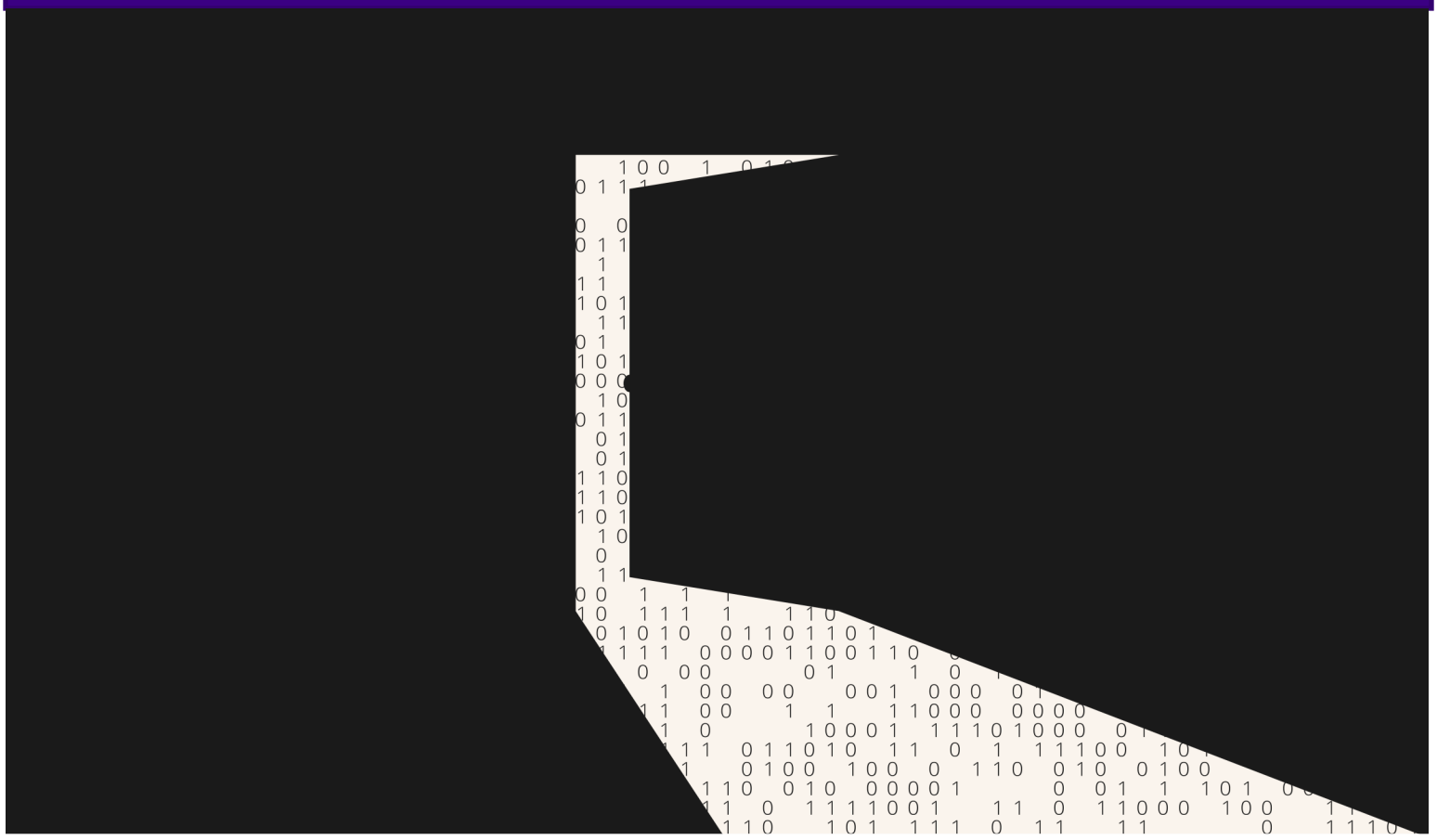
THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

TASK FORCE REPORT



Extremist Use of Social Media: Balancing Privacy and National Cybersecurity

2017

Henry M. Jackson School of International Studies
University of Washington, Seattle
Task Force Report Winter 2017

Extremist Use of Social Media:

Balancing Privacy and National Cybersecurity

Faculty Advisor
Dr. Jessica Beyer

Evaluator
Paul Nicholas
Senior Director, Global Security Strategy and Diplomacy, Microsoft

---

Editor
Phoibe Purcell

Coordinator
Xingyue Yang

Authors
Jane Birkeland
Jordan Johnson
Kristy Soo Jung Kwon
Serena Eunbich Ko
Taelim Leena Lee
Natalie Meek
Tae-Hyun Thomas Park
Cameron Rosenberg
Hannah Ross
Rajeev Stephens
Marielle Trumbauer
Priya Uppal
Julia Yoon

Table of Contents

Executive Summary

Social media is used by extremists, terrorists, activists, and ordinary people. The complexity of tackling extremist use of social media lies in balancing the privacy of civilians and US national security interests. Currently, there is a lack of comprehensive policy across industry and government to effectively manage extremist usage—providing a unique dilemma in dealing with extremist use patterns for online recruiting and communication efforts, while maintaining privacy and security for ordinary citizens.

We have sought to propose solutions to this dilemma through research of the following aspects of social media usage:

- Recruitment and communication efforts between extremists and citizens
- Private industry's efforts to balance between online security and privacy
- Existing constitutional rights, government policies, and organizations relevant to addressing extremist use of social media
- Civil society's role in keeping the government accountable for citizen rights in relation to cybersecurity-related policies

Through our research, we found an overall lack of coordination and communication between industry and government, which creates grey areas in current policy and law. The following recommendations have been made to effectively address extremist use of social media:

- Civil Society Interaction
    - Sponsor ad-campaigns that seek to raise awareness of extremist contact via social media and how to approach and report such situations
    - Begin the education of children and young adults, focusing on internet safety and online extremism
    - Create an official summit that includes industry and civil society to enhance cybersecurity discourse.
- Industry Interaction
    - Take into account what industry has already implemented when creating new policy

- Maintain that the removal of extremist accounts stays in the hands of industry
- Allow the legal collection of necessary information by the government and law enforcement if the person(s) in question present a clear and present danger

In this report, we will outline extremist use patterns of social media and explore the balance of civilian privacy with national security. We will then address existing government responses to extremist use patterns and end with civil society's role in keeping government accountable to the people it serves. We will lastly demonstrate that the afore summarized recommendations are the best way to effectively address extremist use patterns of social media for fundraising and communication efforts.

Introduction

Phoibe Purcell

Used by activists, governments, and ordinary citizens alike, the Internet has contributed to increased global interconnectedness; news, shopping, television, movies, family, and friends are now only clicks away—and with the rise of social media, communication and the sharing of thoughts and ideas has never been simpler. However, because the far reach of social media transcends physical borders, it has become the tool of choice for terrorist and extremist groups to recruit, communicate, and quickly spread information. Because there is a lack of unity in the terminology and policies aiming to address this issue, government and industry often clash when they are tasked with handling terrorist and extremist groups that wish to abuse these platforms.

Extremists have used Twitter, YouTube, and encrypted messaging applications to recruit new members, redirect vulnerable and unsuspecting users to extremist material, and to communicate and coordinate with one another. In addition, groups such as Black Lives Matter and the Alt-Right have been characterized as "extremist" and have also faced criticism for using social media to mobilize and communicate. Unfortunately, it has been difficult for private companies to figure out how to properly regulate this activity and cooperating with U.S. government has proven to be an additional challenge.

Now, with so many moving their lives online—sharing space with extremists and activists—security and privacy have become top priorities for both ordinary people and for private companies. As users of the Internet, we expect to have our personal details and private information protected from third parties—malicious or otherwise. Thus, the conflict often arises between government and industry when attempting to balance personal privacy and the matter of national security.

To address this problem, we researched extremist recruitment and communication efforts with ordinary citizens via the use of social media, in addition to the current efforts of private industry to balance online security and privacy with government requests for information. We then sought to clarify existing constitutional rights, government policies, and organizations relevant to addressing extremist use of social media, along with the role of civil society in keeping the government accountable for its cybersecurity-related policies.

Unfortunately, the issues of extremism, social media, and cybersecurity are multifaceted, and require more than one solution. We found a lack of comprehensive policy that addressed relations with private industry and the need for information in a format adapted for modern technology. To remedy this, we recommend encouraging the early education of children and young adults focusing on internet safety, in addition to the government sponsorship of an ad-campaign outlining online extremist behavior and ways to approach and report such instances. Subsequently, the government should look to the steps private industry has already taken when implementing their own cybersecurity policy, allowing the removal of user accounts to remain under the industry's discretion.

The government should then establish their own procedure for accessing and obtaining user data from private companies in the interests of national security if the persons in question present a clear and present danger or have close ties to someone who presents a clear and present danger. Any violations of this policy would be overseen by the judicial system, keeping checks and balances on government activity. In addition, the government should look to create an official trilateral summit that includes industry and civil society to enhance cybersecurity discourse. Working together, these groups should shape cybersecurity-related terms and policies from various perspectives.

With the continued widespread use of social media, it becomes increasingly important to have uniform policies and guidelines between government and industry that address the

treatment of extremism online. However, the security and privacy of ordinary citizens should not be compromised in the interest of maintaining national security. It then becomes the responsibility of the government to approach this problem with the cooperation of private industry and civil society, to keep the people's best interests in mind on a national and global scale.

Extremists and Social Media Use Patterns: Twitter, YouTube, and Encrypted Messaging

Jane Birkeland, Jordan Johnson, Kristy Soo Jung Kwon, and Marielle Trumbauer

The advent of social media has dramatically altered the way in which extremists communicate with their members, ordinary citizens, and the outside world. Throughout the past decade, YouTube and Twitter have seen a proliferation of usage by extremist groups such as Al Qaeda and ISIS to recruit, radicalize, and mobilize potential and active terrorists. For instance, from September to December 2014 alone, there were approximately 46,000 Twitter accounts affiliated with ISIS, with 1,000 followers each (Berger and Morgan, 2015b). Extremist manipulation of digital accounts allows them the opportunity to influence ordinary citizens—commanding and delegating tasks that support and glorify their organizations' objectives and aims.

Further, these platforms have given extremists a pedestal from which to openly promote their ideals, generate and advertise visual content, and abuse the use of algorithms in search engines or news feeds (Berger, 2015). Similarly, the popularity of encrypted messaging applications has increased potential for private messaging and the exchange of detailed instructions regarding attacks beyond the oversight of authorities or other unwanted parties (Stalinsky and Sosnow, 2015). After Edward Snowden's leaks of the US government's illicit surveillance of citizen's social media content, Al Qaeda increased its use of encrypted technology to carry out different communications (Stalinsky and Sosnow, 2015).

The widespread use of Twitter, YouTube, and encrypted messaging applications is of particular importance, in relation to marginalized populations that carry personal and political grievances toward its state (Hamm and Spajj, 2015). These groups have proven to be susceptible and vulnerable to influence by extremists, and their ideological appeal can

encourage individually-motivated "lone wolf" attacks (Hamm and Spajj, 2015). The use of social media by extremists is key in manipulating and converting ordinary citizens to serve the organization and its activities. Indeed, in 2015, approximately 3,000 Western nationals traveled to ISIS-dominated regions of Syria and Iraq to assist the extremist group in their operations of combat and promotion of propaganda (Blaker, 2015, 3). Holistically, the strategies employed by extremists have persuaded the minds and hearts of ordinary citizens in favor of advancing their interests and have contributed to fostering heightened trust, support, and participation in organizational goals and activities (Berger and Morgan, 2015). Therefore, extremist use of social media is problematic as it allows terrorists to attract ordinary citizen recruits to engage in acts of violence or future attacks, through extremist actors' ability to use social media accounts to generate and spread terrorist-related content, such as messages or visuals that spark individual interest or curiosity in support of the organization. The following sections will analyze extremist use patterns of platforms that have been utilized more frequently by these groups: Twitter, YouTube, and encrypted messaging applications. That is, Twitter and YouTube serve to attract ordinary citizens to their propaganda, while encrypted messaging works to directly message these individuals, and lock-in their values.

Extremists have used functions such as auto-play and trending hashtags to expose ordinary citizens to their messages, and correspondingly use encrypted messaging to further manipulate the emotions and thoughts of individuals to support their organization and secure loyalty. In response, we recommend that the government should sponsor ad-campaigns that outline how to indicate when someone is in communication with extremists via social media, and advise individuals on how to approach the situation to report such instances. Secondly, the government should invest in the early education of children and young adults, focusing on internet safety and how to recognize the signs of extremism online and in their peers.

Extremist use of social media platforms and messaging applications can be perceived as posing an inherent threat to national security.

Extremist Use Patterns on Twitter

The centrality of Twitter to modern extremism is a critical aspect in understanding its inclusion in this report. In the fourth quarter of 2016, Twitter had 320 million active users (Kerby, 2016). This makes it the third most popular platform globally, following Facebook and Instagram. A key part of these statistics is that 79% of Twitter's users are located outside of the United States, representing significant international involvement and use (Kerby, 2016). In 2013, Twitter had over 200 million users and 460,000 new accounts being created each day (Johnson, 2013). In 2016, one quarter of Internet users used Twitter, with 36% of people aged 18-29 using the platform (Greenwood et al.). The website, however, faces numerous challenges when it comes to account management and creation. For example, in 2013, 32% of Lady Gaga's followers were fake accounts, 35% were inactive, leaving 33% of followers considered "real" (Johnson, 2013). Fake accounts are an important consideration because they represent the ease with which users can cheat the system—an essential part of how terrorists use social media. The Anti-Defamation League identified Twitter as the most used platform for the dispersion of information by ISIS (Hashtag Terror, 2015). The evidence is clear—Twitter is one of the most quintessential platforms for the promotion of terrorism.

Twitter Use Patterns

In 2006, Jack Dorsey founded Twitter ("The History of Twitter", 2017). The initial intent was to allow users to update their friends on what was happening in their lives and "keep tabs on each other" through short status updates. Messages are limited to 140 characters and profiles can be either public or private. Users can send direct messages to others and can use hashtags to find related content.

Like other social media platforms, extremists leverage the pseudo-anonymity and ease of Twitter to target vulnerable individuals and convince them to adopt their ideology. With specific mention of Twitter, the International Association of Chiefs of Police outlines four key terrorist strategies: recruitment, radicalization, mobilization, and response (International Association of Chiefs of Police, 2014, 2). Recruitment is based on identifying users who have retweeted, favorite, followed, or commented on posts that were put out by fighters or associates of the specific terrorist organization. Radicalization involves "Issu[ing] statements and press releases, disseminating propaganda, and providing justification or encouragement for attacks" (International Association of Chiefs of Police, 2014, 2). Radicalization is two pronged: it can be to convince a target to, for example, move to Syria and fight with ISIS or it can be to convince a target to engage in domestic terrorism in the name of the organization, as seen in the San Bernardino case. Mobilization is about using the platform to organize and plot attacks in real time.

Response, the final strategy, ties the other steps together. Extremists can use Twitter to monitor emergency responses, spread misinformation, claim responsibility, and call for copycat attacks (International Association of Chiefs of Police, 2014, 2). An example of this strategy can be seen in the 2008 hotel bombings by Lashkar-e-Tayyiba in Mumbai. The Pakistani government specifically asked Twitter users to stop posting about the incident because perpetrators were also using the platform to track the movements of law enforcement (International Association of Chiefs of Police, 2014, 3). FBI Director James Comey described the entire process of recruitment, radicalization, mobilization, and response specifically by ISIS at the Aspen Institute in July 2015, saying,

> ISIL's M.O. is they broadcast on Twitter, get people to follow them, then move them to Twitter Direct Messaging while they evaluate whether they're a potential liaison either to travel or to kill where they are. Then they'll move them to an encrypted mobile-messaging app, so they go dark to us. (Bean, 2015)

Structural Challenges for Twitter: Pseudo-Anonymity

Twitter faces the challenge of shutting down and managing accounts that post or advocate for extremist content, but the ease with which terrorists can create new accounts has increased the size of the Twitter response team dramatically. Twitter has labeled their response team the "tweet threat team," and their main job is to identify and shut down these accounts (Bean, 2015). The specific challenges that come along with these suspensions is that extremist accounts can easily pop up again, such as @turjuman123 which was suspended 122 times (Bean, 2015). This has led to an increase in Twitter's daily suspension rate by 80% since 2015, a dramatic step up over the short period of just one year (Roberts, 2016). In 2016 alone, Twitter suspended 235,000 accounts for "threatening or promoting terrorist acts, primarily related to ISIS" (Twitter, 2016; The Camstoll Group, 2016, 2).

These suspensions bring up a critical characteristic of Twitter—pseudo-anonymity. This concept refers to the fact that the user is not completely anonymous, as they can be on certain posting boards where there is no user name. However, the name of the account on Twitter is the pseudonym being used and it does not have to be an accurate representation of the person behind the account. Extremists can easily create new email accounts and use fake identities to register. The only problem that they face is reestablishing their user/follower bases when their accounts are banned. This is affirmed by the Anti-Defamation League in their statement that, "Twitter users are also able to conceal their identities more effectively than on forums and other social networking sites. And while Twitter accounts can be—and indeed, sometimes are—shut down by Twitter, new ones can almost always be immediately established" (Anti-Defamation League, 2014). The leveraging of social media is a key part of modern terrorism and Twitter is the ideal platform with which to accomplish those goals due to the nature of the design.

