ISIS Online: U.S. Rights and Responsibilities

February 2017

COUNTER EXTREMISM PROJECT

COUNTER EXTREMISM PROJECT

ISIS ONLINE: U.S. RIGHTS AND RESPONSIBILITIES

Overview

ISIS is the most notable of the many extremist groups that have weaponized social media and messaging platforms—such as Twitter and Facebook—as well as encrypted messaging applications like Telegram and WhatsApp—to recruit, incite violence, and plot attacks.

Social media companies, meanwhile, have for years failed to either acknowledge the severity of the problem of online extremism or to incorporate preventive safeguards onto their platforms. Despite major public relations announcements from 2015 through 2017, U.S.-based companies continue to respond to terrorist recruitment and incitement on a case-by-case basis if at all, actions that do little to prevent systemic abuse of their platforms.

This approach stems primarily from a misalignment of incentives. These corporations are driven by a need to increase market share and profit, rather than the societal goals of public safety and security. Indeed, the companies have often been reluctant to take steps that would slow or stop the misuse of their platforms or terrorist propaganda and incitement. Moreover, these companies have used misleading arguments related to privacy and free speech as an excuse for their inaction.

Unfortunately, such arguments tend to mischaracterize the roles of privacy, free speech, and security in the digital age, precluding a clear and serious public debate. To be clear, removal of social media content is not a free speech issue—rather it is a Terms of Service issue. Companies routinely monitor and govern their own platforms and remove a wide range of speech—from pornography to political dissent—that they believe may have an impact on perception and/or profit.

For example, as ISIS began launching high-profile attacks in the West, Internet and social media companies were slowly compelled to reassess their policies regarding terrorist operations on their platforms. Following the November 2015 attacks in Paris—which killed 130 people, and wounded 350 more—it emerged that ISIS terrorists may have used private messaging applications such as Telegram and WhatsApp to plot attacks. Scrutiny of these companies and others increased following the attacks, compelling Telegram and Twitter to initiate modest policy changes and boast of large sweeps to remove ISIS accounts. Since then, however, ISIS operatives have repeatedly reemerged on these and other platforms.

Technology companies often justify their inaction in the face of widespread misuse of their services by citing free expression and/or privacy concerns. *ISIS Online: U.S. Rights and Responsibilities* seeks to analyze the validity of such claims as well as the relevance of free speech and privacy rights debates to the technology companies operations more generally. The report also analyses the conflicting incentives that have resulted in private sector inaction despite the danger that ISIS misuse of technology poses to the public. The report also relies on historical

examples to illustrate how issues being debated today in online and digital environments are by no means unprecedented. In many cases, past experiences can point the way toward reconciling U.S. rights with matters of national security.

Freedom of Speech, Obligations under the Law and Terms of Service

Free Speech VS. Terms of Service

Discussions about curbing ISIS's prevalence online are often met with appeals to the U.S. right to freedom of speech. These appeals, however, are often steered by a number of misguided beliefs, including the erroneous suggestion that the right to free speech means providing terrorists with easy access to private U.S. digital platforms.

This is not the case. Technology companies are almost exclusively for-profit businesses. As such their mandate is first and foremost to generate profits. Since websites and messaging applications are private spaces, companies have significant control over the kind of speech that is allowable. Usage rules—typically outlined in a company's Terms of Service—need not comport fully with rights enumerated in the First Amendment.

YouTube, for example, elects to remove pornographic content in the United States, even though most pornography is protected speech under the First Amendment to the U.S. Constitution. Twitter bans not only pornographic images, but "excessively violent media" in a user's profile image, header image, or background image, or content that threatens or promote violence, including threatening or promoting terrorism. Facebook does not allow users to "bully, intimidate or harass" or post content that is "hate speech" threatening, incites violence or contains "nudity or graphic or gratuitous violence." WhatsApp, a messaging application, forbids "material that is unlawful, obscene, defamatory, libelous, threatening, harassing, hateful, racially or ethnically offensive, or encourages conduct that would be considered a criminal offense." Clearly, assertions by technology corporations are oftentimes belied by company-specific policies concerning allowable content.

Obligations under the Law

Even though companies have significant control over the content they do and do not allow on their platforms they do not have free reign to protect illegal activity on their sites. Illegal terrorist activity (including speech) in the "virtual world" still constitutes prosecutable activity in the "real world."

