain to the Panopticon: ISP Activity Characterization and Control of Internet Communications*, 10 MICH. TELECOMM. & TECH. L. REV. 445, 498 (2004).

[104] Yaakov Lappin, *Police Arrest Internet Pedophile Ring*, JERUSALEM POST (Jan. 21, 2009, 8:36 PM), http://www.jpost.com/Israel/Police-arrest-Internet-pedophile-ring [https://perma.cc/97WK-3F6H].

[105] Olivia Solon, *Facebook, Twitter, Google and Microsoft Team Up to Tackle Extremist Content*, GUARDIAN (Dec. 5, 2016, 8:47 PM), https://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content [https://perma.cc/CTS8-28R9].

[106] *Microsoft PhotoDNA*, MICROSOFT, https://news.microsoft.com/download/presskits/photodna/docs/photoDNAFS.pdf [https://perma.cc/FH9N-95DB] (last visited Oct. 16, 2017).

[107] *Id.*

[108] *See* COHEN-ALMAGOR, *supra* note 18, at 226.

[109] *See id.*

[110] *See id.* at 227.

themselves of responsibility to combat antisocial and violent speech to the best of their abilities.[111] Most internet intermediaries shy away from assuming such responsibility as it is the easier and more profitable path to pursue.[112]

Consider the case of Anwar al-Awlaki, one of the iconic figures of modern terrorism. The American Yemeni cleric was the leading English-speaking propagandist for Al Qaeda who was also embraced by the Islamic State.[113] An American drone strike killed al-Awlaki in 2011 because of his operational and leadership roles with Al Qaeda and for plotting attacks intended to kill Americans.[114] However, his influence endures beyond the grave.[115] His presence on the internet is immortal.

Strikingly, YouTube hosts the largest collection of al-Awlaki's lectures and speeches. On January 18, 2015, I conducted a simple YouTube search for "Anwar al-Awlaki." My search produced 68,400 results, which included many of his lectures. I repeated this same search on January 5, 2017. This time, the search yielded 68,000 results. In 2015, some of the titles at the top search were *Battle of the Hearts and Minds*; *Islam Judgment Day*; *Never Trust a Non-Muslim*; *Death: The Hereafter Series*; *The Grave*; and *Allah Is Preparing for Victory*. In 2017, some of the titles were *Persevere and Endure, The Uniqueness of the Shaheed*, *The Resurrection Day of Judgment*, and *Islam Judgment Day*. Anwar al-Awlaki's videos have proved to be very influential in inciting terror.[116]

In 2015, Democratic presidential candidate Hillary Clinton urged the government to work with internet intermediaries to shut down jihadist websites and chat rooms.[117] Some security experts called on YouTube to ban videos of lectures by al-Awlaki.[118] These videos helped radicalize some very dangerous jihadists, including the terrorist Nidal Hasan from Fort Hood in Texas, who murdered thirteen people and wounded thirty-two others in a 2009 shooting rampage;[119] Roshonara Choudhry, a twenty-one-year-old student who stabbed Member of Parliament Stephen Timms in May 2010 for

[111] *Id.*

[112] *Id.*

[113] Scott Shane, *The Enduring Influence of Anwar al-Awlaki in the Age of the Islamic State*, CTC SENTINEL, July 2016, at 15, https://ctc.usma.edu/v2/wp-content/uploads/2016/08/CTC-SENTINEL_Vol9Iss713.pdf [https://perma.cc/7BW5-FGUE].

[114] *See id.*

[115] *See id.*; *see also* SCOTT SHANE, OBJECTIVE TROY: A TERRORIST, A PRESIDENT, AND THE RISE OF THE DRONE 291–92 (2016).

[116] For discussion on YouTube's evident refusal to remove al-Awlaki's videos, see Alexander Tsesis, *Terrorist Speech on Social Media*, 70 VAND. L. REV. 651, 661–62 (2017).

[117] *See* Erick Eckholm, *ISIS Influence on Web Prompts Second Thoughts on First Amendment*, N.Y. TIMES (Dec. 27, 2015), https://www.nytimes.com/2015/12/28/us/isis-influence-on-web-prompts-second-thoughts-on-first-amendment.html [https://perma.cc/KX25-XQ9U].

[118] *Id.*

[119] Billy Kenber, *Nidal Hasan Sentenced to Death for Fort Hood Shooting Rampage*, WASH. POST (Aug. 28, 2013), https://www.washingtonpost.com/world/national-security/nidal-hasan-sentenced-to-death-for-fort-hood-shooting-rampage/2013/08/28/aad28de2-0ffa-11e3-bdf6-e4fc677d94a1_story.html [https://perma.cc/K373-QQHF].

supporting the Iraq War;[120] the Boston Marathon bombers;[121] the San Bernardino terrorists;[122] the terrorists who aimed to kill people who attended the "Draw Muhammad" cartoon contest in Garland, Texas;[123] Mohammad Youssef Abdulazeez, who murdered four U.S. Marines in attacks on two facilities in Tennessee in July 2015;[124] and Omar Mateen, who murdered forty-nine people and wounded fifty-three others in a June 2016 mass shooting at Pulse nightclub in Orlando.[125] Several other plots featured young men who watched and identified with al-Awlaki online, after his death.[126] In the face of such evidence showing the influence of online videos, some American law professors expressed agreement with Clinton. As Professor Eric Posner wrote, "Never before in our history have enemies outside the United States been able to propagate genuinely dangerous ideas on American territory in such an effective way."[127] Posner suggested enacting a law that would make

