ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

The Surveillance State & Censorship Legislation Conundrum

Dragnet Surveillance & Censorship Legislation Will Do Nothing to Eliminate Cyber Jihad & Lone Wolf Recruiting

June 2017

By: James Scott, Senior Fellow, The Institute for Critical Infrastructure Technology

The Surveillance State & Censorship Legislation Conundrum

Dragnet Surveillance & Censorship Legislation Will Do Nothing to Eliminate Cyber Jihad & Lone Wolf Recruiting

June 2017

Authored by: James Scott, Sr. Fellow, ICIT

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Support ICIT

Information should be liberated, not commoditized.

This powerful philosophy is the bedrock of The Institute for Critical Infrastructure Technology (ICIT), a nonprofit, nonpartisan 501(c)(3) cybersecurity Think Tank located in Washington D.C. Through objective research, publications and educational initiatives, ICIT is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from Advanced Persistent Threats including Cyber Criminals, Nation States, and Cyber Terrorists.

Financial capital from generous individual and corporate donors is the lifeblood of the Institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark. Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our National Security and the protection of our personal information.

http://icitech.org/support-icit/

Contents

Backdoors for the Good Guys, Means Backdoors for the Bad Guys

Cyber-insecurity is not a natural problem; it is unintentionally caused by a combination of the negligence, naivety, and ignorance of irresponsible data managers or it is intentionally resultant of the actions of malicious insiders, unknown threat actors, or reckless data stewards. Cybersecurity does not follow the laws of the physical world. For instance, the public relies on the government to protect it from or respond to floods, earthquakes, or other natural disasters. The public relies on government for defense from military excursions. Where the government cannot directly prevent or respond to a disaster, the public depends on the government to responsibly regulate protections; as is the case with building security and other regulations. Meanwhile, in the realm of cybersecurity, the public is increasingly reliant on private businesses to responsibly protect data and freedoms, even though those same organizations have repeatedly failed to do so in the past because repeated government legislative efforts critically jeopardize the security and privacy of the public. Recently, state agencies have begun initiatives to inject backdoors, weaken encryption, and exploit discovered or implanted system vulnerabilities in attempts to identify early indicators of terrorist activity, to locate and apprehend suspected criminals, and to dismantle adversarial networks or disable dangerous technology. Requirements to weaken encryption or intentionally hobble an otherwise secure application primarily impact consumers (whose data is stolen and abused) and small and medium businesses and non-profits (who cannot afford cyber-insurance or the lawsuits resulting from a breach) [1]. Further, the establishment and expansion of dragnet surveillance capabilities presuppose an intentionally permanent instability of national and global communication networks. System vulnerabilities are unanimously exploitable by script kiddies, cybercriminals, techno-jihadists, digital mercenaries, nation-state advanced persistent threats (APTs) and the agencies which introduce or require the vulnerability in the first place. Governments are thereby complicit in every attack that leverages that flaw.

The Rise of the Lone-Wolf Threat & Ease of Cyber Jihad

Self-polarized lone wolf threat actors are the new profile of terrorists (of all varieties and denominations) across the globe. Before the internet, troubled individuals often did not radicalize to the point of action because in order to do so they had to physically identify, locate, and connect with a tangible local congregation of like-minded individuals. Now on the Internet, radicalization can occur instantly and anonymously within significantly larger and more geographically distributed groups. Statistically, physical membership in hate groups has actually diminished because troubled lone wolves can instantly gratify and cultivate their radical beliefs, they can remotely plan their assaults with online resources (Google Maps, etc.), and they can consume propagandist narratives to model their campaigns around and to assure them that their purpose is worth serving and that their sacrifice will be remembered.

Lone wolf threat actors feel isolated and turn to the internet for community and purpose. Their online accounts exhibit behaviors of seeking attention, polarization, and further isolation as those that they interact with subjugate them or disagree with their adopted ideology. Once they feel that they can no longer communicate with the online communities of their past, their only outlet becomes the radicalization network which capitalizes on their seclusion and desire for attention, renown, or purpose. Social media recruitment channels and keywords, such as Twitter hashtags, can be used to track radicalization efforts or dismantled to diminish the propagation of recruitment materials. Identifying, monitoring, and apprehending recruiters, potential recruits, and radicals can preempt attacks, but it will only delay the overall campaign as no individual is indispensable to the network.