Structural Challenges for Twitter: Shout-outs and Other Functions

On Twitter, the extremist account-holders facilitate the dissemination of content that is used to manipulate potential recruits into participating in attacks. The aforementioned issue has been compounded by the "shout-out": supporters or insiders of the terrorist entity that direct newly-discovered recruits to recently re-opened accounts (The George Washington University Program on Extremism, 2016; Vindino and Hughes, 2015, 24). Indeed, by the later-half of 2014, the work of shout-outs has culminated into building a network of more than 50,000 followers on Twitter (73% of whom belong to 4,500 accounts) from which ISIS could actively encourage to pursue organizational-building activities or recruit additional citizens (Liang, 2015, 5).

Essentially, the shout-outs play a significant role in increasing awareness of other available channels containing videos and images that promote a sense of approval and legitimacy in carrying out acts of violence and attacks on others. By steering users to the newly created accounts, the shout-outs contribute to the growing number of followers who can become directly contacted, informed, and influenced by the extremists. In this respect, terrorists can gain leverage over the aforementioned target group in shaping a strong desire and commitment to inflict harm and damage on behalf of the organization (Colraine, 2016). Further, extremists have strategically employed the use of technical codes or functions to successfully direct more people to their online networks, and sway their support for organizational plans and attacks (Berger, 2015). For one, the extremist entities use trending contemporary hashtags unassociated with extremism, including those referring to current events, such as #WorldCup, or recent topics, e.g.: #BlackLivesMatter (Brunson et al., 2016, 14; Friedman, 2014). In fact, ISIS uses its Twitter handle "@ActiveHashtags" to promote to its sympathizers trending hashtags that can be integrated within their messages (Milmo, 2014). Such usage of hashtags has contributed to the terrorists' ability to interact and obtain

an active response from ordinary citizens, as every tweet containing unrelated hashtags generated approximately seventy-two re-tweets of the initial content (Milmo, 2014). Similarly, 500 to 2,000 ISIS Twitter accounts, combined with the efforts of hundreds or thousands of ISIS sympathizers, spew out massive amounts of hashtags and other content in short lengths of time, applauding the organization's achievements in attack or killings (Berger, 2014; Berger and Morgan, 2015b).

Holistically, these methods allow the extremists to make their ideology visible to a wider audience. Moreover, such frequency in posts enables terrorists to not only become ranked higher on search engines (Berger, 2015), but also gain a level of prominence with citizens. That is, there is a point of entry in which the terrorists can shape how ordinary citizens may process certain information or conceptualize the published activities of the extremists. In that case, the terrorists' rapid spread of images, news, and other marketing material significantly contributes to the indoctrination and recruitment of ordinary citizens. Thus, these factors emphasize the challenges posed by the extremists' use of social media.

Content-based Strategies on Twitter

Terrorists have learned how to manipulate Twitter to advance their messages through the uploading of sensitive content. In particular, extremists upload images of graphic violence and killings of victims in order to further increase the legitimacy in battling and vanquishing their enemies (Klausen, 2015, 13). For instance, in August 2014, as a response to the American-led coalition's counter-airstrikes and bombing in Iraq, ISIS circulated pictures and videos of poles adorned with the decapitated heads of Westerners placed in several cities (Andrews and Schwartz, 2014). In an attempt to glorify the agility and force of their organization to civilians, one of ISIS's online posts included the comment:

> O Westerners, your governments have lost their minds, and they will let you pay the cost of their stupidity, the Islamic State is too strong, so you must yield to it. (Berger and Stern, 2015) (Anti-Defamation League, 2014)

The extremists' written and visual publications highlight the image of strength and dominance in combat against their enemies, or conquering other territories. That is, the published visuals on Twitter serve to not only showcase the achievements of the organization in its use of violence, but to also persuade external viewers toward victories of extremist-related efforts, in a way that enhances the level of attention or curiosity for the processes that shaped the successful outcome.

Social organizations or sports team mascots, such as the lion from the Detroit Lions team, are frequently used within Twitter posts to evoke a sense of familiarity and rationale with the organization (Vindino and Hughes, 2015, 23). ISIS sympathizers commonly use profile pictures that display the Detroit Lions logo, which emphasize the universal symbol of bravery in both American and jihadist culture (Smith, 2015). As such, the extremists' attempt to promote positive imagery of sacrificing one's life to serve the organization and physically engaging in its battles (Vindino and Hughes, 2015, 23). In other words, these entities allude to a sense of excitement, adventure, and solidarity that will result from fighting alongside fellow comrades in the battle against the adversary (Barrett, 2015, 17). Moreover, these tactics serve to conflate the similarities in objective of the terrorist organization and a recognized social group, and elevate a sense of trust and legitimacy within the potential recruit for the organization and its work. Hence, these tactics may deceive the individual into fostering a terrorist-related cause, without knowledge of the nefarious ends.

On a similar note, extremist recruits are often provided with salaries in exchange for active membership and engagement in combat within the terrorist organization (Liang, 2015, 3). That is, extremists are tactful in offering a source of steady income as an incentive for the individual to build a stable life working under the authority and protection of the entity. Such

rewards incentivize the potential recruit to have a stake in participating in terrorist-related attacks, and to continue supporting the organization's use of violence. Overall, the use of positive symbolism and financial motivators significantly factored in the exit of approximately 3,000 Western citizens to ISIS-dominated regions in Syria and Iraq in 2015—in order to assist the extremist group in their combat operations and promotion of propaganda (Blaker, 2015, 3).

Extremist Use Patterns on YouTube

YouTube, first developed in 2005, has become the primary website to upload, watch, and share personal and professionally made short videos with anyone with access to the Internet. While YouTube is host to harmless content such as family made vacation videos and makeup tutorials, it also can be taken advantage of and used for malicious purposes. One such misuse of YouTube includes the extensive posting and sharing of terrorist propaganda such as recruitment and hate speech videos.

YouTube averages around four billion video views every day (Mahmood, 2012). The site reaches more 18-49 year olds than any cable network in the United States, with 81% of United States millennials using YouTube, and users watching 46,000 years' worth of content annually (Smith, 2017). Any videos uploaded to YouTube with terrorist rhetoric have the potential to convert U.S. citizens to extremist views from the comfort of their own home. Essentially, one can find a recipe for salmon, as well as the leader of Boko Haram preaching to his following (Searcey, 2016) on the exact same website. Hence, this poses quite the challenge for both the leadership at YouTube and the U.S. government as well.

YouTube's Stance Regarding Extremist Use

Officially, YouTube has taken a stance that does not promote the uploading and sharing of extremist video content on its site. According to its Terms of Service, YouTube says the following under the sub-category of Content Related to Terrorism (YouTube, 2017):

> YouTube strictly prohibits content intended to recruit for terrorist organizations, incite violence, celebrate terrorist attacks or otherwise promote acts of terrorism. We also do not permit foreign terrorist organizations to use YouTube. Content intended to document events connected to terrorist acts or news reporting on terrorist activities may be allowed on the site with sufficient context and intent. However, graphic or controversial footage may be subject to age-restrictions or a warning screen.

While the rules remain relatively clear regarding YouTube's stance on terrorist content in the Terms of Service Agreement, users do not obey them. Whether it is small Islamic terrorist factions like the Turkistan Islamic Party (TIP) or more prominent terror groups like ISIS/ISIL, Al-Qaeda, or Boko Haram, one can find otherwise prohibited video content easier than ever before, all in one location.

While YouTube consistently tries to fix this growing issue, it also works against itself using its own algorithms. One such example is that of "autoplay," a feature on the site that, once the intended video is seen, automatically loads a related video for the consumer to watch with about five to ten seconds to opt out. The conclusion is that someone can begin watching a video they had no intention to if they are not quick enough to exit. While this creates great numbers for YouTube, it can also have dangerous side effects. An example of the dangers of autoplay in promoting terrorist content is that of U.S.-turned terrorist Anwar Al-Awlaki.

Case Study: Anwar Al-Awlaki

Anwar Al-Awlaki was an American-born terrorist who was also a renowned senior recruiter and motivator for Al-Qaeda. Though Al-Awlaki was killed in a drone strike in 2011, his videos live on through the power of the Internet and autoplay. It only takes four

"autoplayed" videos to get from a general Al-Awlaki speech to one featuring explicit anti-American preaching (Wallace, 2016). Autoplay also has a lengthy queue, so the tenth or twentieth video could be drastically different from the first. Al-Awlaki, though deceased, is not a threat to take lightly: a study completed in 2015 shows that approximately one quarter of Americans involved in Al-Qaeda or ISIS activity were "substantially influenced" by his teachings and sermons (Wallace, 2016). Al-Awlaki has over five thousand videos remaining on YouTube. He has been known to say such things to his followers such as, "Jihad today is obligatory on every capable Muslim," and "arms training is an essential part of preparation for Jihad" (The Telegraph, 2012).

Another algorithm that can be counterproductive is "autofill." Autofill, unlike autoplay, is seen all over the Internet. Autofill suggests things for a person to look for mid search, for example "Adele Rolling in the Deep" after typing "Adel." Though the online community has seen autofill everywhere from Google to Facebook to even text messages, predictive software can also suggest content that should not be advertised. Anwar Al-Awlaki videos quickly turn from his name to death videos (Wallace, 2016).

YouTube and the U.S.: Problems and Solutions

Although YouTube deleted 640 terrorist-related videos in 2012 (The Telegraph, 2012), extremist content continues to be uploaded constantly. However, the U.S. government has its fair share of problems too. One main issue that both parties share is the double-edged sword that is the right to free speech. Many terror groups use the First Amendment to justify initial use of American-based social networks, making YouTube the choice for video hosting. Jihadist channels emerged into the public spotlight after private forums were not reaching large enough audiences and have since become very flexible in dodging prosecution (Klausen et al., 2012). By posting links in the description box of less controversial videos, consumers

of content can be transported to a spot on the Internet that is less regulated and more dangerous.

The issue with YouTube is that it is unique. Other video sharing sites such as Vimeo do exist, but not in the same wide reaching capacity that YouTube does. Shutting down YouTube is not an option. Therefore, the challenge is how much control YouTube should have over its subscribers' content and then how much control the U.S. government can try to exert over YouTube itself. As will be discussed in later sections, government and industry interactions have seen their share of problems. Google has even attempted to combat the problem internally but the data is sparse. Within YouTube, linked videos next to terror content that subtly dissuade watchers from continuing to support the illicit video have had promising results of 300,000 deterred (Schwartz, 2016). However, this does not indicate if the watcher looked somewhere else for the same content on the site or was deterred entirely. While there is no simple solution at hand, YouTube and U.S. officials have been working to resolve these issues as they evolve.

Extremist Use of Encrypted Messaging Applications

The last few years have seen an increase in encrypted messaging as a tool in extremist communication and consequential terrorist attacks. Many believe that the growing popularity of encrypted messaging applications, such as Telegram, Wickr, and WhatsApp, among young people and extremists poses a threat to national security and Americans themselves (Colraine, 2016). Encrypted messaging allows for unmonitored communication between extremists and targeted members of society, which can result in a greater probability of terrorist attacks being carried out on American soil. It also can lead to extremist group operations being more easily carried out and increasing American susceptibility to radicalization (Stalinsky and Sosnow, 2015). Extremist use of these applications results in the specific targeting of, and

psychological preying on vulnerable individuals, which can strengthen terrorist groups such as Al-Qaeda and ISIS.

Research conducted by the MEMRI Jihad & Terrorism Threat Monitor has uncovered Al-Qaeda's use of encryption tools for communication purposes, and their willingness to communicate with anyone willing to "wage jihad" against "unbelievers" since 2007 (Stalinsky and Sosnow, 2015). Similarly, ISIS has been relying on encryption technologies ever since the terrorist group's inception and is continuously seeking to recruit people skilled in this field (Stalinsky and Sosnow, 2015).

Following the 2013 Snowden leaks, jihadis have been less likely to use unencrypted communication and actively refrain from using specific communication platforms that do not provide the same amount of privacy as encrypted messaging applications (Stalinsky and Sosnow, 2015). According to a February 2015 MEMRI report, as the use of Al-Qaeda and ISIS's "own encryption software" has decreased there has been an increase in the use of Western encrypted social media apps (Stalinsky and Sosnow, 2015). The importance of encrypted messaging in furthering extremist activity cannot be denied by the fact that Al-Qaeda and ISIS worked to develop and distribute their own encrypted technology. Extremist groups are using encrypted messaging as a means of communication that is meant to spread their message and image of jihad.

The Dangers of Encrypted Messaging

Communication through encrypted messaging platforms is the final step in establishing a concrete relationship between extremist recruiters and citizens. In a 2015 Homeland Security hearing, Michael McCaul, House Committee on Homeland Security Chairman, explicated ISIS' use of encryption explaining that recruiters have become experts in monitoring and preying on "Western youth" who are prone to messages regarding Islamist

terror. Recruiters intentionally seek out those questioning Islam and life within the "Islamic State" (Stalinsky and Sosnow, 2015). Once trust is established between a recruiter and possible recruit via social media platforms and proof of a possible recruit's dedication meets the recruiter's expectations, users are directed to secure apps such as, WhatsApp and Kik or "data-destroying apps" such as Surespot and Wikr, in which hidden messages regarding the process of joining ISIS and other communications are exchanged (Stalinsky and Sosnow, 2015). Through encrypted messaging, recruiters directly draw in questioning young minds and mold them according to the needs of the extremist group. Direct communication and engagement between recruiters and possible recruits can serve to make the recruit feel significant and included within a larger group. The ability of recruiters to track the interests of recruits allows them to send specialized information that is specific to their desires. Psychological coercion of recruits over encrypted messaging applications is used as a means of crowd sourcing for extremist groups (Colraine, 2016).

Extremist use of encrypted messaging has likely assisted in an increased success rate of terrorist attacks against the West. According to the Homeland Security Committee, between the years 2014 and 2016, the number of "ISIS-linked" attacks increased by more than "50 percent," and "more than 40 percent" of planned conspiracies were successfully carried out (Homeland Security Committee, 2016). These statistics demonstrate ISIS's growing ability to plan and carry out more frequent terrorist plots. Extremist's increased use of encrypted messaging applications to communicate with extremist recruits, sympathizers, and supporters over the last four years has only been a provision in the growth of extremist attacks and plots. Extremist groups capitalize on law enforcement's inability to decrypt communications sent over encrypted applications, which results in the higher success rate of planned attacks and the decreased rate of disrupted attacks as seen in the Homeland Security Committee's report (Kisswani, 2011).

Additionally, the number of "inspired" plots significantly rose in 2015 making up two-thirds of plots against western targets, and in over half of the cases a single suspect was involved (Homeland Security Committee, 2016). By using global network connections, the steep increase in "crowd-sourced" conspiracies demonstrate extremist groups ability to disseminate "terror" electronically and encourage radicalization through encrypted communication, which then drives individuals to act on behalf of parent extremist groups (Homeland Security Committee, 2016).

The dangerous relationship between social media platforms and encrypted messaging applications creates a partnership in which individuals are seduced into the world of extremist organizations through exposure to propaganda. They then are targets for easy and private communication with extremist group members and recruiters, which can result in an increase in radicalization, mobilization, and ultimately—terrorist attacks.

Manipulation of the "Lone Wolf"

The private, one-on-one contact encrypted messaging is particularly dangerous when applied to aggrieved and marginalized populations. Individuals in these populations may be emboldened to carry out "lone-wolf" attacks—those in which the perpetrator is not affiliated with an official extremist group—through close contact with terrorist recruiters (Hamm and Spajj, 2015). As FBI Director James Comey accentuates, lone-wolves are highly susceptible to participating and engaging with terrorist-related activities, as these attackers become attracted to extremist ideology, train themselves in attack strategies, and attempt to renew a sense of empowerment in their own lives (Pelley, 2014). As such, the at-risk individuals are most in danger of becoming encouraged and persuaded by extremists to carry out physical acts of violence on other civilians (Berger and Morgan, 2015, 58).

Such instances show that encrypted messaging serves as a dangerous conduit for terrorist groups and marginalized populations to converse and interact with each other, and carry out violence and harm in relation to terrorist-inspired ideology. In particular, social media use is problematic, as individuals with personal or political grievances can gain greater opportunities to communicate and network with the terrorists. That is, the presence of "personal and political grievances" within the individual contributes to a growing sympathy and embrace of terrorist ideology (Hamm and Spajj, 2015, 10). In turn, these emotions facilitate the absorption and internalization of the stated messages from the extremists, which triggers a desire to do greater outreach to the extremist units. As such, these relationships not only enable the marginalized individual to separate from his past suffering, but also to cultivate a life of meaning and empowerment through association in an organization that engages in violence and coercing others through terrorism (Hamm and Spajj, 2015, 12).

Recommendation

Combatting the prevalence of extremism through social media requires a multifaceted approach. Our recommendation relies on the development of educational programs in the form of campaigns and school development. Campaigns enable social media websites and governments to target individuals who are working or out of school. The general public may not be aware that extremists are searching for targets on social media, therefore, a public service announcement over television and radio regarding use of social media platforms would be beneficial. Simply alerting the public that these kinds of people are active on social media would greatly raise awareness. At the very least, the government should sponsor an ad-campaign that outlines indicators that someone is in communication with recruiters or group members via social media and provides people with a number or website that they can seek out that provides them with advice on how to approach the situation and a means of reporting such instances. The second part of our recommendation relies on the early education of

children and young adults in Internet safety and how to recognize the signs of extremism online and in their peers. Through these programs, youth can learn the methods in which they can stop, report, and combat terrorism. Young adults are the primary users of social media and therefore the front line of defense in recognizing detrimental behaviors.