> it a crime to access websites that glorify, express support for, or provide encouragement for ISIS or support recruitment by ISIS; to distribute links to those websites or videos, images, or text taken from those websites; or

[120] Vikram Dodd & Alexandra Topping, *Roshonara Choudhry Jailed for Life over MP Attack*, GUARDIAN (Nov. 3, 2010, 7:18 AM), https://www.theguardian.com/uk/2010/nov/03/roshonara-choudhry-jailed-life-attack [https://perma.cc/4WYC-9EX9].

[121] On April 15, 2013, Dzhokhar Tsarnaev and his brother Tamerlan Tsarnaev detonated two bombs near the finish line of the Boston Marathon, which killed three spectators and wounded more than 260 others. *Boston Marathon Bombings*, HISTORY, http://www.history.com/topics/boston-marathon-bombings [https://perma.cc/GY8G-J3TW] (last visited Oct. 16, 2017).

[122] On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik killed fourteen and wounded twenty-two at Farook's office holiday party before being killed themselves in a shootout with police. *Everything We Know About the San Bernardino Terror Attack Investigation So Far*, L.A. TIMES (Dec. 14, 2015, 4:03 PM), http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html [https://perma.cc/6KZN-YWWP].

[123] On May 3, 2015, Elton Simpson and Nadir Soofi opened fire at the entrance to an exhibit featuring controversial cartoons of the Muslim Prophet Mohammed. Catherine Shoichet & Michael Pearson, *Garland, Texas, Shooting Suspect Linked Himself to ISIS in Tweets*, CNN (May 5, 2015, 2:55 AM), http://edition.cnn.com/2015/05/04/us/garland-mohammed-drawing-contest-shooting/ [https://perma.cc/4FYC-TSRJ].

[124] Jamiles Lartey & Agencies, *Four U.S. Marines and Gunman Killed in 'Act of Terrorism' in Tennessee*, GUARDIAN (July 16, 2015, 6:02 PM), http://www.theguardian.com/us-news/2015/jul/16/chattanooga-tennessee-active-shooter-navy-reserve-center [https://perma.cc/JF8C-9K52].

[125] Ralph Ellis et al., *Orlando Shooting: 49 Killed, Shooter Pledged ISIS Allegiance*, CNN (June 13, 2016, 3:05 PM), http://edition.cnn.com/2016/06/12/us/orlando-nightclub-shooting/ [https://perma.cc/G4GT-NVVS].

[126] *See, e.g.*, Tsesis, *supra* note 116, at 661–62; Liz Goodwin, *San Bernardino Attacks Latest Example of Anwar al-Awlaki's Deadly Legacy*, YAHOO! (Dec. 23, 2015), https://www.yahoo.com/politics/san-bernardino-attacks-latest-example-1327003987255350.html [https://perma.cc/NZ4H-KHKG]; Robert Windrem, *Dead Cleric Anwar al-Awlaki Still Sways Terror Wannabes*, NBC NEWS (July 25, 2015, 5:53 AM), http://www.nbcnews.com/news/us-news/dead-cleric-anwar-al-awlaki-still-sways-terror-wannabes-n397506 [https://perma.cc/GP2Y-5RHW].

[127] Eric Posner, *ISIS Gives Us No Choice but to Consider Limits on Speech*, SLATE (Dec. 15, 2015, 5:37 PM), http://www.slate.com/articles/news_and_politics/view_from_chicago/2015/12/isis_s_online_radicalization_efforts_present_an_unprecedented_danger.2.html [https://perma.cc/HSG5-HTQU].

> to encourage people to access such websites by supplying them with links or instructions.[128]

Posner supports urging Facebook, YouTube, and other social networking sites to crack down on terrorist propaganda.[129]

Likewise, Mark D. Wallace, chief executive of the advocacy group Counter Extremism Project called on YouTube and other platforms to permanently ban all of al-Awlaki's material, saying that it should be censored in the same way that child pornography is censored.[130]

Anwar al-Awlaki was a frequent contributor to *Inspire* magazine, an English-language jihadist magazine published by Al Qaeda in the Arabian Peninsula.[131] The magazine, known for its high production standards, inspires jihadists, provides instructions for how to mount terrorist attacks, and encourages people to carry out attacks where they live.[132] It attempts to target traditionally adversarial populations, such as Muslims who live in the West.[133] In 2015, the fourteenth issue of *Inspire* was published focusing on lone-wolf operations in the West, including the attack on Charlie Hebdo's office in Paris[134] and attempting to capitalize on the current racial unrest in the United States by calling on African Americans to embrace Islam and kill "racist politicians."[135] The fifteenth issue of *Inspire*, published in 2016, reiterated the call for lone-wolf operations;[136] provided instructions for how to make parcel bombs, magnetic car bombs, and door trap bombs;[137] and warned about a knife revolution heading towards America as part of the Jihadi holy war.[138] The sixteenth issue of *Inspire*, published later in 2016,

[128] *Id.*

[129] *See id.*

[130] *See* Scott Shane, *Internet Firms Urged to Limit Work of Anwar al-Awlaki*, N.Y. TIMES (Dec. 18, 2015), http://www.nytimes.com/2015/12/19/us/politics/internet-firms-urged-to-limit-work-of-anwar-al-awlaki.html [https://perma.cc/LD7U-57VD].