In every country targeted by self-radicalized lone wolves, Law enforcement is overexerted and under-resourced. National or global dragnet surveillance initiatives will only further exhaust agencies resources and further obfuscate adversary communiqués within a massive cloud of noise. Instead, law enforcement should concentrate on monitoring Deep Web forums and on dismantling the distribution channels and generation resources of radicalization propaganda materials. Lone wolf threat actors research, recruit, and discuss their plans, within radical online communities prior to actually launching the physical attack because, at their root, they desire recognition and a like-minded community more than they believe in their actions. These are troubled individuals who want to be remembered for something, and they often seek affirmation that someone in some online community will remember their narrative. The polarizing publications distributed on the open Internet and Deep Web contain radicalization campaigns, intended attacks blueprints, choice targets, etc. and they are pivotal in terrorist campaigns. For instance, in November 2016, ISIS's publication Rumiyah, published articles urging Western readers to utilize rented trucks and handheld weapons in multi-stage public attacks. The article included infographics and characteristics of vehicles and physical weapons to avoid. This template almost definitely influenced the London Bridge and other recent campaigns. Other publications include Kybernetiq and Dabiq. The magazines regularly include spreads detailing "hagiographies of mujahids" who died in Western assaults. The profiles appeal to vulnerable and susceptible individuals and are extremely influential in the radicalization process because they promise infamy and purpose to those who have none.

Nation-state dragnet surveillance of the open and free Internet will be more detrimental to global populations than sophisticated Intelligence and Counter-Intelligence efforts that precisely monitor and target recruitment channels. Adversaries can always find new message boards, encrypted messengers, etc. to utilize in their terror campaigns. Average citizens cannot. In fact, no national or global effort to surveil civilian web traffic can map, control, or monitor Deep Web, where most nefarious activity occurs. Even tracking sophisticated adversaries who rely on multiple jump boxes or VPNs would be difficult or impossible. Every effort that reduces

freedoms or invades privacy is in a way, a secondary adversarial victory because it is a self-inflicted social harm on the free world without significantly impeding adversarial campaigns. Radicals have little or no switching costs in their communication and recruitment mediums. It costs them nothing but time and human resources to create more Twitter accounts or set up a new Deep Web site. A greater impact can be achieved by surveilling specific communications, identifying code words, etc. than on mass surveilling entire populations and attempting to discern radical rhetoric through the noise. Instead of targeting disposable assets, resources would be more effectively spent targeting key figures and infrastructure in the propaganda machine. Consider the publications used to polarize many lone wolf actors are pretty professional. There cannot be many graphic designers or publishers within ISIL.

The retraction of civilian freedoms is a knee-jerk reaction that only benefits adversaries in the long-term because they can adapt and utilize unconventional mechanisms; whereas average civilians cannot. Even the repeated campaigns to backdoor or decrypt WhatsApp missives, if successful, would deprive citizens of private and secure messaging while adversaries could transition to Deep Web communication mechanisms or even to unconventional channels such as mobile game chat rooms. Any effort to monitor all Internet traffic or to censor particular dialogues is a dangerous slippery slope that will inevitably inflict societal harm far exceeding any transitory advantage over radical adversaries. Any and every freedom sacrificed out of fear of a threat is nothing but a concession to their cause and an affirmation that they should continue their efforts [2].

The Failed U.K. Surveillance State Will Become Weaker with Backdoors and Dragnet Censorship Legislation

Dragnet surveillance legislation has propagated in response to recent terror incidents that were catalyzed by digital propaganda and polarization mechanisms. In March, a car-and-knife attack on Westminster ended with five casualties. The May Manchester bombing killed 22 civilians. The London Bridge terror attack resulted in seven deaths and dozens of injuries following a van-and-knife assault. Following the London Bridge terror attack, May commented, We cannot allow this ideology the safe space it needs to breed – yet that is precisely what the internet, and the big businesses that provide Internet-based services provide," she continued, "We need to work with allied democratic governments to reach international agreements to police cyberspace to prevent the spread of extremist and terrorism planning." The Conservative Tories have committed wide-ranging plans to regulate the Internet in an attempt to deter digital radicalization of lone-wolf threat actors and other terrorists [3]. They believe that the digital world and the tangible world should both be delimited by the same strong rules. The believe, "Our starting point is that online rules should reflect those that govern our lives offline," and

