Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

COUNTERTERRORISM IS A PUBLIC FUNCTION: RESETTING THE BALANCE BETWEEN PUBLIC AND PRIVATE SECTORS IN PREVENTING TERRORIST USE OF THE INTERNET

This paper, part of the Legal Perspectives on Tech Series, was commissioned in conjunction with the Congressional Counterterrorism Caucus

ALEXANDER GUITTARD

SEPTEMBER 2019

About the Program on Extremism

The Program on Extremism at George Washington University provides analysis on issues related to violent and non-violent extremism. The Program spearheads innovative and thoughtful academic inquiry, producing empirical work that strengthens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions that resonate with policymakers, civic leaders, and the general public.

About the Author

Alexander Guittard leads US national security partnerships for M&C Saatchi, where he works with US national security and development agencies to develop advertising campaigns that advance US foreign policy around the world. He advises the US Government on the role of strategic communications in countering terrorism and disinformation. He developed strategic partnerships across the Middle East, Southeast Asia and sub-Saharan Africa to support clients that include the US Department of State, USAID, and the US Department of Defense.

He previously served as a US Foreign Service Officer and began his career as an Army officer. He served in US Embassy London as the counter-terrorism and asymmetric threats policy lead. He speaks Arabic, Persian and French, is a fellow at ISD and a Society Advisory Group board member for the British Council.

The opinions and characterizations in this piece are those of the author and do not necessarily represent those of his current or previous employers or the U.S. Government.

The views expressed in this paper are solely those of the author, and not necessarily those of the Program on Extremism or the George Washington University.

Introduction

In the closing scene of The Social Network, one of Mark Zuckerberg's lawyers marveled at Facebook's global expansion, asking "In Bosnia, they don't have roads, but they have Facebook?" While the statement (and much of the film) was factually incorrect, it captured the "move fast and break things" mentality of companies like Facebook as they revolutionized the way people around the world communicate. Despite its benefits, this revolutionary shift in communications has posed several public policy challenges, from election integrity to the erosion of local journalism to terrorism.[1] As someone who has worked in counterterrorism for nearly a decade, first in government and now from the private sector, I've seen this evolution firsthand.

To date, most efforts to deny terrorists the benefits of a free and open internet are voluntary and industry-led. These include the Global Internet Forum to Counter Terrorism and its Hash Sharing Consortium, the expansion of dedicated counterterrorism teams at Facebook and Google and the launch of initiatives such as YouTube Creators for Change.[2] These are positive and socially responsible initiatives that should be encouraged to grow.

However, the U.S. government – both its political leadership and its CT experts – should not take the convenient route of outsourcing difficult public policy issues to private companies. These issues should be addressed legislatively and in partnership with industry. Curbing terrorists' use of the internet begs important social questions about the limits of free speech, the definition of terrorism, and national sovereignty over the internet at a time when the U.S. public is increasingly skeptical of the ability of internet companies to act in the public interest.[3]

By examining similar experiences balancing security with technological advancement, CT policy makers will see that cooperation with the private sector is often contentious at first, with industry eschewing new regulation. This paper will examine three such cases: the restriction of radio in WWI, the introduction of counter-money laundering requirements on banks and the introduction of airline passenger screening. These cases show when the government acts within its Constitutional authorities to set clear expectations and work with industry in good faith, industry, government and the public benefit.

Setting Clear Expectations: Updating the Regulatory Environment

Both government and the private sector share the same goals in preventing terrorists from using the tools of an open society to harm its citizens. Despite often heated political rhetoric, most companies are responsible actors who work with authorities every day to prevent terrorists from communicating, transferring funds, recruiting or otherwise advancing their goals.

In my experience, however, governments and the private sector are not speaking about the same problems with the same vocabulary. Preventing terrorists, or indeed any criminal from benefitting from a company's services is generally a compliance issue managed by a legal team. No company could long operate in the United States without meeting these legal requirements.

The challenge facing governments and the tech sector is that many of the uses of the internet by terrorists today are in fact legal under U.S. law. Brian Fishman, a terrorism expert who leads Facebook's CT efforts, observed:

"Generally speaking, terrorists use the Internet in much the same way as other people," Fishman writes, describing a range of activities that includes audience development, brand control, secure communication, community maintenance, financing, and information collection and curation.[4]

What then is the obligation of a company or a government to stop bad actors from using technology for these purposes? Broadly, governments and citizens expect companies to prevent terrorists from using their platforms and services. Companies are often happy to comply, often voluntarily. For their part, companies want to avoid increased regulation and losing the trust of their customers. In general, companies prefer voluntary action to regulation, as it allows them to set the limits of their cooperation. This is all fine where it works, but the current balance sets unfair expectations for all parties and forestalls difficult public policy decisions about free speech and the role of social and digital media in public life.