[131] *See* Cohen-Almagor, *supra* note 8, at 6.

[132] *See id.*

[133] *See id.*

[134] *See* Ibrahim Ibn Hassan al-Asiri, *Charlie Hebdo: Military Analysis*, INSPIRE, Summer 2015, at 38–51, https://azelin.files.wordpress.com/2015/09/inspire-magazine-14.pdf [https://perma.cc/86LN-823M]; *see also* Raphael Cohen-Almagor, *The Charlie Hebdo Affair: Between Speech & Terror*, CRITIQUE (Jan. 7, 2016), http://www.thecritique.com/articles/the-great-war-series-part-ii-charlie-hebdo-free-speech-religious-violence/ [https://perma.cc/QWA8-LDGS].

[135] *See* Abdillah al-Moravid, *The Blacks in America*, INSPIRE, Summer 2015, at 23, https://azelin.files.wordpress.com/2015/09/inspire-magazine-14.pdf [https://perma.cc/86LN-823M].

[136] *See* Sheikh Nasser al-Anisi, *Lone Jihad Between Strategy and Tactic*, INSPIRE, Spring 2016, at 42–45, https://azelin.files.wordpress.com/2016/05/inspire-magazine-15.pdf [https://perma.cc/DWX8-TUZ3].

[137] *See Home Assassinations: Parcel Bomb, Magnetic Car Bomb, Door Trap Bomb*, INSPIRE, Spring 2016, at 74–89, https://azelin.files.wordpress.com/2016/05/inspire-magazine-15.pdf [https://perma.cc/DWX8-TUZ3].

[138] *See* Abu 'Awadh, *O Knife Revolution, Head Towards America*, INSPIRE, Spring 2016, at 36–41, https://azelin.files.wordpress.com/2016/05/inspire-magazine-15.pdf [https://perma.cc/DWX8-TUZ3].

contained rules for dealing with civilians in lone-wolf terrorist operations[139] and a message to "Muslim brothers" in America.[140] It also explained how to prepare pressure-cooker bombs.[141] The terror-inciting magazine is widely available on multiple websites and Google locates it quickly.

I opened this Article with the fictitious story about John who took a stool to the street, stood on it, and began calling to kill soldiers. *Inspire* repeatedly calls on people to kill innocent civilians. Anwar al-Awlaki told jihadists in his videos to kill not only soldiers but any American: "Don't consult with anybody in killing the Americans, fighting the devil doesn't require consultation or prayers seeking divine guidance. They are the party of the devils."[142] Following the Fort Hood shootings in 2009,[143] al-Awlaki wrote a post headlined "Nidal Hassan Did the Right Thing," in which he argued:

> Nidal Hassan is a hero. He is a man of conscience who could not bear living the contradiction of being a Muslim and serving in an army that is fighting against his own people. This is a contradiction that many Muslims brush aside and just pretend that it doesn't exist.[144]

I have mentioned Microsoft PhotoDNA.[145] Hany Farid, a professor of computer science at Dartmouth who helped develop PhotoDNA, explained that it is not difficult to design software to find images of al-Awlaki or samples of specific audio or video footage: "It's not a technical problem, . . . [i]t's a policy issue. I think the speech and privacy issues are tricky. But to say there's nothing we can do about it is cowardice.'"[146] It is also unreservedly irresponsible.

YouTube has community guidelines, one of which concerns violent or graphic content.[147] It says:

> It's not okay to post violent or gory content that's primarily intended to be shocking, sensational, or disrespectful. If posting graphic content in a news or documentary context, please be mindful to provide enough information to help people understand what's going on in the video. Don't encourage others to commit specific acts of violence.[148]

[139] Shaikh Hammed al-Tameemi, *Rulings of Lone Jihad*, INSPIRE, Autumn 2016, at 28–33, https://azelin.files.wordpress.com/2016/11/inspire-magazine-16.pdf [https://perma.cc/B983-BQ5M].

[140] Abd Allah Al-Murabit, *A Message to Our Muslim Brothers in America*, INSPIRE, Autumn 2016, at 36–39, https://azelin.files.wordpress.com/2016/11/inspire-magazine-16.pdf [https://perma.cc/B983-BQ5M].

[141] *See The Successful Pressure Cooker Bomb*, INSPIRE, Autumn 2016, at 10–11, https://azelin.files.wordpress.com/2016/11/inspire-magazine-16.pdf [https://perma.cc/B983-BQ5M].

[142] Robert Mackey, *Anwar al-Awlaki in His Own Words*, GUARDIAN (Sept. 30, 2011, 12:32 PM), https://www.theguardian.com/world/2011/sep/30/anwar-al-awlaki-video-blogs [https://perma.cc/ZL9F-6LX8].