Current Industry Efforts, and Techniques for Balancing Users' Rights and National Security

Hannah Ross, Cameron Rosenberg, Julia Yoon, Taelim Leena Lee

Social media is continually changing, almost by the day, and the government has simply fallen behind. To fill this ambiguous space, industries have stepped in with their own solutions. Some of these solutions have been effective, however, it differs from platform to platform and government guidance has not been uniform or clear. Therefore, the government must consider what the industry believes is important, along with the policies they have already put in place. In such a new context, old governmental systems simply will not work, and any legislation must consider current activities and usage of social media today. We recommend that they should then establish a set process to access necessary data from private industries while maintaining the company's privacy policy. However, the government should allow the removal and managing of extremist accounts to stay in the hands of private companies.

Monitoring for Extremist Usage

The issue of individual privacy on social media and potential threats to national security that such privacy could facilitate is one without any clear definition. That is to say that the relationship between the social media industry, the government, and extremists is one that presents a significant problem that does not have a clear solution, nor a precedent for an obvious answer, as this issue is so new and unfamiliar. As a result, monitoring for extremist usage on social media is an incredibly complex problem that depends on industry leaders, as well as independent analysts, to find a way to best deter and eliminate accounts that are sympathetic to, and directly support, extremist causes.

For the purpose of this analysis of various monitoring strategies, the term "extremists" is largely limited to terrorist organizations with a particular emphasis on ISIS, and groups such as the Alt-right, and Black Lives Matter. It is important to observe how social media companies monitor the vastness of their respective platforms for extremist usage, and compare that to different—perhaps more effective—strategies that have been employed elsewhere. Moreover, research into the incentives of these social media companies that conduct independent monitoring of their sites is of particular interest because of how certain private policies may clash with policies set forth by the federal government.

Twitter Efforts to Control ISIS

Twitter is perhaps the main tool for mass-broadcasting pro-ISIS related sentiment. For that reason, looking at how Twitter monitors and controls the unwanted extremist usage is of the utmost value. In April 2015, Twitter claimed that it had deleted more than 10,000 ISIS related accounts in one day, citing the accounts' use of "violent threats" sent in tweets (Gladstone, 2015). While this appears to be an effective way to eliminate many unwanted accounts, Twitter does not make information related to accounts and users on its platform public so it cannot be independently verified. Thus, their ability to effectively monitor all of the accounts affiliated with ISIS remains unclear. Additionally, independent researchers believe that as recently as 2015, ISIS had over 90,000 affiliated Twitter accounts (Gladstone, 2015) and so deleting 10,000 of those accounts, while impressive, is not making an exceptionally significant difference. Also of note, the users operating the deactivated accounts were able to immediately create new accounts, albeit without the same number of followers initially (Berger and Morgan, 2015). Twitter has shown the urgent need to prevent extremist ideas from taking root on its platform. Michael Coates, the Chief Information Security Officer for Twitter criticized the dependency on anti-virus measures and archaic

authentication, and emphasized that "security management" must evolve into "risk management" ("Innovation and Focus.").

Problems with "Backdoors"

Currently, it is impossible to determine what account will be a vehicle for ISIS until it has been created and has published information. Creating a "backdoor" for the government could help stop ISIS's spread on social media, but it has its own problems regarding users' privacy. The government has asked technology companies for access to individuals' private devices or entry to personal data many times. Most of the time, technology companies cooperate with government to prevent extremist use of social media, but in multiple cases industries have prioritized user privacy.

However, even though backdoors into products could allow the government to address extremist use of social media, backdoors create vulnerabilities that could be used for nefarious purposes, such as giving terrorist groups access to the same data. This would both endanger national security and compromise individuals' privacy rights.

Privacy versus security, and technology companies versus government legal cases are common. The government claims the cooperation of technology companies can play a crucial role in protecting citizens' safety from extremist groups' use of the Internet and social media. Most technology industries agree with this argument, but their concern lies in the violation of privacy rights and freedom of expression. Companies argue that giving access to the government or creating backdoors poses a threat to ordinary people's personal information.

Moreover, it is difficult to identify extremist users from millions of ordinary customers. Tracking down millions of usernames and granting government an authority on users' personal data to prevent extremist use will create an unsafe online environment and may endanger IT companies. It is crucial for technology companies to build trust with their

customers and protect their users' privacy rights, not only for ethical reasons, but also for long-term benefit. Building a backdoor may solve a temporary problem, however, in the long-run, a backdoor that helps the U.S. government may backfire and put national security in danger.

Freedom of Speech vs. Privacy on Public Platforms

For companies, protecting customers' privacy is essential for building and maintaining user trust. Without protection of users' privacy and free expression, the potential lack of trust could result in companies losing their customers. Social media was created with the intention to share information with the world, but if users do not feel safe to share their personal and business information online, they may stop using it.

The blurred space between industries private policies and the government protections needs to be defined in order close the gap in cybersecurity policy. In addition to freedom of speech, it is important to consider the central privacy protection afforded to U.S. citizens. The Privacy Act was created in 1974 to protect privacy rights and to limit the ability of federal agencies to collect, maintain, use, or disseminate information about private individuals (Firehock 1992, 1510). Congress made this law because of the extent of private information kept by federal government (Ibid, 1513). Thus, according to this Act, individuals can access and demand files related to information about themselves.

However, the effectiveness of the Privacy Act when it comes to accomplishing its goals is still debatable. First, it is often difficult to keep the balance between the conflicting interests, such as the balance between individuals' right to privacy and the need for government to function effectively (Ibid, 1512). For example, according to the subsection (d)(2) of the Privacy Act, individuals may amend information related to themselves that is not "accurate, relevant, timely, or complete" (Ibid, 1513). However, at the same time, some types

of records are prohibited from individuals from accessing in the name of the national security issues. In this case, agencies can limit the rights of individuals to access to, to amend of, and to disclose of certain records (Ibid, 1514).

In addition to measures such as the Privacy Act and other privacy related legislation, the United States ratified the International Covenant on Civil and Political Rights—which includes Article 17, related to privacy (Article 17 of the International Covenant on Civil and Political Rights). However, there is controversy around whether to prioritize national security or citizens' privacy. However, it is clear that both factors are important and need to be considered when making decisions regarding security and privacy.

In addition to privacy law, Section 230 of the Communication Decency Act of 1996 protects individual private platforms with content created by users. For example, Twitter is not responsible for an extremist posting something inflammatory on its platform. It also means that it is legal for Twitter to restrict what its platform is being used for, such as Twitter being allowed to take down the extremist's post even if it is governmentally protected free speech. (47 U.S. Code § 230) However, this limited legislation has been insufficient regarding ever evolving social media practices. The Communication Decency Act was passed more than twenty years ago, and the Internet has changed considerably in that time. While the ideas of this legislation may carry forth, there has been too much change for the government to keep up. Therefore, industries have had to build their own policies.

Technology Companies' Privacy Policies

Many existing technology companies have their own agendas in protecting users' privacy. For example, a recent Microsoft 2016 Corporate Social Responsibility Report states that Microsoft will "[enhance their] company-wide privacy principles and the Microsoft Privacy Statement to protect our customers' personal data and their right to privacy."

(Hauser, 2016) Indeed, Microsoft updated privacy principles and the Microsoft Privacy Statements in 2016 illustrate that they care about customers' personal data and their right to privacy. Microsoft makes sure customer content traveling between services is protected and confirms there are no backdoors through the transparency of their software code (Microsoft, 2016). Twitter is also a big supporter of protecting users' private data and information. In Twitter's privacy policy, it states they:

> May preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request; to protect the safety of any person; to address fraud, security or technical issues; or to protect our or our users' rights or property. (Twitter, 2016)

In addition, both companies have strict guidelines for managing how government may access customers' data. For example, the government needs the appropriate warrant, court order, or writ of specific accounts.

Government efforts to circumvent online security measures to access private customer data is a problem for the technology industry's security and privacy of online communications. In order to protect customers' data and build customers' trust, Microsoft has reinforced encryption across their services, strengthened legal protections for customer data, and expanded the transparency of their code since end of 2014 (Meisner, 2013). The company keeps its transparency about government requests by notifying their customers when legal order is received related to their data (Microsoft, 2016). Through Law Enforcement Requests Reports and National Security Request Reports, which are published every six months, Microsoft stays balanced between government requests and their customers' privacy as they cooperate with legal requests in an appropriate manner, while remaining transparent and faithful to their customers.

With a growing presence of government surveillance, Twitter also took a public stand for transparency and privacy rights. Since 2012, Twitter has also published a biannual report

including statistics of governmental requests and copyright notices. Twitter's effort to protect users' privacy continues to grow. In the midst of relentless requests by the government for user data, Twitter has disclosed national security letters ('NSLs') to be more transparent for their users. The NSLs were accompanied by gag orders from 2015 and 2016, preventing Twitter from notifying the impacted account holders or publicly disclosing their existence. The FBI recently stated that the gag orders have been lifted and that Twitter may notify the account holders.

Twitter had been fighting against the governmental prohibition from reporting on the actual scope of surveillance of its users. Twitter stated:

> Our ability to speak has been restricted by laws that prohibit and even criminalize a service provider like us from disclosing the exact number of national security letters ('NSLs') and Foreign Intelligence Surveillance Act ('FISA') court orders received — even if that number is zero.

This is an ongoing case, Twitter v. Lynch (2014), where Twitter filed a lawsuit against the U.S. government for not being able to report on the actual scope of surveillance of Twitter users by the U.S. government. Twitter wrote:

> We think the government's restrictions on our speech not only unfairly impacts our users' privacy, but also violates our First Amendment right to free expression…we are also considering legal options we may have to seek to defend our First Amendment rights. (Kessel, 2014)

Twitter and Microsoft, as well as many other IT companies, believe users' privacy needs to be protected. They support transparency and privacy rights of users and encourage the U.S. government to set a clear guideline regarding this issue. In addition to private policies, the regulation on withdrawing extremist usage in social media platforms should remain in the hands of the industry, not the government. Thus, in order to develop a better way to detect extremist use of social media, top companies gathered together to work on this goal.

Industry Collaboration and Cases Illustrating Regulation Gaps

With that in mind, however, it is perhaps most important for Twitter to find a way to ensure individuals who have had their account suspended are not able to simply create a new account. This is the goal of the recent coalition of Twitter, Facebook, Microsoft, and YouTube. These companies claim they "curb the spread" of online terrorism by creating a shared database of "hashes" that serve as a kind of online fingerprint (Facebook, 2016). The idea behind this shared database is that each company will collect terrorist imagery that is posted on the respective platforms so that each company can more efficiently identify and remove content that they deem to be extremist-related.

The issue with this collaboration, however, lies in Facebook's assertion that, "each company will continue to apply its own policies and definitions of terrorist content when deciding whether to remove content when a match to a shared hash is found" (Facebook, 2016). This notion seems to undermine the potential efficacy of this type of collaboration. While it may make it easier to monitor potentially ISIS related accounts, if there is not a multilateral coordinated action to remove the content from all social media sites involved in this coalition, then the coalition is largely useless.

The issue of collaboration reveals the problem with any company trying to monitor for extremist use. These are all businesses whose end goal is to make money, so the question of incentive is an important one in determining how companies can better monitor and remove extremist accounts. One major reason companies such as Twitter and Facebook seemingly lack an incentive to more stringently monitor their respective sites for ISIS and other extremist usage can be attributed to a U.S. law that protects Internet-based companies from the liability for anything an individual posts on their site (Communications Decency Act of 1996).

Because these social media companies are mostly free from liability, it also grants them a legitimate reason to not expend a significant effort to monitor and suspend accounts related to ISIS or other extremists. The only concrete incentive for these companies to monitor for this type of extremist usage is their public image. In fact, Twitter only began to extensively investigate extremist accounts after public backlash regarding their perceived apathy towards the issue after they allowed images and videos of the beheading of James Foley, by ISIS members, to circulate online in 2014 (Greenberg, 2015). Perhaps some form of governmental incentive should be offered to the social media companies to ensure they will more strictly monitor for extremist usage.

We will discuss three public cases of the government v. technology companies that explicitly review the problems within the relationship between government and industry in recent years, and examine how these problems will impact the government's request for cooperation from technology companies to stop extremists from abusing social media and mobile technology.

In this section, we will explore three cases of IT industry versus government cases that will be used to discuss and explicitly show the technology industry's perspective on privacy, and challenges with the government.

Apple v. FBI

The aftermath of the mass shooting in San Bernardino, California, propelled the problem on encryption and threats on cybersecurity into the mainstream. Of course, the legal clash between American technology companies and American law enforcement occurred multiple times over the last decade. Most of the time Silicon Valley willingly cooperated with American law enforcement when customer content was protected. However, Farook's iPhone was a different case. First, the FBI led the case into the mainstream media, and the attention given to this case increased the public's interest of their own protection against search

warrants. Apple argued that the software requested by the FBI was capable of destroying encryption built into the iPhone, and that the FBI's request violated First Amendment rights. The courts previously declared that writing code is a form of free speech (The New York Times, 2016). Apple was deeply concerned about future use of permanent a backdoor for further investigation that would pose a threat to ordinary individuals' privacy. Apple argued that,

> If Apple creates new software for a particular case, other federal and state prosecutors—and other governments and agencies—will repeatedly seek orders compelling Apple to use the software to open the back door for tens of thousands of iPhones. (Domonoske, 2016)

The blurry line in the midst of industry's private policy and the government's protection on right of speech question the government's request of backdoor that is intended to protect national security from extremist use. Without a clear guideline to follow, industries created their own policy to protect their customers' personal data and privacy, which lead to cases such as the San Bernardino shooter's iPhone.

Microsoft v. United States Government

The dispute over privacy in cyberspace can occur on both the domestic and international level. In this case, the debate was taken overseas when a New York district court requested a warrant for emails and private information about one of company's customers (Conger, 2016). Microsoft filed the case in 2013 arguing that the information needed by the U.S. government was stored in Ireland and, thus, the U.S. government had no claim over the information. The very next year, a court again demanded Microsoft hand over the customer's email information. However, Microsoft appealed to 2nd Circuit. Throughout the case, Microsoft's supporters including Amazon, Apple, European governments, and media argued on the side of Microsoft as they claimed the U.S. government should gain access through international agreements rather than through a U.S. based search warrant

(Conger, 2016). The question of what method law enforcement should use to access online data is debatable because the rise of digital data has left areas of the law undefined.

The extension of government accesses to online information poses a threat to cybersecurity due to complex interlinked consumers' backgrounds. Microsoft President and Chief Legal Officer Brad Smith stated on this issue as being important for three reasons:

> It ensures that people's privacy rights are protected by the laws of their own countries; it helps ensure that the legal protections of the physical world apply in the digital domain; and it paves the way for better solutions to address both privacy and law enforcement needs. (Smith, 2016)

As most U.S. technology companies become global companies, security in the online world has become essential. Extremist groups such as ISIS target an array of people online for recruitment. To protect national security while protecting user privacy, global technology companies and the U.S. government need to bridge the gap between industry's private policy and existing government policy, to determine the definition of extremist use of social media.

Twitter v. United States Government

WikiLeaks is an international non-profit organization that publishes secret information from anonymous sources. The documents posted in WikiLeaks are a controversial form of free speech because the information can be a threat to national security. Indeed, the U.S. Justice Department requested data from Twitter of one of WikiLeaks' former volunteer Birgitta Jondottir, also Icelandic member of Parliament. To find the leaking source of the army video, the U.S. Justice Department requested Twitter give it access to Jondottir tweets since November 1, 2009 (Zetter, 2011).

It was clear that Jonsdottir had no intention of handing over her personal data as she tweeted, "USA government wants to know about all my tweets and more since novermber 1st 2009. Do they realize I am a member of parliament in Iceland?" Jonsdottir started a legal

fight to stop the U.S. government from gaining access to her private Twitter account. Twitter went to court to make the information public (Rushe, 2011). Twitter stated:

> We're not going to comment on specific requests, but, to help users protect their rights, it's our policy to notify users about law enforcement and governmental requests for their information, unless we are prevented by law from doing so.

Twitter's legal counsel Ben Lee also said, "As we said in our brief, Twitter's terms of service make absolutely clear that is users own their content. Our filing with the court reaffirms our steadfast commitment to defending those rights for our users" (Gabbatt, 2012).

Not only Twitter, but also many other technology companies have fought for the right to inform users about law enforcement requests on their personal data. For example, a legal fight began when the Obama Administration tried to secretly seek the email records of another WikiLeaks' journalist from Google to prevent public backlash, referring back to Jonsdottir's case (Gallagher, 2015). This is one of most common dilemmas industries and government face today because of the blurry space between national security and privacy.

Evaluating of Extremists vs. Activists

The following three case studies illustrate the challenges in determining what content is considered extremist and what should be done to tackle it. Here we examine ISIS, the Alt Right, and the Black Lives Matter movements on Twitter as a window into the challenge posed. While it is almost universally accepted that ISIS poses a threat to national security and should not be given a platform because their ideas are inherently violent, the Alt Right and Black Lives Matter have been called extremist movements by critics. These two movements, in particular, highlight the tension between activists, whose rights must be protected, and extremists, who pose a threat to national security.