For example, U.S. law proscribes granting terrorists "advice or assistance derived from scientific, technical or other specialized knowledge." The law comes after the USA PATRIOT Act's section 805(a)(2)(b), which broadened the definition of "material support" to criminalize the act of providing terrorists with "expert assistance or advice." There are even cases in which mere advocacy for terrorism is criminalized. In 2010, the Supreme Court's *Holder v. Humanitarian*

Law Project decision held that speech can be criminalized if it constitutes "advocacy performed in coordination with, or at the direction of, a foreign terrorist organization."

These illegal forms of activity can and have been prosecuted in the United States, even when the activity occurs through the private companies online. During the past few years, U.S. court documents have shown that ISIS operatives have engaged in a number of different kinds of illegal activity on Twitter,[1] WhatsApp,[2] and other platforms.

Case Study: Child Pornography

Indeed, private companies have worked with U.S. law enforcement for years to confront child pornography, a category of speech that remains unprotected under the U.S. First Amendment. There are many lessons that can be drawn from U.S. government-led as well as private-led efforts to eradicate child pornography on the Internet.

Beginning in 2004 and extending through 2008, U.S. law required Internet service providers to report any known cases of child pornography as soon as possible, under 42 U.S.C. § 13032. The law was repealed on a national basis in 2008, but at least 12 states continue to require technicians and Internet service providers to report child pornography if and when they find it. While Internet service providers are by and large protected from liability under U.S. law if found to be hosting child pornography, they can be court-ordered to share some information with the government. An Internet service provider can, for example, be court-ordered to release details on a customer who used the service to share pornographic images of children.

Many technology companies also actively work to remove child pornography from their sites by using hashing algorithms specifically developed to be able to quickly and effectively recognize known images previously deemed to violate child pornography laws. Google, Facebook, and MySpace are some of the companies that routinely discover and report cases of child pornography. Twitter has a stated policy of reporting content that promotes child sexual exploitation to the National Center for Missing & Exploited Children (NCMEC), removing the materials, and permanently suspending accounts that promote such content from its site.

CEP's unique eGLYPH technology, developed by the world's foremost hashing expert, Dr. Hany Farid in June 2016 to detect extremist images, video, and audio for removal from a company's platform may serve as a template for addressing terrorist activity online. CEP unveiled eGLYPH, requiring Internet service providers and websites to flag and report terrorist content in a way that is objective, transparent to the public, and effective could help prevent violent and horrific extremist content from being used to radicalize people to terrorist violence.

Privacy and Encryption: Law and Limitations

[1] U.S.-based ISIS supporters on Twitter have included Ali Shukri Amin, Jaelyn Young, and many others. For more, check out CEP's Global Extremist Registry.
[2] U.S.-based ISIS supporters who have used WhatsApp for their ISIS-related activity include Arafat Nagi, Mufid Elfgeeh, and Heather Elizabeth Coffman, among others. For more, check out CEP's Global Extremist Registry.

Notwithstanding the tacit right to privacy and anonymity provided under U.S. law, entities operating in the communication field, including modern telecommunications and Internet companies, have broadly cooperated with law enforcement. Such past cooperation between tech companies and the U.S. government can serve as a template for developing the necessary laws and policies to overcome the challenges of encryption.

Case Study: Communications Assistance for Law Enforcement Act (CALEA)

In October 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes." According to the Federal Communications Commission, the law requires telecommunications companies to modify "equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve."

Among other features, the law required companies to ensure that they could provide governments with the resources to intercept "wire and electronic communications" and obtain access to call-identifying information, pending a court order or other lawful authorization. The FCC explains that CALEA was enacted "[i]n response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance."

Although CALEA specifically applied to telecommunications companies, the purpose of the law was to address technological concerns that can foreseeably apply to messaging applications today. The law has subsequently been updated to ensure that newer technologies such as Internet access providers and providers of VoIP also comply with CALEA standards.

To date, the obligations set out by CALEA do not apply to private networks, cellphones, email, Web hosting, or domain name lookup services. Nonetheless, the impetus for the law—public safety—is relevant and consistent with the need to ensure that law enforcement, with legal authorization, has the ability to access new communications technologies such as encrypted applications. CALEA can and should serve as an example of how to achieve balance between privacy safeguards and the need for legitimate government access.