[143] *See supra* note 119 and accompanying text.

[144] Mackey, *supra* note 142.

[145] *See supra* notes 104–08 and accompanying text.

[146] Shane, *supra* note 130.

[147] *Community Guidelines*, YOUTUBE, http://www.youtube.com/yt/policyandsafety/communityguidelines.html [https://perma.cc/5USG-3B6E] (last visited Oct. 16, 2017).

[148] *Id.*

Based on the continued presence of al-Awlaki's videos on YouTube, it is clear that YouTube is not enforcing this standard. Having community guidelines and not enforcing them is a sham.

Lauren Weinstein, cofounder of People for Internet Responsibility, noted that the ISIS recruitment videos are

> colorful, fast-paced, energetic, and incredibly professional . . . state of the art 21st century propaganda aimed at young people. By contrast, Western videos that attempt to push back against these groups seem more on the level of the boring health education slide shows we were shown in class back when I was in elementary school.[149]

Weinstein advocates fighting effective propaganda with no-less-effective counterpropaganda.[150] She acknowledges that YouTube runs "a variety of increasingly sophisticated automated systems to scan for various content potentially violating their [Terms of Service]," but these systems do not provide a bulletproof solution as "a great deal of material slips through and can stay online for long periods."[151] Instead of calling for government interference or regulation, Weinstein suggests that YouTube install a visible abuse-reporting button to enable internet users to quickly report problematic material and that YouTube use volunteers or paid officers to report abuse.[152]

While Weinstein's suggestions have merit, some of her basic assumptions are misinformed. Sixty-eight thousand pieces of information about Anwar al-Awlaki cannot be described as material that simply "slips through." It suggests clear negligence. YouTube's managers do not think it is their business to be proactive in taking down this material. Even if we consider the possibility that YouTube takes down video clips and then terrorist organizations immediately upload clips to replace the removed data, YouTube has the technological tools to filter its server far more effectively than it currently does. Again, it is first and foremost a question of will, not of ability.[153]

I can think of a situation in which a jihadi man is radicalized via the internet after watching al-Awlaki YouTube videos. That person will commit a terrorist attack, murdering a few innocent people who were in the wrong place, at the wrong time, until he surrenders himself. In the police interrogation he reveals the radicalization process he underwent after watching al-Awlaki video clips. When this information is subsequently publicized, families of the victims sue YouTube for reckless conduct. It would be an agonizing ordeal for all concerned.

To avoid this scenario, direct calls for violence, calls for recruiting fighters for jihad, and activities designed to fund raise terror should be censored. This does not mean that true facts of people being killed, humiliated, and tortured,

[149] Lauren Weinstein, *A Proposal for Dealing with Terrorist Videos on the Internet*, LAUREN WEINSTEIN'S BLOG (Dec. 21, 2015), http://lauren.vortex.com/archive/001139.html [https://perma.cc/P3VV-HRBL].

[150] *See id.*

[151] *Id.*

[152] *Id.*

[153] *See supra* notes 97, 109 and accompanying text.

or images of innocent victims of bombings—which cause moral outrage in potential perpetrators, who decide they have to do something about it—should be censored. Certainly, true images of the horrors of Syrian President Bashar al-Assad's barrel bombings should not be censored as if they never happened. Marc Sageman advised in his comments that quite a few people who volunteered to fight for the cause of jihad did so because they identified with an endangered community and wished to defend this community.[154] Sageman was involved in some of the American cases either as an investigator or expert witness and had access to all of the discovery material, not just the second-hand, sensationalized press accounts.[155] Sageman stresses the importance of continued discourse over the internet with these outraged people.[156] He thinks that true facts showing the destruction of Muslim targets contribute more to political violence through identification of the recipient than through straight advocacy of violence. He sees no problem in censoring the latter.[157] He argues that we need to establish clear and transparent conditions that would assure that political and corporate agencies would not overstep and trample on free speech rights.[158] Eternal vigilance is in part the responsibility of democratic citizenry.[159]

IV. TOWARD GREATER RESPONSIBILITY

The internet is a very new phenomenon. In historical terms, it is an infant. The internet entered into most people's lives when it started its commercial phase during the early 1990s.[160] We are in the early stages of learning how to make the most of this wonderful innovation, exhausting its massive potential for our benefit while erecting defense mechanisms against potential abusers who wish to exploit the internet for antisocial and harmful activities. We are in the process of finding a balance between freedom of expression and a no-less-important competing interest: social responsibility.

Since 2015, Twitter has used partial automation of "proprietary spam-fighting tools" to identify accounts that may promote terrorism.[161] The alleged terrorism-promoting material must be reviewed before the accounts can be disabled.[162] Sinead McSweeney, Twitter's vice president of public policy, said that since mid-2015, Twitter has suspended more than 360,000

[154] Comments by Marc Sageman, Senior Fellow, Foreign Policy Research Inst., Ctr. for the Study of Terrorism (Mar. 6, 2017).