ISIS

ISIS, and Al Qaeda before them have used social media—in particular, Twitter—to contact potential Western recruits. It is hardly controversial to say that social media should not be hosting their rhetoric. In 2015, two Americans were killed in Jordan, and ISIS said the shooter was associated with their group. In August 2016, the American victims' families filed a lawsuit against Twitter saying that, by giving ISIS a platform, Twitter was acting against the Anti-Terrorism Act. Their argument was that Twitter had provided a way for ISIS to recruit, and therefore was at fault for the shooting (Geuss, 2016). Twitter argued that because they have no inherent blame in who uses the platform, they were not at blame for the men's deaths. Twitter cited Section 230 of the Communications Decency Act of 1996, which frees them from liability (Geuss, 2016).

Twitter's inability to track down every Twitter account related to ISIS is not in itself illegal. On the other hand, Section 230 also says that a social media platform does not have to host anything it does not want to host. A private platform does not have to follow free speech mandated by the government, and, therefore, Twitter has ultimate control over the content on its platform.

As discussed throughout the report, ISIS is a clear threat to national security, but when it comes to controversial domestic groups, the technology industry has had to make their decisions reactively.

The Alt-Right

In 2016, a new movement sprang up alongside President Donald Trump's rise to power. Short for "alternative right," the Alt-Right is marketed as rebranded conservatism for millennials. Created by the head of the National Policy Institute, Richard B. Spencer, the movement has since gained a life of its own. Described by the Southern Poverty Law Center

as “a suit-and-tie version of the white supremacists of old, a kind of professional racist in khakis” (Richard Bertrand Spencer, 2016), Spencer is the head of an institution that states that its purpose is “dedicated to the heritage, identity, and future of people of European descent in the United States” (Farivar, 2016).

To outside critics, the Alt-Right is viewed as a prettier reincarnation of Nazism and white nationalism, and in many cases, they are correct. However, the movement itself is not unified. Milo Yiannopoulos, a former editor at Breitbart, wrote in a Facebook post that, “The New York Post inexcusably refers to me as an ‘Alt-Right extremist.’ I am neither Alt-Right nor do I hold any extremist views” (Yiannopoulos, 2017). Not to be outdone, the Alt-Right website, The Right Stuff, wrote an article disavowing Yiannopoulos, who they condemn for being a gay man of Jewish heritage. The piece is full of anti-Semitic, homophobic and transphobic sentiment and slurs, reminding readers of its ultimate goal of white supremacy (T. Scot). Not even Spencer agrees with the media’s assessment of Yiannopoulos as a part of the Alt-Right movement (SHUTTERSHOT45, 2016).

To outsiders, Yiannopoulos and Breitbart and Spencer are interchangeable, with the title “Alt-Right” used as an umbrella for all movements within this new conservative ideology. However, the “Alt-Right” is divided into factions; it is the Alt-Right of Spencer and the Breitbart movement that use social media.

On the day of Trump’s inauguration, Spencer was filmed being punched by an unknown attacker (Weiner, 2017). The next day he was on social media calling on members of his Alt-Right group, saying:

> [People in the Alt Right] are going to need to step up to offer some kind of protection, or we can’t have a public movement, and if we don’t have a public movement we are not going to win, period. (Alt Right, 2017)

Although he was referring to physical protection, he needed to get his message out fast, and YouTube was an effective way to do so.

However, even in public, he used social media to signal himself as a member of the movement. He used a commonly known Internet meme, that is, a picture or saying to convey additional meaning (Meme, n.d.). His was of "Pepe the Frog," which the Anti-Defamation League listed among its hate symbols (Pepe the Frog, 2016). It seems ridiculous, but it demonstrates the fact that people who know that symbol from social media would know at a glance what movement he was aligned with, even if they did not know him.

Because of his controversial use of social media, his Twitter account was suspended. He claimed that "he was 'alive physically,' but he likened the suspensions to 'digital execution squads all over the alt-right,' and compared it to the 'Night of Long Knives'…" (Farivar, 2016). He was banned based on Twitter's hateful conduct rules, which read:

> You may not promote violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or disease. We also do not allow accounts whose primary purpose is inciting harm towards others on the basis of these categories. (Twitter, n.d.)

Twitter later claimed he was suspended because of a technicality and his account was reinstated. But, the suspension raised questions about freedom of speech issues.

In the Breitbart movement, Milo Yiannopoulos is still permanently banned from Twitter. In July 2016, Yiannopoulos began an attack on Twitter of actress, Leslie Jones. Breitbart claimed that Yiannopoulos made no threats against Jones, although Jones reported him to Twitter and his Twitter account was permanently suspended (Kew, 2016). He claims that what he sent was hate mail, nothing more offensive than a critique, and that Jones was simply playing the victim by reporting him (Nolan, 2016). However, Twitter viewed this as targeted harassment and Yiannopoulos lost his ability to connect with others through that platform.

Conservatives have claimed that it was political bias that Twitter responded so differently to accounts seen as "liberal," such as Black Lives Matter (Kew, 2016). Although

Yiannopoulos recently left Breitbart News at the end of February 2017, he is arguably still a prominent figure and still has supporters, meaning he may simply change platforms (Alpert, 2017). Regardless of his current status, it was a highly publicized event in the Breitbart Alt-Right movement and worth evaluating larger claims made during this suspension.

His suspension is an important event because it is a problem of how to limit hate speech and what defines hate speech. Twitter's harassment policy is purposefully vague, so nothing can fit it exactly. There must be a policy to keep harassers from acting that maintains free speech, and Twitter's vague policy is not enough. Whether or not Twitter actually has a bias, its policy needs to be reviewed, along with other platforms, because there could be politically motivated censorship in the future.

The problems with Twitter's moderation are compounded by the very real violence that happened outside Yiannopoulos's speeches in January and February 2017, notably the shooting at the University of Washington, Seattle (Wong, 2017) and the violence at University of California, Berkeley (Park & Lah, 2017). The violence at Berkeley resulted in Yiannopoulos's speech being cancelled because of the physical danger it posed to him and his audience (Park & Lah, 2017). In the threat of violence, one could argue that a social media movement caused real world violence.

Black Lives Matter

Black Lives Matter also began online. It started as a hashtag on Twitter after Trayvon Martin's killer was released in 2013 with no punishment. #BlackLivesMatter first appeared on Alicia Garza's Twitter, (Garza, n.d.) which resonated with others. As Garza argued, "Opal [Tometi], Patrisse [Cullors] and I [Alicia Garza] created the infrastructure for this movement project – moving the hashtag from social media to the streets" (Garza, n.d.).

Black Lives Matter gained traction in August 2014 after a police officer shot Michael Brown, a black teenager—although the movement eventually spread to cover all African Americans. Ferguson, Missouri, Brown's hometown, was brought into the national spotlight because of the protests that sprung up immediately after his death. Brown had been shot by a police officer, and Black Lives Matter demanded more accountability for police officers and an end to the brutality used against the citizens.

Social media was important for Black Lives Matter because events that might bypass the traditional news cycle were publicized (Shalby & Sreenivasan, 2014). News was immediately provided for everyone and allowed people to search events in real time. Additionally, officers would not be able to spin the stories because the events were portrayed as they happened (Shalby & Sreenivasan, 2014).

One voice to emerge from the protests was that of DeRay Mckesson. Using Twitter and the live streaming service Periscope, he filmed the protests extensively. In fact, Twitter bought Periscope after it was used so successfully by the protests in Ferguson (Mattise, 2017). Now, he believes that social media is an extremely helpful way of getting information to people. Mckesson argued:

> We didn't invent resistance; we didn't discover injustice. We exist in a legacy of people who've done this work, but what's new is we have a different set of tools. Today, I can talk to 600,000 people at the drop of a tweet in a way that King, Fannie Lou Hamer, and Coretta couldn't (Mattise, 2017).

Black Lives Matter is not entirely a social media movement; it has moved to the streets in protest, but it still relies heavily on Twitter.

Unlike the Alt-Right, where each core group has a website to focus around, Black Lives Matter does not have one clear center. There is a website called blacklivesmatter.com, but it is much sparser than any of the Alt-Right websites and not a center hub of the movement (Garza). While the ideals are the same across every protest—uplifting Black lives—it is not centralized and groups do not simply wait for instructions from some far-off

leader. It is difficult to pin down precisely what each Black Lives Matter local group demands, but in the end, it all comes back to that same idea, that Black lives are in danger and the societal structures that allow and do not punish police killings of African-Americans must be addressed. The movement has also expanded to focus on larger oppressive societal structures as well.

Former New York mayor and current White House cybersecurity adviser Rudy Giuliani said in July 2016 that Black Lives Matter is inherently racist and poses a very real danger to police forces, saying "it puts a target on their back" (Giuliani, 2016). A "We the People" petition to label Black Lives Matter a terror organization garnered 141,000 names and then-President Obama responded to the petition by saying, "We shouldn't get too caught up in this notion that somehow people who are asking for fair treatment are somehow, automatically, anti-police, are trying to only look out for Black lives as opposed to others" (Flores, 2016). The president of the Southern Poverty Law Center, Richard Cohen, stated firmly in July 2016 that Black Lives Matter is not a hate group (Cohen, 2016). He stated that there was no bigotry from the leaders and that there is, "nothing at all to suggest that the bulk of the demonstrators hold supremacist or Black separatist views" (Cohen, 2016).

Social media allows people to converge quickly. As has been apparent in the last few months, protests have popped up "spontaneously" across the country. These protests are not born when thousands of people had the idea to go alone and just happened to meet others there; it was that social media allowed the message to be sent to the protestors, who could convene together. Black Lives Matter protests require much less planning than civil rights protests in the past.

This is all well and good until violence happens outside the Internet. In August 2016, five police officers were killed in Dallas, Texas during a protest. It has since been established that the shooter was not affiliated with Black Lives Matter (Jenkins, 2016) but it has set a

precedent that there could be violence. The concern about potential violence has made police forces increase their presence at protests. Damon Crenshaw, vice president of the Next Generation Action Network, organized the protest and said afterwards, "Why all of a sudden are we the target? We're not protesting because we're mad at them. We're protesting because the problems still exist and they won't talk to us" (Jenkins, 2016). Black Lives Matter leaders dislike this because the increased police presence can increase the potential for more violence and police brutality.

Much like at Yiannopoulos's speeches or in his Twitter feed, neither group called directly for violence or attacks. Every large group will have outliers—and when it gets big enough—have violent followers. And while the leaders of each group can condemn the perpetrators, the fact remains that the large crowds of protestors drew violent people. Social media allows for people to gather quickly, but can also draw violence quickly. If they so choose, social media companies could legally take away activists' platform, thereby making the organization protests harder to organize in an attempt to reduce this violence.

While the Southern Poverty Law Center has been very clear about how they view each movement, there will always be people who disagree and may have completely opposite views. People who disagree with Twitter's vague policy implementation could potentially leave and use a different platform. But the movement could widen the gap between political parties and reinforce the "bubble" people live in (Solon, Levin, & Wong, 2016), where it could be impossible to find common ground in the future.

Social media has changed the way people interact with each other in a very short period of time. New social media platforms are popping up constantly, meaning that by the time a Twitter-specific policy is passed, said website may be obsolete. Legislation must be broad enough to cover changing platforms, but specific enough that it is not simply an "I'll

know it when I see it" form of surveillance. However, the rights of individual platforms to choose what it is used for must be maintained.

Alternative Monitoring Techniques

Being a main target for spamming and hacking attacks, in 2014, Facebook implemented ThreatData, a framework that collects threat information from a variety of sources that includes malicious websites. Some examples of feeds are malicious URLs from multiple open source blogs and malware tracking sites, and Facebook's internal sources of threat intelligence (Facebook Security, 2014). The CISO of Facebook, Joe Sullivan has stated that instant response is necessary to fight the threats that are rapidly changing in its form and size.

As the largest web search engine, Google has launched a new cybersecurity project named 'Project Zero,' which is built to "improve the security of any software depended upon by large numbers of people" (Zero, 2014). Google has announced that security efforts will be undertaken transparently, with every bug "filed in an external database." Project Zero will only report to the software's vendor without third parties, and they aim to significantly reduce the number of people harmed by targeted attacks.

Potentially, Twitter could look to more time and cost effective measures to monitor for extremist usage rather than attempt to manufacture some kind of internal incentive beyond public image. In an independent study of the monitoring of ISIS related Twitter accounts, machine learning models were used to conduct statistical analyses of various Twitter users to determine how to best monitor their behavior and track extremist use patterns (Ferrara et. al, 2016). The study employed the method of Random Forests, a technique that can be applied to monitoring Twitter accounts automatically by slightly changing the search and relationship criteria with each search (Breiman, 2001). The goal of the study was to demonstrate how already-existing search methods can be applied from other fields to

effectively monitor the activity of extremist users on Twitter. This method resulted in successful prediction of ISIS-related Twitter accounts as much as ninety-three percent of the time (Ferrara et. al, 2016).

The purpose of studies such as this is to reveal how there are several alternative options that social media companies can employ to more efficiently monitor their sites for extremist usage. Twitter and other social media companies could look to independent studies such as this one for monitoring techniques that can make their own efforts more effective.

Recommendation

The issue for social media companies in terms of protecting personal privacy versus ensuring national security creates a difficult situation to navigate. The companies have no concrete legal obligation to internally monitor for extremist usage, yet the U.S. government is constantly demanding user information to track such usage. Moreover, the companies have an implicit duty to maintain the privacy of their users, a responsibility that causes significant problems in determining what is and is not allowed on their respective platforms. Determining what is activism and what is extremism is not always a simple task, nor is monitoring for these types of users to be able to determine if there is a problem that should be dealt with at all.

There is a constant battle between social media companies and the government in terms of what the correct course of action should be regarding users who present a threat to national security. Indeed, the social media companies understand that threats must be dealt with, but not at the expense of the other users' personal privacy. In determining the best policy decision for the government in terms of cyber security as it relates to extremist usage of social media, it is paramount that the government maintains personal securities to ensure trust between themselves and social media companies, as well as the vast majority of the population that actively uses these various platforms. Perhaps, then, some form of

governmental incentive should be offered to the social media companies to ensure they will more strictly monitor for extremist usage. Ultimately, the decisions should go to the industry as to what they will host, but the government should create very clear guidelines as to what constitutes extremist content.

U.S. Government Response to Extremist Use of Social Media: Balancing National Security vs. Rights

Serena Eunbich Ko, Natalie Meek, Rajeev Stephens, and Priya Uppal

As illustrated, extremist use of social media poses a serious and growing national security challenge. However, current U.S. government action in relation to extremist use of social media is unclear and routinely uses outdated law. It is necessary to impose legislation that balances national security and privacy in the realm of cyberspace.

This section outlines the constraints on the U.S. government in tackling extremist use of social media. First, we discuss the constitutional rights that American citizens have, and specifically, the liberties outlined in the First Amendment, which can be applied to social media usage. Second, we will discuss U.S. Supreme Court cases which have established precedents for allowances of free speech in private spaces. Third, we will discuss four government policies that are at the heart of the national security vs. privacy debate. Fourth, moving from constitutional rights, we will discuss the roles, efforts, and controversies of the Federal Bureau of Investigation (FBI) and National Security Agency (NSA). Finally, we will conclude with a recommendation that will establish the baseline for a policy that will balance the interests of national security and privacy.

Our recommendation is that law enforcement and intelligence agencies should be able to legally collect any and all information necessary in the interests of national or state emergency or in the interests of crime prevention, on any U.S. or non-U.S. person, if and only if the person or persons in question present a clear and present danger or have close ties to someone who presents a clear and present danger. Agencies will have to file a request to the Foreign Intelligence Surveillance Court, backed with evidence as to why they need to collect this information, who will then either deny or approve the request based on the evidence. At any point in the FISC review, industry can provide evidence in cooperation with or in

contradiction to law enforcement and intelligence agencies' efforts, in courts up to and including the U.S. Supreme Court. Any violation can result in state or legal trial up to and including Supreme Court trial, where punishment may result in revoking of security clearance, removal of position, and possible fines and jail time. In regards to violation of the First Amendment it will remain the jurisdiction of the United States Supreme Court to evaluate each case. The trial must be conducted as according to the due process of law under the Fifth Amendment, maintaining the innocence of every defendant until proven guilty.

The Evolution of Speech Rights Related to Social Media Use

> The First Amendment, ratified in 1791 as part of the Bill of Rights states that:
>
> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. (Tennessee, 2016)

In the United States the First Amendment guarantees freedom of speech for citizens unless the words said can be proven in the court of law to incite a clear and present danger to the public. These rulings can be made by courts up to and including the U.S. Supreme Court, which has naturally set precedents that extend down to the lower courts in landmark rulings. The ambiguity in First Amendment rights is problematic when attempting to apply its rules to the communication and fundraising efforts employed by terrorist groups using social media.

Allowed Speech under the First Amendment

It is important to understand the different laws and precedents that may be used to evaluate extremist use patterns of social media. According to the United States Courts, "freedom of speech includes the right not to speak, to use certain offensive words and phrases to convey political messages, and to engage in symbolic speech" (Courts, 2017). On the other hand, "freedom of speech does not include the right to 'incite actions that would harm others

(e.g. shouting fire in a crowded movie theater), and to make or distribute obscene materials'" (Courts, 2017). Different metrics have been used by the U.S. Supreme Court over time to determine what is protected or unprotected under the First Amendment. The following precedents including a clear and present danger, a bad and dangerous tendency, and obscenity are just a few examples of tests that have been used to evaluate freedom of speech cases (Chemerinsky, 2017). All relate to extremist use of social media.