continue, “It should be as unacceptable to bully online as it is in the playground, as difficult to groom a young child on the internet as it is in a community, as hard for children to access violent and degrading pornography online as it is in the high street, and as difficult to commit a crime digitally as it is physically” [4]. Their plan is to transform the UK into a global leader in the regulation and use of the Internet and personal data [3]. The document states “Some people say that it is not for government to regulate when it comes to technology and the internet. We disagree." Members of the party confirmed to journalists that the phrasing indicates intentions to restrict what can be shared, posted, or published online [4]. It repeatedly suggests that the government may even decide which news stories from which news sources may be published online [3]. It may also change how online firms are paid for digital content or services [4]. Prime Minister Theresa May suggested that an international agreement regulating online content was necessary to stymie terrorist ideologies and she is seeking a global commitment from technology firms and governments to monitor and regulate web traffic; especially communications. At a campaign event, she stated, “We do need to have those international agreements to control cyberspace so that terrorists cannot plan online" [3] [5]

This motion to control cyberspace follows the Investigatory Powers Act, which allows the government to compel Internet corporations to record consumers’ browsing history and to empower ministers to break WhatsApp and other message encryption. The Act requires ISPs to maintain a list of Internet users’ online visits for one year, it grants intelligence agencies more power to intercept digital communications, and it allows Police to access stored browsing history without a warrant or court order. The government is encouraging technology companies to incorporate backdoors into encryption messaging services and other secure programs even though doing so weakens the security and privacy of all other users and injects dangerously exploitable vulnerabilities into the programs [4]. Weakening encryption, installing backdoors, etc. seriously endangers customers and their data and the processes undermine business activities. Data is transitory, and the Internet is an open and shared commodity. Asymmetric regulation could destabilize global economies or incite geopolitical conflicts. International corporations or organizations that process international web traffic would be specifically impacted because their compliance with dragnet surveillance regulations violates laws in other areas where they operate. In point, without an international agreement, Internet Service Providers cannot comply with any UK initiatives that would authorize the monitoring of users on behalf of the UK government because it would break laws in other countries and incite international conflicts.

Under the Tories plan, Internet companies are subject to a levy that will fund advertising campaigns that espouse the dangers of the Internet and that "support awareness and preventative activity to counter internet harms.” The dragnet surveillance initiatives suggested by UK leadership could lead to policies that block or shut down websites and companies that

either refuse to block content or refuse to allow communications to be monitored. In a section entitled “the safest place to be online”, the manifesto justifies this level of dragnet surveillance and public chilling by claiming, "In harnessing the digital revolution, we must take steps to protect the vulnerable and give people confidence to use the internet without fear of abuse, criminality or exposure to horrific content." Overall, the regulations could lead to government censorship of the Internet similar to the Great Firewall of China. In response to an inquiry on whether she would dismiss China-style digital censorship, May stated only that she would “work with companies.” She also did not discount the possibility of shutting down Internet entities that refused to comply with instituted dragnet regulations. As a point of note, even China’s Great Firewall is regularly circumvented, and it does not prevent Chinese Deep Web communities from forming.

Establishments that refuse to comply with the Investigatory Powers Act or other privacy-invasive regulations will be subject to strict and formidable punishments. The proposal introduces a sanctions regime that enables regulators to fine or prosecute organizations that fail or refuse to execute their legal duties to remove content that is in violation of UK law. The government does not believe that the risks to consumers outweigh the potential benefits, that the invasive security measures or weakened privacy protections jeopardize citizens, or that the regulations will significantly disrupt businesses operations.