[155] *Id.*

[156] *Id.*

[157] *See id.*

[158] *See id.*

[159] *See id.*

[160] *See, e.g.*, KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET 243 (1998); Raphael Cohen-Almagor, *Internet History*, INT'L J. TECHNOETHICS, Apr.–June 2011, at 52–53; Barry M. Leiner et al., *The Past and Future History of the Internet*, COMM. ACM, Feb. 1997, at 107–08.

[161] Associated Press, *Tech Companies Move to Target Terrorist Propaganda Online*, DAILY MAIL (Dec. 6, 2016, 3:31 AM), http://www.dailymail.co.uk/wires/ap/article-4004554/Tech-companies-target-terrorist-propaganda-online.html [https://perma.cc/Z72Y-S5RR].

[162] *See id.*

accounts for violating Twitter's policy on violent threats and promoting terrorism.[163] "The company said it has expanded the teams that review reports around the clock, adding new tools to help detect suspicious accounts and hiring people fluent in different languages."[164] Facebook has also taken steps to combat violent and terroristic material. It uses "image-matching technology to compare images to ones it's already removed. The effort lets Facebook review images to avoid removing legitimate and protected uses, such as a photograph published by a news organization."[165] At the same time, these major internet intermediaries repeatedly voice their commitment to protecting "users' privacy and their ability to express themselves freely and safely."[166]

A recent report claims that "Facebook, Google, and Twitter are working more aggressively to combat online propaganda and recruiting by Islamic militants while trying to avoid the perception they are helping the authorities police the Web."[167] In December 2016, a new program created by Facebook, Microsoft, Twitter, and YouTube was announced, which would help to automatically identify videos or images the companies should remove by using a "database of unique digital fingerprints."[168] In a joint statement, the four companies pledged to share among themselves "the most extreme and egregious terrorist images and videos [they] have removed from [their] services—content most likely to violate all [their] respective companies' content policies."[169] When such content is identified by one of the companies, it immediately notifies the other companies and together they can remove violent content that violates their rules.[170] In response, the White House stated that "the innovative private sector is uniquely positioned to help limit terrorist recruitment and radicalization online."[171]

On June 26, 2017, the same companies announced the establishment of the Global Internet Forum to Counter Terrorism.[172] This initiative "adds

[163] *Id.*

[164] Ellen Nakashima, *Twitter Says It Shut Down More Than 235,000 Accounts Promoting Terrorism Since February*, WASH. POST (Aug. 18, 2016), https://www.washingtonpost.com/world/national-security/twitter-says-it-shut-down-more-than-235000-accounts-promoting-terrorism-since-february/2016/08/18/7fc5b7b4-653d-11e6-96c0-37533479f3f5_story.html [https://perma.cc/PXF3-YZVP].

[165] Associated Press, *supra* note 161.

[166] Mike Isaac, *Facebook and Other Tech Companies Seek to Curb Flow of Terrorist Content*, N.Y. TIMES (Dec. 5, 2016), http://www.nytimes.com/2016/12/05/technology/facebook-and-other-tech-companies-seek-to-curb-flow-of-terrorist-content.html [https://perma.cc/KGL8-KJN5].

[167] Tova Cohen, *Israel Eyes Law to Remove Online Content Inciting Terrorism*, REUTERS (June 22, 2016, 7:15 AM), http://www.reuters.com/article/us-israel-security-socialmedia-idUSKCN0Z8174 [https://perma.cc/JQP4-6ZEH].

[168] *See* Associated Press, *supra* note 161.

[169] *Id.*

[170] *Id.*

[171] *Id.*

[172] John Mannes, *Facebook, Microsoft, YouTube and Twitter Form Global Internet Forum to Counter Terrorism*, TECHCRUNCH (June 26, 2017), https://techcrunch.com/2017/06/26/facebook-microsoft-youtube-and-twitter-form-global-internet-forum-to-counter-terrorism [https://perma.cc/VM4F-994B].

structure to existing efforts by the companies to target and remove from major web platforms recruiting materials for terror groups."[173] Together, the companies' "leaders say they will collaborate on engineering solutions to the problem, sharing content classification techniques and effective reporting methods for users."[174] In addition, each company will contribute to technical and policy research and will share best practices for counterspeech initiatives.[175]

In Europe, in recent years, there has been a trend toward imposing increased responsibility on internet intermediaries for hosting illicit materials.[176] One relevant case is *L'Oréal SA v. eBay International AG*.[177] The case concerned the sale of L'Oréal products on eBay without L'Oréal's consent.[178] The Court ruled that the duty on eBay and similar entities is much more onerous than was generally thought and that negligent omission short of active participation can be the basis of liability.[179] The case established that internet intermediaries may incur liability for unlawful activities of which a diligent economic operator would have been aware.