The first case worthy of mention is Schenck v. United States (1919) where the precedent for words inciting a "clear and present danger" (Costly, 2017) was made. This precedent is of central importance in addressing extremist use of social media. The case involved a socialist named Charles Schenck who, along with his party, distributed 15,000 pamphlets urging men to resist the draft into World War I (The Editors Of, 2016). The defense argued that Schenck's action was protected under freedom of speech but the Supreme Court, in a unanimous ruling written by Oliver Wendell Holmes, decided otherwise (The Editors Of, 2016). An excerpt of the statement reads:

> Words which, ordinarily and in many places, would be within the freedom of speech protected by the First Amendment may become subject to prohibition when of such a nature and used in such circumstances as to create a clear and present danger that they will bring about the substantive evils which Congress has a right to prevent. (The Editors Of, January 2016)

Although Holmes wrote this statement in reference to the specific case Schenck v. United States (1919), the landmark ruling presents the important point that it matters when and where words are said in reference to their legality. That said, other doctrines including a "bad and dangerous tendency" (Chemerinsky, 2017) have also been used historically, as in the U.S. Supreme Court Case Gitlow v. New York (1925). In Gitlow v. New York (1925), a member of the communist party in New York was arrested for publishing a radical newspaper that advocated overthrowing the United States government (The Editors of, May 2016). In this case, the violation of free speech was due to the rhetoric of political instability that

Gitlow was preaching. This case could be relevant to extremist cases today because of anti-American and anti-government rhetoric often used by extremists to recruit on social media. A third parameter that is important in relation to extremist use of social media is obscenity. Obscenity is another doctrine that can be used to evaluate extremist behavior depending on the severity of content posted. Obscene content is unique in that it was never meant to be included under the protections of the First Amendment (Ruane, 2014). The U.S. Supreme Court has come to evaluate obscene materials according to a three-pronged Miller test (Grocki, 2015). The relevant parts of the test in relation to extremist use patterns include whether adult community standards find the matter unhealthy, degrading, or shameful (Grocki, 2015). Thus, the test has specific merit for use in determining the illegality of posting words, photos, and videos that extremist groups often post to incite fear and demonstrate their power.

Freedom of Speech in Private Spaces: The Shopping Mall

Freedom of speech in private spaces has also been the subject of a variety of Supreme Court cases that seek to define and establish precedents that balance privacy, privatization, safety of Americans, and constitutional rights. The following cases surrounding shopping malls provide examples of allowances under the First Amendment, which can be applied to social media and cyberspace. One of the first notable cases was Marsh v. Alabama where the definition of public versus private property was considered in relation to First Amendment rights. The defendant was distributing religious pamphlets on a sidewalk of a privately owned central business district (Policinski, 2012). The Supreme Court ruled that the sidewalk was inherently public, once the property was opened to public use (Policinski, 2012). The defendant was protected under the First Amendment despite the private ownership of the town. This case demonstrates that private property is a grey area in regard to federal laws.

Marsh v. Alabama is especially relevant amongst the current clashes between industry and government such as the case surrounding the San Bernardino shooter's Apple iPhone. The ruling in Marsh v. Alabama (1946) was extended to shopping malls in the case Amalgamated Food Employees Union v. Logan Valley Plaza (1968), where the Supreme Court noted that shopping malls had taken on characteristics of municipalities, and, thus, were subject to federal laws (Policinski, 2012). That said, in Hudgens v. NLRB (1978), the Supreme Court decided that unless owners intended to make shopping malls equivalent to public spaces, that as private properties, the First Amendment guaranteed no rights there (Policinski, 2012). The assortment of rulings surrounding shopping malls cases is indicative of the different rulings the U.S. Supreme Court has made about freedom of speech, private spaces and federal laws. It demonstrates that there is space to try cases surrounding private social media platforms in courts up to and including the U.S. Supreme Court.

Constitutional Rights and Social Media

The First Amendment guarantees freedom of speech unless that speech is deemed unconstitutional in the court of law. There are a number of metrics to evaluate freedom of speech in relation to security, including a clear and present danger, a bad and dangerous tendency, and obscenity (Chemerinsky, 2017). These precedents should be used to inform decisions surrounding extremist use of social media.

Furthermore, the examples of Supreme Court Cases in shopping malls are another way that the private platforms of social media may be handled in the court of law. The current ambiguity in allowances of speech under First Amendment rights is a major contributor to the inability to effectively manage extremist use of social media platforms. That said, the best way to deal with extremist use is on a case-by-case basis where a

defendant should be tried in courts up to and including the U.S. Supreme Court for posting words, photos, and videos that may or not be protected under the First Amendment.

Government Surveillance Laws, Acts, and Policies

Freedom of speech shapes the ways in which government may control dangerous speech. However, the issue of finding and stopping extremists—online or otherwise—is a matter of broader national security as well. This section of the report will focus on the four following pieces of legislation in relation to government surveillance:

- Communications Assistance to Law Enforcement Agencies (CALEA);
- The Foreign Intelligence Surveillance Act and Foreign Intelligence Surveillance Court (FISA/FISC);
- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), in particular Section 215 of the USA PATRIOT Act, and the Freedom Act;
- The All Writs Act.

For each policy, we will examine their historical context and what they do in terms of government surveillance. We will examine the fallout of the latter two policies; Edward Snowden and the iPhone controversy, respectively.

CALEA: Historical Context and Effects

On January 25, 1994, Congress put forth H.R. 4922 as an act to "make clear a telecommunication carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes." On October 25th, 1994, CALEA became public law as the bill set forth in January was passed (US Congress, 1994, pg. 1). CALEA ensures the private telecommunications' carriers to enable government surveillance efforts on their customers, pursuant to some kind of legal authorization. Due to the laws of

CALEA, telecommunications carriers are legally obliged to do the following: intercept subscriber calls, deliver intercepted communications in a format that can be transmitted to the government and/or to a location that does not belong to the carrier, reveal caller-identifying information, and facilitate the interception of calls so long as it is unobtrusive and presents a minimum level of interference with the subscriber's service.

The following is the verbiage used in the CALEA bill, detailing what effects it provides government and law enforcement surveillance in terms of CALEA requirements:

> Requires a telecommunications carrier to ensure that its equipment, services, or facilities that provide a customer or subscriber to originate, terminate, or direct communications are capable of: (1) isolating and enabling the Government, pursuant to a court order or other lawful authorization, to intercept all of the subscriber's wire and electronic communications over such facilities concurrently with their transmission or at any later time acceptable to the Government; (2) isolating and enabling the Government, pursuant to a court order or other lawful authorization, to access call-identifying information (CII) that is reasonably available to the carrier except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices, such CII shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number); (3) delivering intercepted communications and CII to the Government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by federally procured equipment, facilities, or services to a location other than the premises of the carrier; and (4) facilitating authorized communications interceptions and CII access unobtrusively and with a minimum of interference with any subscriber's telecommunications service in a manner that protects the privacy and security of communications and CII not authorized to be intercepted and information regarding the Government's interception of communications and CII access (US Congress, 1994, pg. 2-3).

CALEA is a commonly used policy by law enforcement but in its verbiage, it fails to address the realm of cybersecurity. In terms of national and civil security balancing with privacy in the realm of cybersecurity, cyberspace needs to be addressed, as that has become an important line of communication as can be seen with ISIS recruitment on social media.

FISA/FISC: Historical Context and Effects

FISA was put into law on October 25, 1978 in order to "authorize electronic surveillance to obtain foreign intelligence information (Government Publishing Office, 1978)." Under FISA, electronic surveillance means "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication" (Government Publishing Office, 1978). The term "foreign" specifically refers to a "foreign power," which is a "foreign government or any component thereof, whether or not recognized by the United States;" or an "agent of a foreign power" which means, "any personal other than a United States person, who acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power" (Government Publishing Office, 1978).

FISA made two significant impacts on how the U.S. government conducts its domestic surveillance. Firstly, FISA provided a framework for how law enforcement and government agencies can legally collect electronic surveillance in the domestic realm. Secondly, FISA created the Foreign Intelligence Surveillance Court, which provided guidance and approval for the government agencies' cases. What this specifically means is that the FISC is the approval authority for government surveillance, in particular, for foreign surveillance—or to gain information on agencies and countries outside of the United States. However, one thing to note is that FISA/FISC did enable the surveillance efforts that were done in accordance to Section 215 of the USA PATRIOT Act, so the term "foreign intelligence" has been used loosely.

This relates to the balance of national security, civil security, and privacy in cyberspace because the FISC is currently the authority that grants approval for surveillance—although they had a bad track record during the USA PATRIOT Act, there have been

revisions to the FISC in relation to the FREEDOM Act and they play a key role in our recommendation

USA PATRIOT Act/FREEDOM Act: Historical Context and Effects

The USA PATRIOT Act was an act that empowered law enforcement and intelligence agencies to monitor people within U.S. borders with the objective of preventing terrorist attacks. The Act was passed during the Bush Administration after the 9/11 attacks with little debate in Congress (Electronic Privacy Information Center, 2017).

The FREEDOM Act was passed into law by President Obama on June 2, 2015. The FREEDOM Act specifically addresses Section 215 of the USA PATRIOT Act (US House of Representatives Judiciary Committee, 2015).

The intent of the USA PATRIOT Act was to enable law enforcement and intelligence agencies to conduct the same type of surveillance on terrorists that these agencies do on criminals on a normal basis. As Senator Joe Biden said on the debate floor in regards to the USA PATRIOT Act, "The FBI could get a wiretap to investigate the Mafia, but they could not get one to investigate terrorists. To put it bluntly, that was crazy. What's good for the Mob should be good for terrorists" (US Congress, 2004).

While the intent was to keep Americans safe, the USA PATRIOT Act has also resulted in the NSA compromising ordinary Americans' privacy. Section 215 of the USA PATRIOT Act enables government agencies "access to records and other items under the Foreign Intelligence Surveillance Act" (US House of Representatives, 2001). The bill itself goes into more detail explaining that "Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503" and dictated that it allowed its users to attain "access to certain business records for foreign intelligence

and international terrorism investigations," "congressional oversight," and "DNA identification of terrorists and other violent criminals" (US House of Representatives, 2001).

What this means is that through petitioning FISA and under Section 215, government officials collected cellphone data on every single cellphone in America—including phone numbers, call history, call length, locations, and other sensitive pieces of information. With this information, the NSA can ascertain private information about citizens—information such as gender, religion, political activism and leaning, health information, among other data (CNN, 2015). The NSA abuse that has been enabled by Section 215 was leaked to the public by Edward Snowden, a controversial subject we will talk about in the next section.

The FREEDOM Act was passed into legislation for the express intent of addressing the abuse of power that Section 215 of the USA PATRIOT Act enabled. The FREEDOM Act "prohibits bulk collection of ALL records under Section 215 of the PATRIOT Act, the FISA pen register authority, and national security statutes" (US House of Representatives Judiciary Committee, 2015). It has put into effect the following legislation:

- "Amicus curie at the FISA court to provide guidance on matters of privacy and civil liberties, communications technology, and other technical or legal matters." (US House of Representatives Judiciary Committee, 2015)
- "All significant constructions or interpretations of law by the FISA court must be made public." (US House of Representatives Judiciary Committee, 2015)
- "Tech companies will have a range of options for describing how they respond to national security orders, all consistent with national security needs." (US House of Representatives Judiciary Committee, 2015)

In simpler terms, what the FREEDOM Act does is provide regulation and revision to Section 215 of the USA PATRIOT Act but still enables national security effort by providing a framework for closer supervision of FISA. It also does this by closing "a loophole . . . that

requires the government to stop tracking foreign terrorists when they enter the U.S" (US House of Representatives Judiciary Committee, 2015). At the time of this report's publication, the USA PATRIOT Act is still in effect however the FREEDOM Act has replaced some of its legislature—namely Section 215.

USA PATRIOT Act/FREEDOM Act: Edward Snowden

The information Snowden leaked consists of information of the following nature: NSA collecting information on millions of private telecommunications companies' customers, using a program called PRISM to collect information through Internet companies such as Google and Facebook; a list of overseas cyber-attack targets; the bugging of European Union offices; foreign intelligence services coordinating with NSA surveillance efforts; warrantless searches on U.S. citizens' emails; the classified budget of 16 different spy agencies; and the NSA's ability to access user data from most major smartphones, among many other leaks (Business Insider, 2013).

The FREEDOM Act was put into legislation two years after Edward Snowden's leaks. This most likely happened because the demand for greater government transparency grew significantly after the ensuing outrage from what Snowden revealed. Snowden's leaks show that the government violated the privacy of its citizens and not even in the interest of national or civil security. This abuse of power is exactly what our policy recommendation is trying to prevent while still enabling the government and law enforcement to be successful in their missions.

All Writs Act: Historical Context and Effects

The All Writs Act is a law that was put into effect in the United States in 1789. The laws of the All Writs Act can be found in the 28 USC 1651. According to law in the aforementioned section, "The Supreme Court and all courts established by Act of Congress

may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law . . . An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction" (United States Code, 1789). To minimize the over-two-century old legalese, what this essentially states is that the All Writs Act enables court judges the ability to issue orders, or writs, to have people comply with their wishes so long as it is within legal limitations (Lewis, 2016). Being that it is an incredibly broad law, there has been some debate that this could set an ugly precedent for user privacy in the future.

All Writs Act: iPhone Controversy

Perhaps the most recent controversy related to the All Writs Act started on December 2, 2015. On that date two active shooters assaulted and killed 14 people and injured 21 people at the Inland Regional Center. After the two shooters were killed by law enforcement, the Federal Bureau of Investigation (FBI) took the lead in the investigation and sought access to one of the shooter's iPhones. Due to its advanced encryption, the FBI sought Apple's help to unlock the phone and give the government access to the shooter's information (Calamur et. al., 2015).

However, Apple CEO Tim Cook denied these requests saying that what the FBI was requesting would require a brand new software, and by creating this software Apple would enable the government to continue to gain access to their customers' cell phones and compromise their customers' privacy in the future (Kharpal, 2016). As a result of Apple's refusal, the government used the All Writs Act to have the judge overlooking the case to legally compel Apple to cooperate with the government—which Apple refused to comply with, stating that the All Writs Act "does not provide the judiciary with the wide power necessary to issue such an order especially absent any statutory support" (Longtin, 2016).

The FBI later found a third-party solution through an Israeli company called Cellebrite; Apple did not take part in unlocking the phone (Kharpal, 2016).

This case remains as an example of the dilemma between private companies and the government when it comes to cybersecurity for several reasons. Law enforcement agencies express concerns about how encrypted data complicates their job and may slow the process of justice while private companies argue that encryption is paramount to the protection of their customers' privacy (Kharpal, 2016).

The iPhone controversy is evident that the U.S. government does not have a clear answer for how to interact with new technology. The All Writs Act was put into legislation during George Washington's presidency. New legislature needs to be implemented with social media and cybersecurity in mind to give a clear direction to all players involved in cyberspace; the government, law enforcement, industries, and private citizens.

Countering Extremist Use of the Internet Using Government-Led Surveillance

Extremist and terrorist groups operating globally have been using the power of the Internet to radicalize, recruit, mobilize, and respond to targeted-communities. More specifically, these groups use social media platforms to target vulnerable young people, and more alarmingly, to spread their messages of hate and intolerance toward the West. In addition, extremists and terrorists have become increasingly aware of the benefits of communicating online, successfully accessing cyberspace through its complexity of networks, which provide ample places for them to hide. They operate in cyberspace from various corners of the globe, including the United States, threatening national security and civil society on the ground, domestically and abroad. As more and more sensitive data is stored online and the consequences of cyber-attacks by extremist groups grow each year, the

U.S. government response efforts and overall focus on cybersecurity sees an increase in urgency to counteract online terrorist activity.

In response, the U.S. continues to engage organizations for surveillance of cyberspace and other actors for the proliferation of innovative solutions to reactively respond to and proactively prevent current and future cyber-use by extremist groups, particularly the Islamic State and its sophisticated use of social media platforms. As FBI Director Comey said in 2016, "As these threats to Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our federal, state, local, and international partnerships" (Comey, 2016). The importance of addressing these threats in an adaptive and confrontational manner requires these partnerships because it increases information sharing, allowing for more discussion, appropriation of knowledge surrounding this topic, and effective countermeasure programs.

FBI Efforts to Tackle Extremist Use of Social Media

Since it was founded in 1908, the Federal Bureau of Investigation (FBI) has been playing its role as the leading federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists. As part of its work to tackle the issue of cybersecurity, within the FBI there is the Cyber Action Team (CAT). CAT is not well-known but plays an important role in discovering hackers who infiltrate government organizations' or major companies' networks to steal state secrets, nations' personal information, and other critical data (The FBI Story, 2015, p. 23). CAT also works to tackle the challenges posted by extremist use of social media.

The FBI has also established an Intelligence Branch, as well as a Bureau Intelligence Council to assess threats, and collect information on cybersecurity-related threats (Federal Bureau of Investigation, 2005). Recognizing the seriousness of this threat, the FBI is

providing training and education at all levels to facilitate full employee integration throughout this program. Comey even stated that, "New agents and analysts now engage in practical training exercises…on effectively integrating intelligence processes to maximize resources" (Comey, 2016). After gathering resources and information, they use that data to determine what threats to prioritize to effectively face the challenges of extremism online.