Multiple technology firms have also warned against hasty attempts to increase regulation or control of the Open Internet as a knee-jerk response to kinetic terror campaigns since the measures would substantially inhibit conventional usage and traffic and it may barely impact adversarial operations. A majority of cyberspace is controlled by private companies such as Google and Facebook. These laws would undermine that control by regulating what content can be published, where it can be posted, and in some cases, how it can be presented. For instance, the manifesto states, "We will put a responsibility on industry not to direct users – even unintentionally – to hate speech, pornography, or other sources of harm" which suggests that it may prevent search engines like Google from directing users to any adult-content. Restrictions would be placed on viewing pornographic websites and any exceptions to access that content would have to be justified and approved by ministers [4].

According to the Opens Rights Group, any approach to regulating the Internet, to monitoring communications, or to weakening encryption increases the risk to private infrastructure and public safety. The group opines that adding government controls on the content of cyberspace would do little to enhance public security and it might make future terrorist operations more difficult to detect and prevent [6]. Cyber-jihadist and other radical networks will respond to any amplified regulation or monitoring by burrowing deeper into unorthodox communication channels and Deep Web [6]. While pushing these networks into more obfuscated channels will

decrease the number of monthly recruits, as the recruitment and propaganda distribution points are technologically harder to find, there is no guarantee that it will significantly deter the dedicated “wound-collectors” who eventually develop into lone-wolf threats.

Dragnet surveillance proposals capture millions of users in a net of privacy invasions and instituted web insecurities in an attempt to catch a few elusive threats. Actions to regulate or censor the global Internet run counter to its purpose as a free and open network. Prime Minister May’s proposal ignores that many of those complicit in recent terror attacks were already known and actively surveilled by intelligence communities. Sweeping mass surveillance may only augment the noise surrounding imminent threats and increase the workload of the already overwhelmed law enforcement community tasked with identifying, monitoring, and preempting threats [7]. The goal of these proposals is to ensure that there is no “safe space for terrorists to be able to communicate online”; however, there is no evidence that such measures will significantly hinder adversarial operations more than they inhibit public privacy and freedoms [4]. In attempting to combat fake news and polarizing propaganda, the Tory manifesto “[takes] steps to protect the reliability and objectivity of information that is essential to our democracy”; however, it could seriously infringe on citizens’ rights to express themselves or to voice dissent from whomever currently leads the government. After all, who does the government intend to appoint to determine whether news stories or social media posts are reliable or objective? If ideally implemented, no political propaganda (of any party) could be spread online. The stark reality is that such subjective governance (as the monitor would likely be appointed by the controlling party) could be abused to silence political opponents as much as nonconforming citizens.

Dragnet surveillance is not limited to the UK. In Germany, authorities rely on state surveillance software, which is secretly installed on mobile phones and sends data to prosecutors. In 2016, Austrian Interior Minister Wolfgang Sobotka promoted a bill to impede terror communication networks by undermining the security and cryptographic mechanisms implemented on certain messaging applications. Austrian Justice Minister Wolfgang Brandstetter championed a similarly invasive bill. Following the Manchester terror attack, the Social Democratic Party of Austria and the Austrian People’s Party pushed for enhanced government dragnet surveillance to assuage terror threats [8]. In contrast to emerging dragnet surveillance laws in multiple countries, a European parliamentary committee pushed forward draft legislation that would protect personal privacy and ban backdoors into end-to-end encryption applications [7].

Under the Telecommunication (Interception and Access) Act of1979, Australian telecommunication service providers are required to store all users' metadata. The data are required to be encrypted and protected from unauthorized access or interference; however, the cryptographic algorithm employed and storage location of the metadata are not specified.

Consequently, massive pools of sensitive data remain vulnerable as individual service providers under-secure the information. The metadata includes Internet and communication records of public servants, critical infrastructure operators, C-level executives, diplomats, politicians, private citizens, etc [20].

On October 13, 2015, Australia passed the Data Retention Bill requiring ISPs to record the web activity of every citizen [19] [20]. The bill limited which federal government departments could access the metadata; but, some entities have attempted to bypass the legislation by requesting that the Australian Federal Police (AFP) conduct searches on their behalf. These departments include the Australian Taxation Office (ATO), the Department of Foreign Affairs and Trade (DFAT), the Department of Agriculture, the Department of Education, and the Department of Social Services. Advice to consult AFP allegedly came from the Attorney-General's Department. To their credit, AFP has declined the requests, citing "resource, compliance, and risk considerations." The access restrictions were implemented to assuage public policy concerns. Nevertheless, 61 government entities applied to be classified as enforcement agencies to gain access to consumers' metadata. At the time of this writing, none had been confirmed by the Attorney-General's Department [20].