The landmark European Court of Human Rights judgment in *Delfi AS v. Estonia*[180] is similarly important because the court held that the online news portal was responsible for defamatory posts on its server.[181] The applicant, Delfi AS, was a public limited company registered in Estonia that owned one of the largest internet news sites in the country.[182] In January 2006, Delfi published an article on its webpage about a ferry company's decision to change the route its ferries took to certain islands.[183] This had dire consequences for passengers who had to pay more for using the ferries.[184] Beneath the article, readers were able to leave comments and many of them wrote highly offensive or threatening posts about the ferry operator and its owner.[185] The owner sued Delfi and successfully obtained a judgment against it.[186] The Estonian court found that the comments were defamatory and that Delfi was responsible for them.[187] The owner of the ferry company

[173] *Id.*

[174] *Id.*

[175] *Id.*

[176] Stephanos Stavros notes in his comments on a draft of this paper that the French authorities were at a certain stage quite active in closing down extremist sites. Comments by Stephanos Stavros, Head of the Office of the Council of Europe Sec'y Gen.'s Special Representative on Migration & Refugees (Mar. 13, 2017). Finland has adopted legislation criminalizing (under certain conditions) the act of knowingly hosting hate speech. *Id.*

[177] L'Oréal SA v. eBay Int'l AG, Case C-324/09 (E.C.J. July 12, 2011), http://curia.europa.eu/juris/liste.jsf?num=C-324/09 [https://perma.cc/QHC5-YWG8].

[178] *Id.*

[179] *Id.*

[180] Delfi AS v. Estonia, 64569/09 Eur. Ct. H.R. (2013), http://hudoc.echr.coe.int/eng?i=001-126635 [https://perma.cc/2CBZ-YTUK].

[181] *Id.* at 6.

[182] *Id.* at 2.

[183] *Id.* at 3.

[184] *Id.* at 29.

[185] *Id.* at 3–5.

[186] *Id.* at 6.

[187] *Id.*

was awarded the equivalent of around €320 in damages.[188] An appeal by Delfi was dismissed by the Supreme Court of Estonia.[189] Delfi then appealed to the European Court of Human Rights.[190]

On appeal, the court held that the finding of liability by the Estonian courts was a justified and proportionate restriction on the portal's right to freedom of expression because the comments were highly offensive, and the portal failed to prevent them from becoming public, profited from their existence, and allowed their authors to remain anonymous.[191] The court further held that the fine imposed by the Estonian courts was not excessive.[192]

Internet news portals make significant revenues from advertisements that are directly linked to comments of internet users.[193] The *Delfi* decision will require them to reconsider central aspects of the way they conduct their business to avoid onerous moderating duties if they wish to avoid incurring liability for defamation.[194] Countries that perceive incitement to terror as a serious concern may expect and demand internet intermediaries to filter their services of such content.

In March 2017, Heiko Maas, Germany's minister of justice and consumer protection, announced his intention to propose a law that would require social media platforms to make it easy for users to report contentious material and impose stiff fines on internet intermediaries whose social media platforms did not respond swiftly to complaints about illegal content.[195] Mr. Maas added that he wishes to increase the pressure on social networks: "This will set binding standards for how companies running social networks must handle complaints and require them to delete criminal content."[196] The law would oblige internet companies to delete or block criminal content within twenty-four hours after having been alerted to the illegal content.[197] Once the law is approved, internet intermediaries may face fines of up to €50 million for not combating terrorist material and hate speech, "potentially the highest such penalty in the Western world."[198]

Also in March 2017, following the terrorist attack of Khalid Masood (a.k.a. "Adrian Ajao") near the Palace of Westminster in which four people died and more than thirty-five others were injured, United Kingdom Home Secretary Amber Rudd vowed to "'call time' on internet firms that give terrorists 'a

[188] *Id.*
[189] *Id.*
[190] *Id.* at 1.
[191] *Id.* at 32.
[192] *Id.*
[193] Hugh J. McCarthy, *Is the Writing on the Wall for Internet Intermediaries?*, 14 HIBERNIAN L.J. 16, 45 (2015).
[194] *See id.*; *see also* Peggy Valcke, Alexandra Kuczerawy & Pieter-Jan Ombelet, *Did the Romans Get It Right? What Delfi, Google, eBay and UPC TeleKabel Wien Have in Common*, *in* THE RESPONSIBILITIES OF ONLINE SERVICE PROVIDERS, *supra* note 93, at 101, 104–07.
[195] Melissa Eddy & Mark Scott, *Facebook and Twitter Could Face Fines in Germany over Hate Speech Posts*, N.Y. TIMES (Mar. 14, 2017), https://www.nytimes.com/2017/03/14/technology/germany-hate-speech-facebook-tech.html [https://perma.cc/XTX7-E9EV].
[196] *Id.*
[197] *Id.*
[198] *Id.*

place to hide' as it emerged that security services are powerless to access" WhatsApp communications.[199] WhatsApp, an instant messaging service owned by Facebook, uses end-to-end encryption that prevents even its own technicians from reading people's messages.[200] Khalid Masood communicated via WhatsApp just minutes prior to his attack.[201] Rudd said that the government is considering legislation to force online firms to take down extremist material and emphasized that it was time for the companies to "'recognise that they have a responsibility' to get their own house in order."[202] Foreign Secretary Boris Johnson said he was "furious" about and disgusted by the failure of internet companies to block extremist material.[203] He further stated that internet companies "need to stop just making money out of prurient violent material."[204] Craig Mackey, acting chief commissioner of London's Metropolitan Police Service, said that these incidents should be a "wake-up call" for the internet industry.[205] "If you are going to have an ethical statement and talk about operating in an ethical way," said Mackey, "it actually has to mean something. That is the sort of thing that obviously politicians and others will push now."[206] The Metropolitan Police Service has a specialized team that spends most of its time working to remove extremist content, but it cannot access all material.[207]