The NSA's Efforts to Tackle Extremist Use of Social Media

In the context of global terrorism, the NSA has been working to protect the U.S. from those who would harm the country (National Security Agency, 2016). The NSA has emphasized the importance of collaboration of national leaders, military leaders, policy makers, and law enforcement personnel to be prepared against those threats from the terrorists and extremists.

However, because the NSA collects data from countries oftentimes without their governments' knowledge, the sovereignty of those countries as well as the privacy rights of their citizens are infringed upon, which proves to be a dangerous problem (Courtney 2015, 545-6). Countries were concerned that this international surveillance might generate information that could be used as a weapon of war. Thus, the mass surveillance by the NSA is a real area of concern for all democracies.

Additionally, the United States is legally obliged to protect the human right to privacy, as codified in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) (Sinha 2013, 899). However, it is still controversial to discuss whether this Article 17 has been well applied to the U.S. as the NSA has been secretly collecting massive amounts of data about American citizens and permanent residents, with the aim of preempting future terrorist attacks using cyberspace, beginning shortly after 9/11. Many people including scholars and politicians wonder whether this massive surveillance by the NSA is legal. Since

electronic surveillance done by institutions like the NSA and the FBI records online behavior, social contacts, interests, and other activities that may extend beyond intended investigatory matters and for longer than is necessary for the investigatory purpose, even ordinary people are in a danger of infringement of privacy.

Department of Homeland Security

In addition to governmental agencies, governmental departments have also taken part in formulating cybersecurity efforts against extremism, though in less active and more bureaucratic ways. The State Department of Homeland Security (DHS) has the role of overseeing the development of "operational procedures for public-private sector coordination on active defense measures" (Department of Homeland Security, 2016), utilizing existing mechanisms for cooperation such as the Industry-led Information Sharing and Analysis Organizations (ISAOs) and the National Cybersecurity and Communications and Integration Center (NCCIC), among other government-led groups and think tanks at the Department of State Bureau of Countering Violent Extremism (CVE) (Department of Homeland Security, 2016). The DHS's role in cybersecurity is relevant to countering extremist use of cyberspace because they operate across a variety of partnerships and prevention efforts affiliated with Countering Violent Extremism (CVE). CVE, generally, aims to address the root causes of violent extremism by providing resources to communities to build and sustain local prevention efforts and promote the use of counter-narratives to confront violent extremist messaging online. Building relationships based on trust with communities is essential to this effort (Department of Homeland Security, 2016). CVE applies to all acts instigated and repeated by violent extremists, and general efforts to counter them, including cybersecurity efforts to prevent violent-extremist messaging and social media use.

The DHS Office of Community Partnerships (OCP) streamlines and oversees the Department's efforts to counter violent extremism domestically to better understand radicalization of vulnerable communities at home. Therefore, OCP plays a role in tech sector engagement to "identify and amplify credible voices online and promote counter-narratives against violent extremist messaging" (Department of Homeland Security, 2016), and in ways that account for past failures by State Department or government actors, like the dismantled and unsuccessful Think Again Turn Away program.

Moving forward, government-led groups, such as the FBI and the NSA, as well as state departments, Department of Homeland Security and the Department of Defense, are continuing to seek various solutions to tackle extremist exploitation of the Internet and are individually and collaboratively working toward new and improved counter-extremist strategies.

Information Sharing

The NCCIC has increased its distribution of information, the number of vulnerability assessments conducted, and the number of incident responses. Given the nature of the evolving terrorist threat in the context of cyber-recruitment and exposure, "building bridges to diverse communities is also a homeland security imperative" (Department of Homeland Security, 2016). Educated and well-informed families and communities within 'ISIS pre-targeted/potential targeted regions' are the best defense against terrorist ideologies. In order to eliminate the spread of online propaganda and social media publications by extremist groups like ISIS, "greater partnerships with the Internet service providers and those who oversee the social media platforms is necessary in getting as close as possible to a solution" (Former CIA Director, David Petraeus). Furthermore, increased information sharing amongst government-

private sectors is crucial to sharing situational awareness of harmful cyber activity like extremist activity on social media.

Therefore, the current mission of NCCIC, relating to the current cybersecurity framework and goals by governmental and industry standards, is to lead the protection of federal civilian agencies in cyberspace, safeguarding critical infrastructure while "protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communication domains" (us-cert.gov). Because they rely on voluntary collaboration with partners, their ability to extend "synchronized response, mitigation, and recovery efforts" (us-cert.gov), to a variety of stakeholders, is representative of their potential for future collaborations between government-private sector relations (us-cert.gov). After encouragement from the Obama Administration in 2015, and carrying over into more recent discussions by the Trump Administration in 2017, discussions have been directed toward the Department of Homeland Security (DHS) to continue the development of Information Sharing and Analysis Organizations (ISAO), which are important for innovatively and collaboratively designing and implementing counter-extremist use of cyberspace. The emergence of ISAO Standards Organization is aimed at "developing transparent best practices that align with the needs of all industry groups, not just those traditionally represented by Information Sharing and Analysis Centers (ISACs)" Increasing transparency and inclusivity amongst participants from any sector, public or private, "will have the opportunity to provide input on the developing standards" (dhs.gov).

Despite its broad use and overall function, the DHS's various information sharing groups act distinctly and uniquely to provide a platform for the exchange of information and ideas between all sectors. Increasing government partnerships with social media companies and other ICT private companies, all the while keeping in mind best practices, will prove to be effective for countering cyber threats such as the extremist use of social media.

Counter-Narrative Programs

Pertaining to counter-narrative strategies and campaigns implemented by both government departments and information and communications technology (ICT) companies, these strategies and campaigns have not yet determined clear and effective solutions in redirecting potential extremists from radicalization through social media. The "Think Again Turn Away" program, implemented by the State Department in 2013, is an example of an ineffective counter-narrative program, particularly relating to this program's presence on Twitter. It shows signs of ineffectiveness by providing a stage for jihadists to voice their opinions. 'Think Again Turn Away' was originally aimed at deterring vulnerable communities online from joining jihad groups by pointing out their fallacies and inconsistencies as a so-called 'state.' The account spread messages about ISIS not being synonymous to the values and religion of Islam, as well as a judgmental narrative about the overall hypocrisy and hate-speech of its leaders. The State Department's account contained counter-narrative material covering articles related to jihadist threats. It also posted various hashtags, "grassroot citizen effort to defeat ISIS using technology to track them," and "ISIS is not about Islam, only terror." (Katz, 2016)

However, such campaigns and their outwardly accusatory language are dismissed as a disingenuous act of reverse radicalization by target audiences and some argue that they, "generate more negativity toward the U.S. and its social media operators" (Katz, 2016). Therefore, they create outlets for ISIS sympathizers and fighters to engage in publicized verbal arguments with the government officials affiliated with the Think Again Turn Away account. They, jihadist recruiters and sympathizers, are provided an equal opportunity to simultaneously launch radical jihadist views and attack the U.S. government. This counter-productive effort by the U.S. State Department is an example of the inefficiencies in past governmental efforts to prevent extremist use of social media. It is also indicative of the

current nature of counter-narrative and counter-extremist programs. They are typically unsuccessful and/or difficult to measure in terms of success.

Understanding and being aware of existing problems and ineffective strategies, including counter-narrative campaigns like the 'Think Again Turn Away' program, is important because it helps shape future campaigns and policies implemented by governmental and state actors. Additionally, it is necessary to understand the mindsets and reasoning behind extremist groups' actions before adopting a solution, proving unsuccessful for past governmental counter-extremist efforts.

Executive Branch Efforts

The Obama Administration made cybersecurity a priority and there are indications that it will also be a priority for the Trump Administration. Obama's Cybersecurity National Action Plan laid out many areas of focus, and leaked versions of a Trump Cybersecurity Executive Order offers insight into the focus of the new administration.

The Obama Administration's Cybersecurity National Action Plan

The Cybersecurity National Action Plan (CNAP) was introduced by the Obama Administration in February 2016, and it concluded its work in December 2016. It was meant to enhance cybersecurity awareness and protections, to protect privacy, to maintain public safety, as well as economic and national security, and most importantly, to empower Americans to have better control of their digital security (obamawhitehouse.archives.gov, 2016).

Based on this policy, the Commission on Enhancing National Cybersecurity was established and began working to enhance cybersecurity awareness and protections at all levels of government, business, and society, to protect privacy, and to ensure public safety (The White House, 2016).

At the same time, a $3.1 billion Information Technology Modernization Fund was proposed for transforming and modernizing government IT, as well as forming the new position of the Federal Chief Information Security Officer to drive cybersecurity policy, planning, and implementation across the Federal Government. The Obama Administration also proposed investing over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget. However, the change in administration means that the fate of these recommendations is unclear.

Predicting the Trump Administration's 2017 Executive Order on Cybersecurity

With the entrance of a new administration, the focus on counter-extremism and cybersecurity is both a continuation of the Obama Administration's Executive Order on Cybersecurity from 2016 and a slowly shifting paradigm away from former policies and recommendations of the Obama Administration. Leaked, but conflicting versions of a Trump Administration Executive Order introduce new programs and changing attitudes toward extremism, with an emphasis on countering ISIS.

Previously, the CVE was aimed at "deterring groups or potential lone attackers through community partnerships and education programs or counter-messaging campaigns in cooperation with companies such as Google (GOOGL.O) and Facebook (FB.O)" (Reuters, 2016). However, the Trump administration has floated the idea of changing the focus and name of the CVE to a more ISIS-specific program. Although not yet been determined, if implemented, this altercation could have the potential to erase former administrative sensitivity efforts to address extremism as a violent ideology, and not as a religiously affiliated entity. As a continuation of the former administration's EO, the CVE program will continue to focus on U.S. residents and radicalization at home. There has been recent conversation regarding new and improved military efforts to fight extremism online, though little to no information about this has yet been released.

In relation to education and information sharing, the Trump Administration, according to released drafts of an Executive Order, is interested in the Department of Education encouraging information sharing with the Department of Defense and the Department of Homeland Security to showcase what children are learning in cybersecurity education. Under this draft order, Defense Secretary James Mattes would be charged with making "recommendations as he sees fit in order to best position the U.S. educational system" (Starks, 2017) to keep an edge on cybersecurity. The goal is "to understand the full scope of U.S. efforts to educate and train the workforce of the future," according to the draft report. Training 100,000 cybersecurity specialists and hackers by 2020 is a possible first step, one previously suggested by former President Obama's special cybersecurity commission on cybersecurity education, prior to Trump taking office (Starks).

If the final executive order is in alignment with what Trump officials have already discussed, former White House cyber official Ryan Gillis says, “it reflects a bipartisan and nonpartisan poly arc from the Bush administration, to the Obama administration, to the Trump administration.” However, there is an added layer of complexity surrounding shifting attitudes by Trump’s Administration toward Islam as a religion, making it difficult to draw parallels to the former Obama Administration’s emphasis on using sensitive and untargeted language toward Muslim communities throughout their Executive Order pertaining to counter-extremism and cybersecurity.

Recommendation

New legislation needs to be implemented to keep the citizens of the United States safe from domestic and international threats while maintaining the integrity of their privacy. New legislation must do the following: explicitly specify what the government can and cannot do when it comes to collecting information about criminal/national security concerns that present a clear and present danger, specify the circumstances that allow for government

intervention and surveillance in these situations, and specify to what extent private companies are obliged to cooperate with government surveillance efforts. All of these should be written and ratified with cybersecurity which means that technology such as smart phones, Internet telephone services, social media messaging, and encrypted data technology, should be clearly outlined in this legislation:

Law enforcement and intelligence agencies can legally collect any and all information necessary in the interests of national or state emergency or in the interests of crime prevention, on any U.S. or non-U.S. person, if and only if the person or persons in question present a clear and present danger or have close ties to someone who presents a clear and present danger. Agencies will have to file a request to the Foreign Intelligence Surveillance Court, backed with evidence as to why they need to collect this information, who will then either deny or approve the request based on the evidence. At any point in the FISC review, industry can provide evidence in cooperation with or in contradiction to law enforcement and intelligence agencies' efforts, in courts up to and including the U.S. Supreme Court. Any violation can result in state or legal trial up to and including Supreme Court trial, where punishment may result in revoking of security clearance, removal of position, and possible fines and jail time. In regards to violation of the First Amendment it will remain the jurisdiction of courts up to and including the United States Supreme Court to evaluate each case.

Definitions

We have defined the following terms to ensure clarity and mutual understanding of our aforementioned policy recommendation, among all stakeholders:

- Clear and present danger: A precedent determined by the Supreme Court speech that is not protected by the First Amendment (i.e. shouting fire in a crowded movie theater) (Courts, U)
- Close ties: Repeated contact with a person that one may justifiably assess that the person has intimate knowledge of person presenting clear and present danger. Close ties may include, but are not limited to, relationships of marriage, blood relation, close work or mission association, and friendship. Please note that "close ties" is not justification enough to collect on someone; evidence must be presented that shows affiliation with "clear and present danger."
- Interests of national or state emergency: The federal or state government's interest in assuring that property and persons remain unharmed and information remains secured. This also entails deterrence of domestic and international terrorism.
- Interests of crime prevention: Law enforcement interest of deterring crime in their local areas. Examples are, but not limited to; murder, rape, fraud, identity theft, burglary, robbery, etc.
- U.S. person: A person who legally resides within the United States, to include legal aliens.
- Non-U.S. person: A person whose citizenship belongs to a foreign country and resides in the United States, regardless of duration of stay in United States.

Civil Society, Cybersecurity, and Government

Tae-Hyun Thomas Park

Civil society, comprised of groups of people linked by common interests in cybersecurity, is another significant key player in managing extremist use of social media. Since the term "civil society" is extensive and can be interpreted in various ways, here it refers to groups and individual activists who focus on defending individuals' rights in cyberspace. It is important to note that their interests in cybersecurity are different from the government's as these groups put more weight on privacy and individuals' rights than national security. Since the term, "cybersecurity" is vague and does not have a clear definition, it ignites conflict between the government and the people. The supporting relationship with civil organizations are crucial to facilitate effective cybersecurity strategy.

Civil society organizations are deeply involved in the government regarding cybersecurity; individual hacktivists cooperate with law enforcement for forensic investigations. Moreover, the civil groups are key players in enhancing the government's accountability regarding their cybersecurity-related policies. No matter how effective the policies the government presents, it will be challenging if the government fails to consider the public sentiment. Therefore, the government needs to create an official summit that includes industry and civil society to enhance cybersecurity discourse. In this trilateral summit, they should work towards shaping terms and policies of cybersecurity in various perspectives. Furthermore, the information of the meeting should be shared with the public to prevent further conflict or distrust that may occur between civil society and the private sector. It is important to understand where the civil organizations stand on this issue and cooperate with them to overcome any obstacles.

Civil Society's Key Role in Cybersecurity

Civil society is deeply involved in various elements of cybersecurity. Three different events illustrate the significant role of civil society in cybersecurity. The first case shows how civil society responded to the government's cybersecurity bills to defend individuals' rights and privacy. In this case, civil society groups were actively involved in the government's cybersecurity polices. They shared detailed information about cybersecurity bills with the public, and challenged the contents of the bills that conflicted with users' rights.

The second case depicts how civil society groups are directly cooperating with the government. Furthermore, it shows that their support of the government also gives them political power. In this case, individual hackers and cybersecurity groups raise their political voice by refusing to cooperate with the government.

The third case shows the most significant role of civil society regarding cybersecurity—which is providing oversight. Civil society groups found out that the government was secretly invading individuals' privacy through utilizing surveillance software. The third case highlights the important role of civil society in cybersecurity; the government does not always act in the public's best interest; therefore, there needs to be a systemic oversight.

Civil Society's Assessment of Cybersecurity Legislation

The role of civil society in defending individuals' liberty and rights is not a mere perception; its feasibility and effectiveness was vividly shown when the SOPA and PIPA bills were introduced in 2011. The protesters used various methods to fight against the bills. As a result, on January 9, 2012, over 800 non-governmental websites protested the bills (Benkler at all, 2015). Many technology companies also joined the battle and criticized the bills, but the civil society's assessment of the government's cybersecurity-related policies

alone is of great importance. While the private sector focuses on their own commercial interests in relation to the government's policies, civil society groups provide an objective assessment of the impact of the policies for the public; their focus is to defend individuals' rights.

Civil society groups focus on defending individuals' liberty and privacy on the Internet. For example, after the Cyber Intelligence Sharing and Protection Act (CISPA) was introduced in February 2013, many civil society organizations worked against the bill and worked to raise the public awareness. The bill originally purported to allow companies to share information with the federal government to prevent against network and other Internet attacks.

Civil society groups such as the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) made a statement against the bill insisting that it would violate citizens' privacy by permitting companies to share vast amounts of personal information with the government in the name of cybersecurity with little meaningful oversight (ACLU, 2012). Furthermore, the EFF criticized the bill for its ambiguity, which allowed companies to share personal information with the government with no judicial oversight (OPSAHL, 2013). These two civil society organizations successfully raised public awareness which contributed to stopping the bill.