Surveillance is Not Security

Rather than pass laws forcing companies to responsibly secure and handle data according to cybersecurity best practices and consumers best interests, governments are participating in the same reckless behaviors such as failing to secure systems and data, ineffectually detecting insider threats, and naively injecting backdoors into sensitive systems and consumer goods [7]. The US government, like every other government, has not proven itself capable of adequately secured its data and systems. In 2010, US Army Intelligence Analyst Bradley Manning disclosed three-quarters of a million documents concerning Iraq and Afghanistan. In 2013, Edward Snowden exfiltrated thousands of documents related to the NSA, GCHQ, and global surveillance, intelligence, and counter-intelligence initiatives. In 2016, the ShadowBrokers leaked, sold, and exploited tools allegedly developed by the NSA [9]. In 2017, contractor Reality Winner exfiltrated and leaked documents related to Russian military intelligence [10]. In 2017, WikiLeaks released “Vault 7”, alleging that the disclosed tools were used by the CIA to target smart TVs, mobile devices, and other IoT devices by leveraging undisclosed vulnerabilities and backdoors.

The White House recently voiced its support for a permanent reauthorization of Section 702 – a surveillance authority that monitors millions of Americans under the premise of monitoring foreigners likely to communicate “foreign intelligence information.” According to Thomas Bossart, a homeland security advisor to President Trump, Section 702 “does not permit the

targeting of Americans. The authority expressly forbids intentional targeting of a United States person for surveillance." However, critics contend that existing law permits the FBI and other federal agencies to search data collected under Section 702, for info about Americans, without a warrant or formal investigation, in cases unrelated to national security or terrorism. Bossart continues, "Over nearly a decade of rigorous oversight, no intentional abuse of the Section 702 authority has ever been identified, and the government has quickly taken action to rectify unintentional mistakes." A declassified 2011 FISA court opinion details the collection of 250 million digital communications under Section 702 that were to be retained for a default of five years. As such, opponents to 702 assert that over a billion communications may be stored on government servers and that roughly half of those files contain information about Americans. There has been a litany of cases alleging unlawful searches of Americans' information, improper conveyance of that data with third-parties, and failures to handle attorney-client communications appropriately. While the Privacy and Civil Liberties Oversight Board of the Executive branch is meant to oversee the program, both President Obama and President Trump failed to appoint nominees for its chair [11] [12].

Under Section 702, a federal court can approve and supervise the collection of foreign persons' information in foreign countries that happen to use American communication infrastructure and services. However, the Foreign Intelligence Surveillance Court approves the entire Section 702 program annually in secret proceedings. It never analyzes whether grounds exist to merit the monitoring of an individual [11]. This is akin to approving wiretappings en-masse without necessitating justification or cause per case. Consider that according to a 2016 report, in 34 years, the court approved 35,000 applications and only rejected 12 requests for foreign surveillance under the Patriot Act [13].

The intelligence agencies recently adopted a policy to limit the Section 702 Upstream program, whereby the government monitors Americans' web traffic via the Internet backbone, for data related to over 100,000 targets. However, the administration expressly reserved the right to restart the program and continue to collect information under Upstream [11].

Dragnet Surveillance Cannot Stymie Terrorism, But A.I. Can

In August 2016, a UK government committee said that Facebook, Twitter, and Google have been "failing to tackle extremism" and the Home Affairs Select Committee said the social networks need to show a "greater sense of responsibility" and they should use their earnings to help solve problems in the online world. In early 2017, Google lost millions in advertising revenue on its YouTube platform when brands boycotted in reaction to their ads appearing before or next to extremist videos. In response, Google adopted a machine learning and artificial intelligence system that utilized video analysis models that rely on content classifiers

to discover more than half of the terrorism-related content removed from YouTube in the past six months. Obviously, artificial intelligence and machine learning alone cannot detect all adversary activity nor can they perfectly prevent false positives that unintentionally remove legal user content. But the solutions better ensure security and privacy than censorship or dragnet surveillance. Artificial intelligence and machine learning systems are taught by humans to increase gradually in accuracy and efficiency.