Most governments do not have a strategy or modern legislation that addresses terrorist use of the internet across all the categories listed above. As a result, public-private CT cooperation varies significantly across issue and geography. Most social and digital media companies will readily comply with a U.S. subpoena for records of the communications of a suspected terrorist, though they may reject requests to alter their algorithms to reduce the frequency of terrorist content on their pages.

The debate over regulating content on social and digital media so far has hinged on the question of whether these sites are neutral platforms or publishers, which exercise editorial controls over content. Platforms are largely unregulated, while publishers could be subject to similar regulations as traditional media. The law that created this distinction, Section 230 of the Communications Decency Act, is over twenty years old and was designed to address problems of a very different internet. A UK Parliament committee examined this issue, concluding:

“Social media companies cannot hide behind the claim of being merely a ‘platform’, claiming that they are tech companies and have no role themselves in regulating the content of their sites. That is not the case; they continually change what is and is not seen on their sites, based on algorithms and human intervention. However, they are also significantly different from the traditional model of a ‘publisher’, which commissions, pays for, edits and takes responsibility for the content it disseminates.”[5]

The report called on the British government to adopt some form of regulation for social media companies. Nearly half of Americans agree.[6] Consequently, as concerns around data privacy, foreign political interference and violent extremism on social media persist, it is likely that public pressure will mount for some kind of formal regulatory framework.

U.S. lawmakers could begin this conversation by updating the twentieth century laws that form the basis for the media regulatory environment to set formal expectations for social and digital media companies around content that is not in the public interest. This would be a complex legal endeavor that would pose difficult constitutional questions but is not without precedent.

At the beginning of the last century, the radio presented several of the same challenges to the U.S. government as social media does today. The technology was disruptive and democratizing in that it made global communications available to the masses. Radio shrank the world and promised users the earliest signs of today's constantly connected life.

When the U.S. entered the First World War, the new technology vexed military and law enforcement authorities and fueled public panic. Media reports often exaggerated the threat that radio-enabled saboteurs and spies to the U.S. "U.S. Government and police experts were much surprised to find that the cabinet which was recently seized with Max Wax, a German Spy, was capable of receiving secret radio messages from Germany," warned one news story from 1917 that could have been republished with minor edits in 2017.[7] When the U.S. entered the war, Congress authorized the president to shut down or takeover all private radio stations.[8] This heavy handed intervention laid the foundation of a regulatory environment based on the idea that airwaves were public property to be managed by government agencies.

Governments today share some of the same impulses towards censorship and greater control of digital and social media on national security grounds.[9] While it is neither practical nor desirable for the government to regulate social media the same way it did radio in the early twentieth century, it is possible to develop a regulatory framework based on a similar principle that our most powerful media channels should act in the public's interest, including on national security.

A potential model could be found in the financial sector, where governments and banks have cooperated readily and openly on counter terrorism for several years. Broadly, the U.S. government does not monitor every financial transaction for compliance with anti-terrorist financing laws. (It may for intelligence purposes.[10]) Instead, it monitors some transactions, typically guided by a targeted legal authority, such as a warrant or subpoena. Compliance is self-enforced, with banks filing regular reports of possible illegal activity with the Treasury Department. Failure to report, or failure to detect illegal activity can lead to heavy fines or jail time.[11]

When this system was first introduced in 1970, it provoked strong objections from the banks, presaging today's concerns from social media companies that the government was violating the constitutional rights of its customers and imposing undue costly administrative requirements. The Supreme Court ultimately weighed in, ruling that Congress had the power to compel banks to self-police and that the cost burdens were reasonable. Writing for the court, Justice Rehnquist observed "The bank plaintiffs proceed from the premise that they are complete bystanders with respect to transactions involving drawers and drawees of their negotiable instruments. But such is hardly the case."[12] The same could be said of today's social and digital media companies.