Cybersecurity continues to rise to the surface of the government sector while public resistance and concerns are growing simultaneously. Out of 193 International Telecommunications Union (ITU) member states, 67 states including the United States have a national cybersecurity framework and computer incident response teams (Puddephatt, Kaspar, 2015). In 2015, the U.S. Senate passed another cybersecurity bill, the Cybersecurity Information Sharing Act (CISA), which allows the sharing of information on the Internet between the government and companies.

While cybersecurity issues were raised in the public and private sector, civil society organizations also joined to provide a different dimension, and help shape the discourse of cybersecurity. Global Partners Digital, a civil society group working with government and international institutions to promote human rights values online, evaluated the passed bill as a lacks public accountability.

As in the case of CISPA and CISA, civil society organizations' criticism allowed law-makers and observers to view this bill from a different perspective. Furthermore, they managed to enhance public awareness on the subject which provides a monitoring system to suppress the government's action when the bill is misused.

Civil Society's Power to Shape Government Policy

Civil cybersecurity groups and individuals are currently cooperating with individual officers in law enforcement for forensic investigations. The most current event, the Muslim ban depicted how the government's policies could backfire the public sentiment and how civil cybersecurity community responded to the government policy. On February 1, 2017, the civil cybersecurity group halted their cooperation with law enforcement agencies after the United States government decided to restrict the entry of individuals from specific nations (Uchil, 2017). A renowned Android phone hacker, Jon Saywer, who has been cooperating with the United States law enforcement claimed that he would no longer assist the agency until Customs and Border Patrol fully complies with the court's order that halted the "Muslim ban." Saywer has been formally helping individual officers in law enforcement agencies via email for forensic investigation (Uchil, 2017). Along with Saywer, another civil cybersecurity community, the Internet Engineering Task Force, raised the same concern worrying that something they coded to help with an investigation might be misused to invade individuals' privacy.

This event does not only show how civil organizations are deeply involved with the current governmental cybersecurity field, but also demonstrates the civil organizations' political power. Civil society can pursue their goals in various ways. Raising public awareness is the most common strategy, but as shown in the previous case, they can also directly challenge the government's policies by defecting their support for government agencies.

Civil Society's Current Efforts to Challenge Governmental Power

In 2015, the ACLU reported that police departments were secretly using a surveillance software created by the government funded company, Geofeedia, to monitor the public's use of social media. Subsequently, private industry responded in accordance with public sentiment. Instagram cut off Geofeedia's access to public user posts, and Facebook also took a similar action. This case suggests the significant role of civil society regarding government transparency on cybersecurity issues. The government often fails to share information with the public regarding cybersecurity, nor does the public take an interest in the subject. Therefore, civil society is responsible for observing government transparency to protect individuals' rights.

In 2014, intelligence officers in the Seattle Police Department headquarters purchased a tracking software that was created by a CIA funded company called Geofeedia. The software gives officers access to watch individuals' posts on social media like Instagram, Twitter, and Facebook. It does not only show the contents, but also detects the locations where posts are uploaded. The controversy with the software is that the police did not obtain City Council approval, nor did they inform the public about their secret use of the surveillance tool. This act violated a Seattle law that requires any City department intending to acquire surveillance to obtain City Council approval (Hertz, 2016). Police departments in

Chicago, Philadelphia, and Austin also used Geofeedia's tracking software. Furthermore, Oakland police used the same software to monitor Black Lives Matter protests from 2014 to 2015. In response to this controversial governmental online surveillance, a City Council member Lorena Gonzalez, cooperated with the ACLU of Washington to strengthen the surveillance law. In October 2016, the ACLU reported that Facebook, Instagram, and Twitter provided data access for Geofeedia's surveillance program. According to the ACLU's report, the current status of three major social network service companies' relation with Geofedia is as follows:

Instagram had provided Geofeedia access to the Instagram API, a stream of public Instagram user posts. This data feed included any location data associated with the posts by users. Instagram terminated this access on September 19, 2016.

Facebook had provided Geofeedia with access to a data feed called the Topic Feed API, which is supposed to be a tool for media companies and brand purposes, and which allowed Geofeedia to obtain a ranked feed of public posts from Facebook that mention a specific topic, including hashtags, events, or specific places. Facebook terminated this access on September 19, 2016.

Twitter did not provide access to its "Firehose," but has an agreement, via a subsidiary, to provide Geofeedia with searchable access to its database of public tweets. In February, Twitter added additional contract terms to try to further safeguard against surveillance. But our records show that as recently as July 11th, Geofeedia was still touting its product as a tool to monitor protests. After learning of this, Twitter sent Geofeedia a cease and desist letter (Cagle, 2016).

Before coming up with the report above, the ACLU of California requested records from 63 police departments in California and found out that 40% of the agencies have acquired social networking surveillance tools (Ozer, 2016). Furthermore, they found out that

the Fresno Police Department used a similar social media surveillance tool to monitor protests like Black Lives Matter movement by identifying hashtags, #Blacklivesmatter and #Policebrutality. ACLU's efforts on revealing the use of surveillance tools by the police department did not only raise public awareness but also successfully made policy changes in both the private and public sector. On October 12, 2016, Twitter suspended Geofeedia's commercial access to Twitter data in response to the ACLU's report and the public backlash. Civil society organizations do not only raise public awareness regarding individuals' rights in cyberspace, but also bring changes to both government and industry. As much as one would like to believe that the government fully abides by the law, it does not always appear that way. The case of Geofeedia shows the important role of civil society; the government can abuse and distort individuals' rights on cyberspace with an absent civil society.

Recommendation

The government is responsible for addressing cybersecurity threats, but it has been challenging for them to make the public to accept its policies and guidelines. The potential conflicts between the government and the public derives from the ambiguous concept of cybersecurity. On the one hand, the government understands and regards cybersecurity as a national security matter, on the other, it still is uncertain to the public. Moreover, both sides are not aware of who the actual enemies are on this matter. While the government is describing cybersecurity as a national security issue, civil society is challenging the notion by striving to define cybersecurity in terms of individuals' privacy. Both national security and individuals' rights are equally important. With these groups wrestling to define cybersecurity, they both provide valuable feedback to each other, creating a deeper understanding of cybersecurity discourse.

Civil society plays a key role in balancing out the government's role in cybersecurity-related policy-making. It is a misconception to assume that the government is solely

responsible for the cybersecurity issue. Without the public's participation, it is difficult to implement the government's policies. Moreover, a lack of understanding public sentiment has the potential to backfire on the government. Civil society can ease the public's adverse reaction to the government's cybersecurity policy due to their subjectivity that shows pure interest in individuals' rights. Their contribution is needed for checks and balances of the government's policies; they need to be assessed to see whether they are violating the constitution or not. As shown in the case above, the government does not always follow standard procedures. Although the civil organizations are not the ultimate decision maker, they can be utilized for assessment, and to enhance government accountability for these policies. To crackdown on the cybersecurity issue, the government and industry need to cooperate with civil society to enhance the cybersecurity awareness to the public.

To enhance the accountability of the government and facilitate cybersecurity policies without backfire from the public, expanding civil society's role in the government sector is recommended. On December 14, 2016, President Trump had a summit with the leading figures of tech industry. The CEOs of Apple, Google and Microsoft participated in the meeting. The detailed discourse of the meeting was not revealed, but according to the New York Times, the leaders mainly talked about immigration and education issues (Streitfeld, 2016). The government should hold a regular trilateral summit that includes both industry and civil society to talk about cybersecurity issues. This will help both the public and private sector to better understand the public's needs and interests in cybersecurity. Civil society will provide subjective feedback to both the public and private sector to shape cybersecurity policies that do not violate individuals' rights.

A trilateral summit must demonstrate transparency. A close relationship of civil society with the public and private sector could raise suspicions of corruption. If civil society loses its pure purpose of defending individuals' rights and begins representing government

and industry, the cybersecurity issue will be entrenched in one side and never represent the public's interests. Therefore, the public needs to have access to the meetings. The government, industry, and civil society, should all make a report of the meetings contents and results to share with the public.

Conclusion

Xingyue Yang

The rapid development of information technology has changed the way ordinary citizens, government, industries, and organizations interact with each other. As one of the main computer-mediated technologies, social media acts as an online communication platform that largely facilitates remote interaction between ordinary citizens, government, and various industries and organizations. However, its ability to reach a large number of audiences via virtual communities and networks also creates problems. In this report, we analyzed how extremist groups use social media as a tool to recruit, communicate, and quickly spread information; how different industries, government officials, and civil society have reacted to this problem; and, finally, offered our own recommendations to improve the efficiency of each group.

We began by analyzing extremist use of social media—Twitter, YouTube, and encrypted messaging applications. Extremists groups use these three tools' abilities to create and share information, attract different audiences, and further manipulate individuals as well as vulnerable populations. As a result of this analysis, we recommend developing educational programs, specifically focusing on creating social campaigns and school programs for students to raise awareness.

Along with the existing issues of extremist social media use, we also analyzed the current efforts of both private industry and government. This analysis brings to focus another issue: with the increasing extremist use of social media, how do industries and government work together to balance between private user rights and national security? In response, we discussed industry's current efforts, including policies on extremist use. With several case studies on cooperative companies and government solutions, we now realize that industry does not have enough guidance. Our recommendation was that the government should create

more clear guidelines for industry, but allow industry to continue to manage content in line with their own policies.

We discussed existing constitutional rights and government policies used to deal with extremist use of social media—particularly, by the U.S. government as well as the actions of several government agencies, including the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). Limited legislation by the U.S. government, as well as a lack of participation in private industry and cybersecurity-related current affairs creates a grey area in monitoring the extremist use of social media—creating uncertainty regarding the responsibility of government and industry. Our recommendation was that government must make processes more clearly defined and transparent in relation to collecting data on potential extremists.

We then addressed civil society, as it plays an important role in sharing information about extremist groups and encouraging ordinary citizens to get involved in tackling extremist problems. Due to its central role in balancing government power and industry motivations, we proposed that a trilateral summit be formed to create civil society oversight into cybersecurity processes.

Although the issues of extremist use of social media are multifaceted, clear guidelines from the government and increased cooperation between government, industries, and civil society can help avoid grey areas in cybersecurity policy. Such transparency would allow for better balancing of individuals' rights and national security.

References

Andrews, N., & Schwartz, F. (2014, August). Islamic State pushes social-media battle with west. The Wall Street Journal. Retrieved from http://www.wsj.com/articles/isis-pushes-social-media-battle-with-west-1408725614?mg=id-wsj

Anti-Defamation League. (2014, August 21). Hashtag terror: how ISIS manipulates social media [Advocacy]. Retrieved from http://www.adl.org/combating-hate/international-extremism-terrorism/c/isis-islamic-state-social-media.html??referrer=https://www.google.com/#.WIPa81MrLIU

Barrett, R. (2014). Foreign fighters in Syria. The Soufan Group. Retrieved February 15, 2017, from http://soufangroup.com/wp-content/uploads/2014/06/TSG-Foreign-Fighters-in-Syria.pdfhttp://soufangroup.com/wp-content/uploads/2014/06/TSG-Foreign-Fighters-in-Syria.pdf

BBC. (2013, December 16). Profile: Edward Snowden. Retrieved January 28, 2017, from http://www.bbc.com/news/world-us-canada-22837100

Bean, D. (2015, August 11). How ISIS made Twitter one of its main recruiting tools - and what can be done about it. Retrieved January 30, 2017, from http://ijr.com/2015/08/380544-how-isis-made-twitter-one-of-its-main-recruiting-tools-and-what-can-be-done-about-it/http://ijr.com/2015/08/380544-how-isis-made-twitter-one-of-its-main-recruiting-tools-and-what-can-be-done-about-it/

Berger, J. M. (2014, June 16). How ISIS games Twitter. The Atlantic Magazine. Retrieved from https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

Berger, J. M. (2015). The evolution of terrorist propaganda: the Paris attack and social media. Brookings Institution. Retrieved February 15, 2017, from https://www.brookings.edu/testimonies/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/

Berger, J. M., & Morgan, J. (2015a). The ISIS Twitter census: defining and describing the population of ISIS supporters on Twitter. The Brookings Institution, 58.

Berger, J. M., & Morgan, J. (2015b, March 5). The ISIS Twitter census: defining and describing the population of ISIS supporters on Twitter. The Brookings Institution. Retrieved from https://www.brookings.edu/research/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/

Blaker, L. (2015). The Islamic State's use of online social media. *The Journal of the Military Cyber Professionals Association*, 1(1), 3.

Breiman, L. (2001). Random Forests. *Machine Learning, 45*. doi: 10.1023/A:1010933404324

Brunson, K., Isberto, C., Karmali, N., Kim, A., & Marguleas, O. (2016). Extremist use of information and communications technology: transcending the privacy and security dichotomy. *International Policy Institute*, 14.

Business Insider. (2013, December 16). Profile: Edward Snowden. Retrieved January 28, 2017, from http://www.bbc.com/news/world-us-canada-22837100

Calamur, K., Koren, M., & Ford, M. (2015, December 3). A Day After the San Bernardino Shooting. Retrieved January 23, 2017, from http://www.theatlantic.com/national/archive/2015/12/a-shooter-in-san-bernardino/418497

Chemerinsky, E. (2017). *Constitutional law*. New York: Wolters Kluwer.

Cohen, R. (2016, July 19). Black Lives Matter is not a hate group. Retrieved from https://www.splcenter.org/news/2016/07/19/black-lives-matter-not-hate-group

Colraine, J. (2016, April 1). Encrypted messaging apps in the age of terrorism and Snowden:

savior or safe haven? Georgetown University. Retrieved from https://repository.library.georgetown.edu/bitstream/handle/10822/1040749/Colraine_georgetown_0076M_13390.pdf?sequence=1&isAllowed=y
Costly, A. (2017). A "Clear and Present Danger". Retrieved February 01, 2017, from http://www.crf-usa.org/america-responds-to-terrorism/a-clear-and-present-danger.html
Courts, U. (2017). What Does Free Speech Mean? Retrieved February 01, 2017, from http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does
Communications Decency Act of 1996, 47 U.S.C § 230
Conger, K. (2016, July 14). Microsoft triumphs in warrant case against U.S. Government. Retrieved from https://techcrunch.com/2016/07/14/microsoft-wins-second-circuit-warrant/
CNN. (2015, May 22). The Patriot Act explained. Retrieved January 28, 2017, from http://www.cnn.com/videos/politics/2015/05/22/the-patriot-act-explained.cnn
DeVos, Stephanie A. (2010). The Google-NSA alliance: Developing cybersecurity policy at Internet speed. *Fordham Intellectual Property, Media & Entertainment Law Journal, 21*(1), 173-227.
Domonoske, C. Selyukh, A. (2016, March 10). Apple Vs. The Government, In Their Own Words. Retrieved from http://www.npr.org/sections/thetwo-way/2016/03/10/469994735/apple-vs-the-government-in-their-own-words
Editors of Encyclopædia Britannica. (2016, May 25). Gitlow v. New York. Retrieved February 01, 2017, from https://www.britannica.com/event/Gitlow-v-New-York
Editors of Encyclopædia Britannica. (2016, January 19). Schenck v. United States. Retrieved February 01, 2017, from https://www.britannica.com/event/Schenck-v-United-States
Electronic Privacy Information Center. (2017). USA Patriot Act. Retrieved January 28, 2017, from https://epic.org/privacy/terrorism/usapatriot/#history
Facebook. (2016, December 5). Partnering to Help Curb Spread of Online Terrorist Content. Retrieved from http://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/
Farivar, C.. (2016, November 16). White nationalist says losing Twitter account was a “digital execution.” Retrieved from http://arstechnica.com/business/2016/11/white-nationalist-says-losing-twitter-account-was-a-digital-execution/
Ferrara, E., Wang, W., Varol, O., Flammini, A., Galstyan, A. (2016). Proceedings from SocInfo 2016: *Predicting Online Extremism, Content Adopters, and Interaction Reciprocity.* doi: 10.1007/978-3-319-47874-6_3
Flores, R. (2016, July 17). White House responds to petition to label Black Lives Matter a “terror group. Retrieved from http://www.cbsnews.com/news/white-house-responds-to-petition-to-label-black-lives-matter-a-terror-group/
Foreign Intelligence Surveillance Court. (2017). About the Foreign Intelligence Surveillance Court. Retrieved January 30, 2017, from http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court
Friedman, D. (2014, August 17). Twitter stepping up suspensions of ISIS-affiliated accounts: experts. New York Daily News. Retrieved from http://www.nydailynews.com/news/world/twitter-stepping-suspensions-isis-affiliated-accounts-experts-article-1.1906193
Gabbatt, A. (2012, May 8). Twitter sides with Occupy protesters in NY court battle over tweet history. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2012/may/08/twitter-occupy-new-york-court

Gallagher, R. (2015, June 20). Revealed: How Doj Gagged Google Over Surveillance of Wikileaks volunteer. *The Intercept_*. Retrieved from https://theintercept.com/2015/06/20/wikileaks-jacob-appelbaum-google-investigation/

Garza, A., Tometi, O., & Cullors, P. (n.d.) The creation of a movement. Retrieved from http://blacklivesmatter.com/herstory

Geuss, M. (2016, August 11). Judge tosses suit accusing Twitter of providing material support to ISIS. Retrieved from https://arstechnica.com/tech-policy/2016/08/judge-tosses-suit-accusing-twitter-of-providing-material-support-to-isis/

Giles, Courtney. (2015). Balancing the breach: Data privacy laws in the wake of the NSA revelations. *Houston Journal of International Law, 37*(2), 543.