In June 2017, the United Kingdom and France announced that they intend to "launch a joint campaign to push internet companies like Facebook and Google to do more to remove terrorist material."[208] British Prime Minister Theresa May said "the Internet must not be 'a safe space' for extremists."[209] She and French President Emmanuel Macron said they intend to "look at proposals to fine social media firms if they fail to take down such content."[210] May and Macron agreed that those firms must do more "and abide by their social responsibility to step up their efforts to remove harmful content."[211] The joint United Kingdom-France campaign "will explore options for

[199] Gordon Rayner, *WhatsApp Accused of Giving Terrorists 'a Secret Place to Hide' as It Refuses to Hand over London Attacker's Messages*, TELEGRAPH (Mar. 27, 2017, 1:54 PM), http://www.telegraph.co.uk/news/2017/03/26/home-secretary-amber-rudd-whatsapp-gives-terrorists-place-hide/ [https://perma.cc/C34C-W77S].

[200] *Id.*

[201] *See id.*

[202] *Id.*

[203] *Id.*

[204] *Id.*

[205] Ben Chapman, *London Terror Attack Shows Tech Firms 'Must Get Their House in Order' Says UK's Top Police Officer Craig Mackey*, INDEPENDENT (Mar. 29, 2017, 1:28 PM), http://www.independent.co.uk/news/business/news/london-terror-attack-facebook-google-wake-up-call-tech-companies-acting-met-police-commissioner-a7656131.html [https://perma.cc/U288-L2SP].

[206] *Id.*

[207] *See id.*

[208] *UK and France to Work Together to Tackle Online Extremism*, BBC (June 13, 2017), http://www.bbc.com/news/uk-politics-40258799 [https://perma.cc/2SHG-MB8K].

[209] *Id.*

[210] *Id.*

[211] *Id.*

creating 'a legal liability' which would allow companies to be punished if they fail to take steps to remove terrorist content."[212]

Israel has been suffering from terrorism more than any other country in the Western world. Time and again, its leaders complain that terrorism has been fueled by incitement on social media sites.[213] In 2016, Justice Minister Ayelet Shaked and Public Security Minister Gilad Erdan said that while the cooperation between Facebook and the Israeli government was bad, recently it had substantially improved.[214] Facebook leaders have finally realized that it must combat online incitement to terrorism and, together with Israel, will devise teams to determine how best to monitor and remove inflammatory content.[215] Facebook released a statement saying: "Online extremism can only be tackled with a strong partnership between policymakers, civil society, academia and companies, and this is true in Israel and around the world."[216]

In January 2017, Hamas launched a social media campaign commemorating the twenty-first anniversary of the assassination of Yahya Ayyash with the slogan "Be like Ayyash."[217] Ayyash, known as "The Engineer," was the chief bomb maker for Hamas and the leader of the West Bank battalion of the Izz ad-Din al-Qassam Brigades.[218] His bombs were used in a number of Hamas suicide attacks that resulted in a total of four hundred thirty-nine casualties.[219] Ayyash's very active terrorist career came to an end in 1996 when he was assassinated by Israeli forces.[220] Facebook regarded the 2017 Hamas celebration of Ayyash's destructive achievements as incitement to murder and shut down a total of ninety pages "belonging to Hamas or sites sympathetic to the group, as well as another [thirty] personal pages belonging to individuals."[221] The same month, the Israeli Knesset passed in its first reading a new bill that would allow the government to seek court orders to force Facebook to remove certain content based on police recommendations.[222] The bill, tabled by Public Security Minister Erdan and

[212] *Id.*

[213] *See* Times of Israel Staff & Associated Press, *Shaked: 'Penny Has Dropped' for Facebook on Incitement*, TIMES ISRAEL (Sept. 12, 2016, 8:41 PM), http://www.timesofisrael.com/shaked-penny-has-dropped-for-facebook-on-incitement/ [https://perma.cc/7GYT-XJU7].

[214] *See id.*

[215] *See id.*

[216] *Id.*

[217] *See* Bassam Tawil, *Palestinians: Glorifying Mass Murderers*, GATESTONE INST. (Jan. 10, 2017, 5:00 AM), https://www.gatestoneinstitute.org/9743/palestinians-glorifying-murderers [https://perma.cc/B5HL-9Q7E].

[218] *See Yahya Abd-al-Latif Ayyash—The Engineer*, ISR. DEF. FORCES BLOG (Jan. 21, 2012), https://www.idfblog.com/hamas/2012/01/21/yahya-abd-al-latif-ayyash-2/ [https://perma.cc/RPF3-S7TS].

[219] *See id.*

[220] *See* Serge Schememann, *Killing of Bomb 'Engineer' Unites Palestinian Factions*, N.Y. TIMES (Jan. 10, 1996), http://www.nytimes.com/1996/01/10/world/killing-of-bomb-engineer-unites-palestinian-factions.html [https://perma.cc/8UGH-9DMU].