Privacy Norms

As law and technology evolve, so do social norms. Activities that once seemed entirely private—like banking—are now infused with safeguards to protect against crimes like money laundering and terrorism financing. The evolving U.S. approach to banking can serve as a template for how social norms can evolve in response to new societal challenges.

Case Study: U.S. Banking

Though banking was long considered a private affair, the 1970 Currency and Foreign Transactions Reporting Act or the "Bank Secrecy Act" shifted societal expectations. The law required U.S. financial institutions to assist government agencies in detecting and preventing money laundering, tax evasion, and other criminal activities by requiring banks to "maintain appropriate records and file certain reports involving currency transactions." In 2001, the USA PATRIOT Act required all appropriate elements of the financial services industry to report potential money laundering. The 2010 Foreign Account Tax Compliance Act (FATCA) further narrowed banking privacy, this time by requiring foreign financial institutions to report information on accounts held by U.S. taxpayers to the Internal Revenue Service (IRS).

Following the passage of the 1970 Bank Secrecy Act, banking conglomerates and civil liberties groups filed suit, challenging the Act's constitutionality. Ultimately, however, the U.S. Supreme Court upheld the Act, and public expectations have since adjusted accordingly. A 2011 poll by the Associated Press showed that a slight majority of respondents—55 percent—favored the U.S. government's analysis of financial transactions for safety-related purposes. The evolving U.S. treatment of the banking sector may serve as an example for encrypted messaging applications. Privacy expectations and governmental laws both evolved to meet emerging threats and law enforcement concerns. Encrypted messaging is yet another sector in which law and the private sector will need to work together in order to confront the threat of terrorism.

Company Responsibility and Perverse Incentives

It can be difficult to reconcile the needs of law enforcement and for-profit technology corporations when the objectives of each are not aligned.

For example, a primary role of the U.S. government is to protect its citizens. The primary goal of a business is to increase revenue and ultimately, profits. Today, privacy concerns have "created a market for products with ever-greater encryption" and as private companies work to position themselves as defenders of privacy and free speech in the eyes of the public, they are also seeking to secure their place in domestic and international markets. Through this lens, companies may be concerned that even good faith cooperation with U.S. law enforcement will hinder their ability to compete in the international market for private messaging.

Case Study: Swiss Banking

The evolution of security in international banking has, after many years, come to meet the standards set by the United States. When the United States modified privacy standards associated with banking in the U.S., a market for more private forms of banking did, indeed, emerge offshore. This was most notoriously the case in Switzerland, where a Swiss bank account carried connotations of wealth, prestige, and access to exceptional privacy.

However, in 2008—in the midst of the global financial crisis—the U.S. began to actively investigate and prosecute Swiss bankers. Swiss bank UBS settled with the U.S. Department of Justice in February 2009. This was particularly difficult since Swiss law had made it a criminal

offense for banks to reveal the name of an account holder (under article 47 of the 1934 Federal Act on Banks and Savings Banks). As a result, once UBS settled with the U.S. Justice Department, UBS and other banks facing prosecution then had to pressure Switzerland to agree to allow them to release data. Meanwhile, the Organization for Economic Cooperation and Development (OECD) threatened to blacklist Switzerland as a tax haven in March 2009. After years of protecting clients, Switzerland made an unprecedented move in August 2009, allowing banks to expose over 4,000 UBS clients.

Other banks followed suit. In January 2013, Switzerland's oldest bank Wegelin announced it would close after pleading guilty to aiding U.S. tax evasion and incurring millions of dollars (ultimately $74 million) in fines. In February 2013, Switzerland signed an agreement conforming to the U.S. FATCA law. In August 2013, Switzerland agreed to allow eligible banks to pay penalties and disclose account information on U.S. customers in order to avoid prosecution. Banks in other countries like Luxembourg—long considered a tax haven—were soon compelled to follow Switzerland's example. Following the Great Recession and resulting backlash against private banks, the OECD has repeatedly declared that "The Era of Bank Secrecy is Over."