Giuliani, R. (2016, July 17). Face the Nation [television broadcast]. Retrieved from http://www.cbsnews.com/news/white-house-responds-to-petition-to-label-black-lives-matter-a-terror-group/

Gladstone, R. (2015, April 9). Twitter Says It Suspended 10,000 ISIS-Linked Accounts in One Day. *The New York Times.* Retrieved from https://www.nytimes.com/2015/04/10/world/middleeast/twitter-says-it-suspended-10000-isis-linked-accounts-in-one-day.html?_r=1

Government Publishing Office. (1978, October 25). Foreign Intelligence Surveillance Act. Retrieved January 30, 2017, from https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

Greenberg, J. (2015, November 21). Why Facebook and Twitter Can't Just Wipe Out ISIS Online. *Wired.* Retrieved from https://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/

Greenwood, S., Perrin, A., & Duggan, M. (2016, November 11). Social media update 2016. Retrieved February 24, 2017, from http://www.pewinternet.org/2016/11/11/social-media-update-2016/# http://www.nydailynews.com/news/world/twitter-stepping-suspensions-isis-affiliated-accounts-experts-article-1.1906193

Gregory R. Firehock. (1992). PRIVACY ACT: THE INCREASED INVULNERABILITY OF INCORRECT RECORDS MAINTAINED BY LAW ENFORCEMENT AGENCIES: Doe v. FBI. *George Washington Law Review, 60*, 1509-1980.

Grocki, S. J. (2015, July 6). Citizen's Guide To U.S. Federal Law On Obscenity. Retrieved February 24, 2017, from https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-obscenity

G. Alex Sinha. (2013). NSA SURVEILLANCE SINCE 9/11 AND THE HUMAN RIGHT TO PRIVACY. *Loyola Law Review, 59*, 861-1049.

Gopalakrishnan, M. (2015, June 23). How extremists target victims on Facebook and Twitter. Deutsche Welle. Retrieved from http://www.dw.com/en/how-extremists-target-victims-on-facebook-and-twitter/a-18535705

Hamm, M., & Spajj, R. (2015, February). Lone wolf terrorism in America: using knowledge of radicalization pathways to forge prevention strategies. National Criminal Justice Reference System. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/248691.pdfhttps://www.ncjrs.gov/pdffiles1/nij/grants/248691.pdf

Hauser, S. (2016, October). Microsoft releases 2016 Corporate Social Responsibility Report. Retrieved from https://blogs.microsoft.com/blog/2016/10/18/microsoft-releases-2016-corporate-social-responsibility-report/#sm.001uy1g0n94fdhv10it133jcc36st

Homeland Security Committee. (2016). #Terror gone viral: overview of the 75 ISIS-linked plots against the west (pp. 3–15). Retrieved from https://homeland.house.gov/wp-content/uploads/2016/03/Report-Terror-Gone-Viral-1.pdf

Huss, R. B., & Simmons, R. (1976, September). Hudgens v. NLRB: Protection of Shopping Center Picketing under the Constitution or NLRA. Retrieved February 13, 2017, from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1012&context=bjell

International Association of Chiefs of Police. (2014). Twitter and violent extremism (Awareness Brief). Washington, DC: Office of Community Oriented Policing Services. Retrieved from http://www.theiacp.org/Portals/0/documents/pdfs/TwitterAwarenessBrief.pdf

Jenkins, R. (2016, August 28). Dallas police squelch critics, questions about deadly attack on officers. Retrieved from http://www.cbsnews.com/news/dallas-police-squash-critics-questions-about-deadly-attack-on-officers/

Johnson, M. (2013, January 23). The history of Twitter | socialnomics. Retrieved from http://socialnomics.net/2013/01/23/the-history-of-twitter/

Kerby, J. (2016, April 4). Here's how many people are on Facebook, Instagram, Twitter and other big social networks. Adweek Magazine. Retrieved from http://www.adweek.com/digital/heres-how-many-people-are-on-facebook-instagram-twitter-other-big-social-networks/

Kessel, J. (2014, February 6). Fighting for more #transparency. *Twitter Blog.* Retrieved from https://blog.twitter.com/2014/fighting-for-more-transparency

Kew, B. (2016, July 19). Milo suspended permanently by Twitter minutes before "Gays for Trump" party at RNC. Retrieved from http://www.breitbart.com/milo/2016/07/19/breaking-milo-suspended-twitter-20-minutes-party/

Kharpal, A. (2016, March 29). Apple vs FBI: All you need to know. Retrieved January 23, 2017, from http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html

Kisswani, N. M. (2011). The reasonable necessary for the implement of telecommunications interception and access laws. The International Lawyer, 45(3), 857–879.

Klausen, J. (2015). Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq. Studies in Conflict and Terrorism, 38(1), 2,13,18.

Klausen, J., Tschaen Barbieri, E., Reichlin-Melnick, A., & Zelin, A. Y. (2012). The YouTube jihadists: a social network analysis of Al-Muhajiroun's propaganda campaign. Terrorism Research Initiative, 6(1). Retrieved February 15, 2017, from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/klausen-et-al-youtube-jihadists/html

Law, C. (n.d.). Marsh v. Alabama. Retrieved February 13, 2017, from https://www.law.cornell.edu/supremecourt/text/326/501

Lewis, D. (2016, February 24). What the All Writs Act of 1789 Has to Do With the iPhone. Retrieved January 23, 2017, from http://www.smithsonianmag.com/smart-news/what-all-writs-act-1789-has-do-iphone-180958188/

Liang, C. S. (2015). Cyber Jihad: understanding and countering Islamic state propaganda. Geneva Center for Security Policy, 5.

Longtin, R. (2016, March 28). Apple, the FBI, and an Act from 1789: The FBI's Impermissible Use of the All Writs Act. Retrieved January 23, 2017, from http://cblr.columbia.edu/archives/13810

Lorenzo Vindino, & Hughes, S. (2015). ISIS in America. The George Washington University Program on Extremism, 23, 24.

Lucas, N. (2016, July 18). Triggered: Ghostbusters actress Leslie Jones reports Milo to Twitter. Retrieved from http://www.breitbart.com/milo/2016/07/18/ghostbuster-leslie-jones-reports-milo/

MacArthur, A. (2016, October 03). The History of Twitter You Didn't Know. Retrieved January 30, 2017, from https://www.lifewire.com/history-of-twitter-

3288854https://www.lifewire.com/history-of-twitter-3288854
Mahmood, S. (2012). Online social networks: the overt and covert communication channels for terrorists and beyond. 2012 IEEE Conference on Technologies for Homeland Security (HST), 574–579. https://doi.org/10.1109/THS.2012.6459912
Mattise, N. (2017, January 16). "We aren't born woke, something wakes us up" – maybe it's Twitter, says activist. Retrieved from https://arstechnica.com/information-technology/2017/01/twitter-was-always-awake-how-one-activist-sees-value-in-a-maligned-platform/
Meme. (n.d.) *Merriam-Webster*. Retrieved from https://www.merriam-webster.com/dictionary/meme
Meisner, J. (2013, December 4). Protecting customer data from government snooping. *Official Microsoft Blog.* Retrieved from https://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/#sm.001uy1g0n94fdhv10it133jcc36st
Microsoft. (2016, October). Privacy and data security. Retrieved from https://www.microsoft.com/en-us/about/corporate-responsibility/privacy
Milmo, C. (2014, June 22). Isis hijacks World Cup hashtags for propaganda. Independent.ie. Retrieved February 15, 2017, from http://www.independent.ie/world-news/middle-east/isis-hijacks-world-cup-hashtags-for-propaganda-30375342.htmlhttp://www.independent.ie/world-news/middle-east/isis-hijacks-world-cup-hashtags-for-propaganda-30375342.html
Missouri, U. O. (n.d.). Brandenburg v Ohio. Retrieved February 13, 2017, from http://law2.umkc.edu/faculty/PROJECTS/FTRIALS/conlaw/brandenburg.html
National Security Agency. *Understanding the Threat.* (2016). Retrieved 23rd of January, from https://www.nsa.gov/what-we-do/understanding-the-threat/.
Park, M., & Lah, K. (2017, February 2). Berkeley protests of Yiannopoulos caused $100,000 in damage. Retrieved from http://www.cnn.com/2017/02/01/us/milo-yiannopoulos-berkeley/
Pascaline, M. (2016, October 26). Terrorism in 2016: 6 biggest terror attacks around the world. Retrieved January 30, 2017, from http://www.ibtimes.com/terrorism-2016-6-biggest-terror-attacks-around-world-2437192http://www.ibtimes.com/terrorism-2016-6-biggest-terror-attacks-around-world-2437192
Pelley, S. (2014, October 5). FBI director on threat of ISIS, cybercrime [Television]. Retrieved February 15, 2017, from http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/
Pepe the Frog. (2016). In *Anti-Defamation League*. Retrieved from http://www.adl.org/combating- hate/hate-on- display/c/pepe-the-frog.html#.WLALWW8rIdV
Policinski, G. (2012, December 19). Do you have free speech in a shopping mall? Retrieved February 13, 2017, from http://www.firstamendmentcenter.org/do-you-have-free-speech-in-a-shopping-mall/
Richard Bertrand Spencer. (n.d.) In *Southern Poverty Law Center*. Retrieved from https://www.splcenter.org/fighting-hate/extremist-files/individual/richard-bertrand-spencer-0
Roberts, J. (2016, August 18). Twitter shuts down 235,000 terrorist accounts this year. Retrieved January 30, 2017, from http://fortune.com/2016/08/18/twitter-terrorists/http://fortune.com/2016/08/18/twitter-terrorists/
Ruane, K. (2014, September 8). Freedom of Speech and Press: Exceptions to the First Amendment. Retrieved February 12, 2017, from Freedom of Speech and Press:

Exceptions to the First Amendment
Rushe, D. (2011, January 7). Icelandic MP fights US demand for her Twitter Account details. *The guardian.* Retrieved from https://www.theguardian.com/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages
Searcey, D. (2016, August 4). Boko Haram leader speaks on YouTube, deepening signs of split. The New York Times. Retrieved February 15, 2017, from https://www.nytimes.com/2016/08/05/world/africa/boko-haram-leader-speaks-on-youtube-deepening-signs-of-split.html
Schwartz, F. (2016, October 20). U.S. targets would-be terrorists overseas with new ad campaign; Facebook videos aim to counter Islamic State's use of social media to lure recruits. Wall Street Journal (Online). Retrieved February 15, 2017, from https://search.proquest.com/docview/1830366294?accountid=14784https://search.proquest.com/docview/1830366294?accountid=14784
Scot, T. (2016, May 6). Milo isn't one of us. Retrieved from http://therightstuff/biz/2016/05/06/milo-isnt-one-of-us
Shalby, C., & Sreenivasan, H. (2014, August 14). How Twitter is getting it right in Ferguson. Retrieved from http://www.pbs.org/newshour/rundown/social-media-affecting-media-reports-ferguson/
SHUTTERSHOT45. (2016). "*Alt Right" Richard Spencer debates Daryle Lamon Jenkins from One People's Project* [YouTube]. RNC 2016, Cleveland, Ohio. Retrieved from https://www.youtube.com/watch?v=2_b28h5autw
Smith, B. (2016, July 14). Our search warrant case: An important decision for people everywhere. *Microsoft On the Issues.* Retrieved from https://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#sm.001uy1g0n94fdhv10it133jcc36st
Smith, C. (2017, February 13). 160 Amazing YouTube statistics (February 2017). Retrieved from http://expandedramblings.com/index.php/youtube-statistics/
Smith, D. (2015, December 1). "American Isis Twitter scene" reveals social media's power to radicalise. The Guardian. Retrieved February 15, 2017, from https://www.theguardian.com/world/2015/dec/01/isis-america-twitter-social-media-radicalisation
Solon, O., Wong, J. C., & Levin, S. (2016, November 16). Bursting the Facebook bubble: we asked voters on the left and right to swap feeds. Retrieved from https://www.theguardian.com/us-news/2016/nov/16/facebook-bias-bubble-us-election-conservative-liberal-news-feed
Stalinsky, S., & Sosnow, R. (2015). Encryption technology embraced by Isis, Al-Qaeda, other jihadis reaches new level with increased dependence on apps, software - Kik, Surespot, Telegram Wickr, Deteckt, TOR: Part IV - February-June 2015. Retrieved February 15, 2017, from http://cjlab.memri.org/latest-reports/encryption-technology-embraced-by-isis-al-qaeda-other-jihadis-reaches-new-level-with-increased-dependence-on-apps-software-kik-surespot-telegram-wickr-detekt-tor-part-iv-f/http://cjlab.memri.org/latest-reports/encryption-technology-embraced-by-isis-al-qaeda-other-jihadis-reaches-new-level-with-increased-dependence-on-apps-software-kik-surespot-telegram-wickr-detekt-tor-part-iv-f/
Sutton, K., Gold, H., & Sterne, P. (2017, February 21). Milo Yiannopoulos resigns from Breitbart News. *Politico*. Retrieved from http://www.politico.com/blogs/on-media/2017/02/milo-yiannopoulos-leaves-breitbart-news-235237
Tennessee, U. O. (2016, September 21). History of the First Amendment. Retrieved February 01, 2017, from http://firstamendment.cci.utk.edu/content/history-first-

amendment
The Camstoll Group (2016, April). Use of social media by terrorist fundraisers & financiers. Retrieved January 30, 2017, from https://www.camstoll.com/wp-content/uploads/2016/04/Social-Media-Report-4.22.16.pdfhttps://www.camstoll.com/wp-content/uploads/2016/04/Social-Media-Report-4.22.16.pdf
The George Washington University Program on Extremism. (2016). From retweets to Raqqa: the American ISIS Twitter scene. The George Washington University Program on Extremism. Retrieved February 15, 2017, from https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Twitter.pdf
The New York Times. (2016, March 21). Breaking Down Apple's iPhone Fight With the U.S. Government. Retrieved from https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html?_r=1
The Telegraph. (2012, June 18). Google removes 640 videos from YouTube promoting terrorism. The Telegraph. Retrieved from http://www.telegraph.co.uk/technology/google/9337993/Google-removes-640-videos-from-YouTube-promoting-terrorism.htmlhttp://www.telegraph.co.uk/technology/google/9337993/Google-removes-640-videos-from-YouTube-promoting-terrorism.html
The Web Harvest. *History of the FBI, Origins: 1908-1910.* Retrieved 23rd of January from https://www.webharvest.gov/peth04/20041023203658/http://www.fbi.gov//libref/historic/history/origins.htm.
The White House Office of the Press Secretary. (2016). *FACT SHEET: Cybersecurity National Action Plan.* Retrieved 30th of January, from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
The White House Office of the Press Secretary. (2016). *Executive Order -- Commission on Enhancing National Cybersecurity.* Retrieved 30th of January, from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity
The White House Office of the Press Secretary. (2017). EXECUTIVE ORDER: PROTECTING THE NATION FROM FOREIGN TERRORIST ENTRY INTO THE UNITED STATES. Retrieved 14th of February, from https://www.whitehouse.gov/the-press-office/2017/01/27/executive-order-protecting-nation-foreign-terrorist-entry-united-states.
Twitter. (2016, February 5). Combating violent extremism. Retrieved from https://blog.twitter.com/2016/combating-violent-extremism
Twitter. (2016, September 30). Twitter Privacy Policy. Retrieved from https://twitter.com/privacy?lang=en
United States. Federal Bureau of Investigation, author. (2005). *The FBI Story 2015.* Retrieved 30th of January, from https://www.fbi.gov/file-repository/the-fbi-story-2015.pdf/view.
United States. Federal Bureau of Investigation. Retrieved 23rd of January, from https://www.fbi.gov/investigate/cyber.
United States Code. (1783). All Writs Act. Retrieved January 23, 2017, from https://www.law.cornell.edu/uscode/pdf/uscode28/lii_usc_TI_28_PA_V_CH_111_SE_1651.pdf
US Congress (Ed.). (2004, May). Congressional Record, Pt. 6, April 20, 2004 to May 4, 2004 (Vol. 150). Government Publishing Office.

US House of Representatives. (1994, October 25). Communication Assistance to Law Enforcement Agencies. Retrieved January 23, 2017, from https://www.congress.gov/bill/103rd-congress/house-bill/4922/text
US House of Representatives. (2001, October 26). H.R. 3162. Retrieved January 28, 2017, from https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
US House of Representatives Judiciary Committee. (2015, June 2). USA FREEDOM Act. Retrieved January 28, 2017, from https://judiciary.house.gov/issue/usa-freedom-act/
Wallace, M., D. (2016, January 25). Remove terrorists from YouTube: column. USA Today.
Yiannopoulos, M. (2017, February 12). [Facebook] Retrieved from https://www.facebook.com/myiannopoulos/posts/845083145629582
YouTube. (n.d.). YouTube Help: Policies, safety, and reporting: Policy Center: Violent or graphic content. Retrieved from https://support.google.com/youtube/answer/2802008?hl=en
Zetter, K. (2011, February 7). Feds Subpoena Twitter Seeking Information on Ex-Wikileaks Volunteer. Retrieved from https://www.wired.com/2011/01/birgitta-jonsdottir/

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY *of* WASHINGTON

The Henry M. Jackson School of International Studies
jsis.washington.edu
Phone: (206) 543-6001 Email: jsis@uw.edu