[221] *See* Dov Lieber, *Facebook Closes Over 100 Hamas-Linked Accounts, Angering Terror Group*, TIMES ISRAEL (Jan. 8, 2017, 5:19 PM), http://www.timesofisrael.com/facebook-closes-over-100-hamas-linked-accounts-angering-terror-group [https://perma.cc/8QJ6-TB7N].

[222] *See id.*

Justice Minister Shaked, is said to be invoked in cases of suspected incitement "where there is a real possibility that the material in question endangers the public or national security."[223]

Nevertheless, law enforcement and the courts are slow to respond to evil on the internet. Internet intermediaries are far more effective. According to Ivan Koedjikov, head of the action against terror department at the Council of Europe, while law enforcement orders took down dozens of what he terms "bad sites" and social network accounts, the private sector has taken down hundreds and thousands of such sites and accounts.[224] At present, self-regulation is far more efficient than government regulation in addressing the challenge.

CONCLUSION

The internet is ubiquitous, interactive, fast, and decentralized. The ease of access to the internet, its low cost and speed, its chaotic structure (or lack of structure), the anonymity it provides, and the international character of the World Wide Web furnish all kinds of individuals and organizations an easy and effective arena for their partisan interests. The internet contains some of the best products of humanity and some of the worst ones. It serves both positive and negative elements in society.

When people through their conduct participate in wrongdoing, they can be seen as complicit and morally liable for those wrongs. Any real understanding of collective action not only allows but demands individual responsibility.[225] It is morally wrong to assist others in their wrongdoing by permitting, aiding, and providing opportunities to terrorists to act in a way that is harmful to others. At present, professional gatekeepers facilitate the commission of terrorism by providing terrorists services that they would otherwise not have the capability to utilize. The principles of freedom of expression and internet freedom are poor excuses for such detrimental abuse.

The international community also has moral, social, and legal responsibilities to unite to combat terror. On this global concern there is a need for cross-country cooperation. More and more countries understand the need to cooperate in order to tackle internet abuse. Given the magnitude of online terrorism, lack of such coordination would constitute utterly irresponsible behavior.

In April 2017, the European Commission disseminated a draft policy paper saying that there is a

> high degree of variation in the approaches taken to removal of illegal content—be it incitement to terrorism, hate speech, child sexual abuse material, or infringements of intellectual property rights. Such divergences may be justified in some cases (e.g. for certain types of illegal content); but

[223] *Id.*

[224] Koedjikov Comments, *supra* note 5.

[225] CHRISTOPHER KUTZ, COMPLICITY: LAW AND ETHICS FOR A COLLECTIVE AGE 9, 144, 146 (2000).

> in other cases they reduce the effectiveness of the system (e.g. by delaying the removal of terrorist propaganda).[226]

The Commission said that "it may come forward with legislative and/or non-legislative instruments by the end of the year to address 'legal fragmentation and uncertainty related to the removal of illegal content by online platforms.'"[227]

Better cooperation is required between internet intermediaries and governments. Indeed, to have effective results in fighting highly dangerous phenomena such as terrorism, cooperation is vital. Businesses are expected and obligated to act responsibly in a way that would benefit their communities and avoid or minimize harm to their stakeholders.

Our task is to balance two important principles: freedom of expression and social responsibility. The forefathers of the internet envisioned creating a free highway—a public space where everyone could say what was on their minds. This wonderful innovation has backfired. The internet is open for use and abuse. We should provide for and promote responsible use but fight against those who abuse. Their abuse corrupts public space and has posed many challenges on all levels: individual, the community, the state, and the international community. We are in the early stages of learning how to cope with and combat abuse. We are slowly developing the necessary tools to enjoy innovation and freedom, while adopting safeguards and rules of responsible conduct.

There is a growing awareness of threats and of the need to provide security. Ignorance and complacence, whether circumstantial or normative, cannot serve as excuses. The role of gatekeeping should be clarified and defined. Facebook and other internet intermediaries are slowly realizing the scope and importance of their responsibilities. There is no power without responsibility. For years, Facebook, Google, Twitter, Yahoo!, and others thought otherwise, but, in fact, greater power requires greater responsibility.

These giant companies are at an important crossroads now, where they must decide if they are willing to continue financing and disseminating evil, or rather adopt standards of CSR, assuring that their platforms will no longer serve and promote clear antisocial activities. Freedom of speech does not mean freedom to abuse the internet to promote violence and terror.

While a great deal is dependent on how we use the internet, a great deal is also dependent on internet service providers, web-hosting companies, and search engines. Facebook and Google have more power than presidents and prime ministers. Power without responsibility is dangerous, corrosive, and undermines our well-being. The internet's way should not be harmful. The internet's way should be enlightening, innovative, entertaining, productive, voicing the best of humanity. To ensure this, boundaries should be introduced, antisocial and violent activities should be curbed, and safe

[226] Julia Fioretti, *EU Mulls Legislation in the Fight Against Online Hate Speech*, REUTERS (Apr. 22, 2017, 2:49 PM), http://www.reuters.com/article/us-eu-hatecrime-idUSKBN17O0M0 [https://perma.cc/WR4K-5ECA].

[227] *Id.*

environments should be established. This requires a combined effort of internet users, business, countries and the international community at large.