The evolution of bank privacy norms both in the United States and abroad may carry meaningful implications for encrypted messaging applications. International norms towards privacy and encryption are by no means set in stone. Even countries and businesses that have built their reputations off of a reverence for privacy can be pushed through market and legal incentives to prioritize public safety and new international norms. The question is then a matter of time: will we wait for market incentives to correct the situation and risk countless lives in the meantime? Or will we address the threat posed by encryption head on?

Progress: Slow and Insufficient

As the threat from ISIS continues, messaging and social media companies have begun to change their public stance towards ISIS's online presence. For years, however, these changes in attitude have lagged far behind what is needed to ensure the safe and systematic elimination of extremist content online, content that clearly violates the stated Terms of Service of these companies. As CEP has long advocated, proactive efforts of technology companies to thwart child pornography can—and should—serve as an example of how to move forward to address the threat of online terrorist activity.

In December 2016, major technology companies Google, Microsoft, Twitter, and Facebook announced their decision to address the presence of extremist content on their platforms through hashing technology. With this announcement, the challenges have now evolved again, particularly in terms of ensuring that these companies follow through on their commitments to effectively identify and remove extremist content through a process that is as objective and transparent as possible. If successful, the challenge is then to incentivize other companies—including website service providers, encrypted messaging companies, and other relevant technology companies—to adopt similarly responsible practices and follow suit.

Telegram—encrypted messaging application

- **January 2015:** An ISIS sympathizer publishes a ranked list of secure messaging apps. On this list, Telegram ranks as one of the safest messaging applications for use by ISIS terrorists.
- **September 2015:** Telegram's CEO rejects responsibility for ISIS on its platform, asserting that "[t]he right for privacy is more important than our fear of bad things happening, like terrorism."
- **November 2015:** ISIS terrorists use Telegram to plot deadly Paris attacks, killing 130 and wounding hundreds more.
- **November 2015:** Following the attacks, the company tries to save face: "Our policy is simple: privacy is paramount. Public channels, however, have nothing to do with privacy. ISIS public channels will be blocked."

Telegram's official policy: "All Telegram chats and group chats are private amongst their participants. *We do not process any requests related to them*… While we do block terrorist (e.g. ISIS-related) [*public*] bots and channels, we will not block anybody who peacefully expresses alternative opinions [emphasis added]."

Twitter—social media company

- **November 2014:** In response to concerns about ISIS on Twitter, a spokesperson sidesteps any responsibility to take action, telling *Mother Jones* that "[o]ne man's terrorist is another man's freedom fighter."
- **November 2015:** Following the deadly ISIS attacks in Paris, Twitter announces it has shut down tens of thousands of ISIS-linked accounts in less than a week.
- **December 10, 2015:** British ISIS recruiter Sally Jones—sanctioned by the United Nations, the United States, and others for her role in recruiting to ISIS—reappears on Twitter under her usual alias, "UmmHussainBritāniya." Her account is live on Twitter for at least two weeks.
- **December 2016:** Twitter, Google, Facebook, and Microsoft announce their plans to use hashing technology to systematically remove extremist content from their platforms.

Twitter's official policy: "You may not make threats of violence or promote violence, including threatening or promoting terrorism."

Conclusion

Time and again, the United States has managed to reconcile constitutional rights and valued principles with the requisites of public safety. As ISIS continues to misuse private companies to further its violent agenda, it has proved useful to remember that this challenge is not unprecedented. Lessons drawn from the fights against online child pornography, terrorism financing, and money laundering can, and have already begun, to serve as blueprints for government and private sector action. Legislation used to ensure cooperation between the two sectors—such as we have seen in the precedents from CALEA and banking—may further this necessary effort while continuing to protect U.S. freedoms.

There is a growing imperative to effectively and seriously address extremist groups not only on the battlefield, but where they plots attacks and lure recruits: through social media, Internet sites, and encrypted messaging applications. We cannot afford to allow ISIS to target our allies—claiming 130 lives and wounding more than 300 in Paris in November 2015—using our very own technology.

Advocacy by governments and groups like the Counter Extremism Project has thankfully and finally shown signs of bearing fruit in this arena, as seen through the December 2016 announcement by Google, Microsoft, Twitter, and Facebook to apply hashing technology to the issue of extremist content. Now, the challenge remains to encourage that these and other major technology companies apply these algorithms in a manner that is objective, transparent and—most importantly—effective.