In Europe, where laws governing free speech are generally less absolute than in the U.S., social media companies already operate under similar requirements. In Germany, Facebook proactively scans and removes white-nationalist and neo-Nazi content, which is illegal under German law.[13] In the U.S., however, social media companies are more hesitant to act on white nationalist content, as the boundary between acceptable political speech and support for far-right terrorism is open for debate.[14]

It is neither fair nor prudent for government and society to offload responsibility for a delicate public task, such as defining the limits of free speech, to private companies. The responsibility lies with governments, specifically legislatures, to define the public interests, set accordant expectations for industry. The rest of the U.S. media sector, primarily television, radio, and advertising, contends with a range of First Amendment-compliant regulations that are designed to promote the public interest and support national security. The same should be possible for social and digital media. While politicians may find it expedient to blame large technology companies, they should instead lead difficult public conversations about the limits of free speech and the shared responsibilities we have to our civic society.[15]

Investing in Security

In addition to providing a clearer regulatory environment, governments should also invest in meaningful approaches that can prevent terrorist use of the internet. In my experience, much of the effort in this space is funded by large technology companies through corporate social responsibility programs. This is due in part to limited government funds for countering terrorism and violent extremism programs.[16] These efforts are positive and should be continued. But letting companies decide how and where to focus the lion’s share of online CT efforts poses public policy challenges. What happens when the interests of the government and Silicon Valley differ?

Governments can begin to address this by investing in technology partnerships with smaller companies that provide contracted services to governments and civil society partners. When the interests of the public and private sectors conflict, such as when Apple refused to unlock a terrorist’s iPhone in 2016, investment in technological alternatives gives governments additional recourse.[17] The British government has adopted this approach fulsomely, investing £600,000 ($774,000) in independent technology that successfully detects terrorist content, something Silicon Valley had previously said was prohibitively expensive.[18] [19]

The cost of investing in technology that will protect American citizens from terrorist use of the internet should not be great, but it can be borne by industry. Another sector targeted by terrorists – airlines – also struggled with early attempts to share the CT burden with government. During the skyjacking era of the 1960s, airlines strongly resisted Congressional efforts to require security screening of passengers. In debates that echo those today, the (then-booming) airlines were concerned that any new regulation could hurt profit and considered the cost of hijacked aircraft negligible.[20]

It was not until a highjacked airline nearly crashed into a nuclear reactor in 1972 that the government successfully mandated security standards.[21] The industry grudgingly accepted, but demanded the government pay for the screening. Ultimately, a balance was struck. The government permitted the airlines to hire private security contractors, funded by ticket surcharges.[22] The practice continued until 9/11, when renewed concerns for passenger safety threatened the survival of the airlines and the government again intervened forcefully to regulate airline security.

Conclusion

Banks, airlines and radio might not seem the most adept analogues for today's social media companies, but these cases show us that finding the balance between embracing new technology and preventing its misuse by criminals and terrorists has often been a contentious process. This tension is a feature of the U.S. system, where private companies enjoy stronger constitutional protections and social and political influence that they do in more statist systems (as my European CT colleagues are wont to point out).

Counterterrorism is an essentially public function, administered under U.S. law by judicial authorities. It is not appropriate to expect private companies to conduct counterterrorism operations, such as intelligence gathering or countering propaganda, outside of this public system. It is also not in the public's interest to allow the most powerful companies to define terrorism, or how to set the limits for how terrorists should be able to use the internet.

U.S. counterterrorism authorities – including lawmakers – should work with industry to codify clear legal expectations for companies to prevent terrorist use of digital and social media, including revising Section 230 of the Communications Decency Act. The White House should provide a national strategy for preventing terrorist use of the internet within its National Strategy for Counterterrorism that includes government investment in tools and technology independent from the largest companies' corporate social responsibility initiatives. This challenge extends well beyond counterterrorism, however, and these efforts should be part of a wider political and social conversation about the role of the internet and digital and social media in American democracy.

References

[1] These public policy questions come as public trust in social media companies is eroding. Pew Research has studied this in greater depth: https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

[2] *Hard Questions: What Are We Doing to Stay Ahead of Terrorists?* By Facebook Newsroom, Nov. 8, 2018: https://newsroom.fb.com/news/2018/11/staying-ahead-of-terrorists/ ;*Meet the little-known group inside of Google that's fighting terrorists and trolls all across the web* by Julie Bort, Business Insider, Aug. 25, 2018: https://www.businessinsider.com/google-alphabet-jigsaw-terrorists-trolls-2018-8?r=US&IR=T; *Facebook, Google tell Congress they're fighting extremist content with counterpropaganda* by John Shinal, CNBC News, Jan. 17, 2018: https://www.cnbc.com/2018/01/17/facebook-google-tell-congress-how-theyre-fighting-extremist-content.html

[3] Pew Research found that only 9% of Americans were "very confident" that social media companies would protect their personal data.

[4] *Crossroads: Counter-terrorism and the Internet* by Brian Fishman for Texas National Security Review, April 2019: https://tnsr.org/2019/04/crossroads-counter-terrorism-and-the-internet/

[5] Disinformation and 'fake news': Interim Report by House of Commons Digital, Culture, Media and Sport Committee, Jul. 24, 2018: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

[6] When asked by the Harvard/Harris poll in October 2017, "Would you support or oppose regulating the targeting of news feeds, search engine results, or advertising based on political affiliation or political viewpoints on social media platforms?," nearly half of the respondents indicated they would: https://harvardharrispoll.com/wp-content/uploads/2017/11/HCAPS-October_Topline-Memo_with-banners_Registered-Voters-Social-Media.pdf

[7] *Remarkable Radio Outfit Built by German Spy* in Electrical Experimenter, May 2017: https://archive.org/details/electricalex519171918gern/page/110

[8] *House Joint Resolution 309*, 65th Congress, July 6, 1918: https://www.loc.gov/law/help/statutes-at-large/65th-congress/session-2/c65s2ch154.pdf

[9] Internationally, the UK government is a leading voice for international calls to curb terrorist content online. These efforts include relying on British intelligence officials, who seldom speak publicly, to issue public warnings to Silicon Valley. One such example: *MI5 chief Andrew Parker: Social media companies must reveal details of terror threats* by Tom Whitehead and Danny Boyle in The Telegraph, Sep. 17, 2015: https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11870917/Six-terror-attacks-foiled-in-year-as-MI5-head-warns-plots-at-three-decade-high.html

[10] *US government 'monitored bank transfers'* by Dave Lee, BBC, April 16, 2017: https://www.bbc.co.uk/news/technology-39606575

[11] HSBC Helped Terrorists, Iran, Mexican Drug Cartels Launder Money, Senate Report Says by Agustino Fontevecchia, Forbes, July 16, 2012: https://www.forbes.com/sites/afontevecchia/2012/07/16/hsbc-helped-terrorists-iran-mexican-drug-cartels-launder-money-senate-report-says/#304f6b635712

[12] *Opinion of the Court*, California Bankers Association v. Shultz, Secretary of the Treasury, 1973: http://cdn.loc.gov/service/ll/usrep/usrep416/usrep416021/usrep416021.pdf

[13] *Germany Acts to Tame Facebook, Learning From Its Own History of Hate* by Katrin Bennhold, New York Times, May 19: 2018: https://www.nytimes.com/2018/05/19/technology/facebook-deletion-center-germany.html

[14] *Report: Twitter hasn't aggressively filtered white nationalist content because it could affect GOP politicians* by Rashaan Ayesh, Axios, April 25, 2019:https://www.axios.com/if-twitter-aggressively-filtered-white-nationalist-content-gop-accounts-might-be-affected-4cdd1f91-719a-4505-934d-91a828080e82.html

[15] *Donald Trump on Apple: 'Who do they think they are?'* by Chris Matyszczyk, CNET, Feb. 17, 2016: https://www.cnet.com/news/trump-apple-iphone-san-bernardino-encryption-fbi-terrorist/

[16] *Trump Shut Programs to Counter Violent Extremism* by Peter Beinart, The Atlantic, Oct. 29, 2018: https://www.theatlantic.com/ideas/archive/2018/10/trump-shut-countering-violent-extremism-program/574237/

[17] *Inside Apple CEO Tim Cook's Fight With the FBI* by Lev Grossman, Time, Mar. 17, 2016: http://time.com/4262480/tim-cook-apple-fbi-2/

[18] *UK unveils extremism blocking tool by Dave Lee*, BBC, Feb. 13, 2018: https://www.bbc.co.uk/news/technology-43037899

[19] *Can We Finally Stop Terrorists From Exploiting Social Media?* by Kalev Leetaru, Forbes, Oct. 9, 2018: https://www.forbes.com/sites/kalevleetaru/2018/10/09/can-we-finally-stop-terrorists-from-exploiting-social-media/

[20] Airlines thought security would "scare the pants off people," invade passenger privacy, and disrupt airport operations, according to Brendan Koerner in *The Skies Belong to Us*, p. 47.

[21] The Skies Belong to Us, p. 208-10

[22] The Skies Belong to Us, p. 218