The system is trained by operators while independent experts still respond to flagged content. YouTube was accused of hosting extremist content in the immediate backlash following the London attacks, and they have since expanded the efforts of their Jigsaw group, which points those seeking radical videos to anti-terrorist content instead. Similarly, Facebook is leveraging machine learning algorithms to identify and remove extreme content using indicators such as friend count, connections to accounts disabled for terrorist activity, or similarities to said accounts [14]. The algorithms also mine words, images, and videos to root out propaganda and messages. Hashes or digital video fingerprints are also used to flag and intercept extremist videos before that are posted. Artificial intelligence is also being used to analyze text that has been removed for supporting or praising terrorist organizations, to identify other propaganda, and to ferret out private groups that support terrorism. [15].

Rather than censor the entire Internet in an attempt to sift through the dynamically increasing pool of user data for the few extremists, state entities could leverage artificial intelligence and machine learning systems to identify potential lone-wolves prior to polarization or to distinguish shifts in the propaganda delivery channels. After all, if Facebook can implement an algorithm that identifies whether users are depressed and if so, alters their content to improve their mood, is it out of the realm of possibility for intelligence agencies to discover developing lone-wolf threat actors prior to radicalization based on their distinct profiles and redirect them to accepting communities that provide them a sense of purpose and meaning without the extremism [16]?

Adversaries Will Exploit Backdoors and Weakened Encryption

Terrorist attacks existed long before the Internet, and they will continue even if online communications are monitored and regulated. If anything, the open and free Internet encourages them to use convenient communication channels which might be actively and unknowingly monitored by law enforcement; whereas, widespread dragnet surveillance will overwhelmingly increase the noise surrounding confidential missives, and will inspire threat actors to communicate via more secure and less obvious channels or more challenging to

monitor portions of the Internet, such as Deep Web, massive multiplayer online games, single-use email clients, etc.

Governments are responsible for securing their peoples' data and for ensuring that private companies likewise secure data in transit, at rest, and during processing. Introducing backdoors into applications and systems forces data stewards to willingly undermine the cybersecurity of their systems and data. Consequently, those systems and data are at significantly greater risk of compromise from every adversary capable of discovering and exploiting the intentional vulnerability in the system. Even just weakening encryption significantly heightens the threat to consumers because otherwise, the threat actor would not be able to abuse any stolen data. Further, cybersecurity is fundamentally governed by cost-to-rewards ratios and risk assessments pertaining to adversarial investment of resources and organizational defenses. Once encryption is weakened, more adversaries will target the system because they will need less skill, time, etc. to breach the defenses and they have a greater chance of compromising the weakened encryption so that they can leverage the data in future campaigns, fraud, etc. Essentially, by requiring organizations to weaken encryption and introduce exploitable vulnerabilities into their applications based on the speculation that doing so could possibly lead to the detection of a few more kinetic assailants, governments are explicitly guaranteeing that a maximum of cyber-threat actors successfully compromise public and private sector systems and exfiltrate treasure troves of PII, PHI, IP, and other data, at a minimal cost of resources.

ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources

[1] Morozov, E. (2017). *Cyber-insecurity is a gift for hackers, but it's our own governments that create it | Evgeny Morozov*. [online] the Guardian. Available at: https://www.theguardian.com/technology/2017/may/06/cyber-insecurity-hackers-data-theft-protection [Accessed 20 Jun. 2017].

[2] Scott, J. and Spaniel, D. (2016). *The Anatomy of Cyber-Jihad: Cyberspace is the New Great Equalizer*. [online] ICIT. Available at: https://www.amazon.com/Anatomy-Cyber-Jihad-Cyberspace-Great-Equalizer/dp/1535193360/ref=tmm_pap_swatch_0?_encoding=UTF8&qid=&sr= [Accessed 20 Jun. 2017].

[3] Griffin, A. (2017). *Theresa May says she is going to regulate the internet worldwide*. [online] The Independent. Available at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/theresa-may-internet-regulation-conservatives-general-election-2017-latest-communications-facebook-a7777136.html [Accessed 20 Jun. 2017].

[4] Griffin, A. (2017). *Theresa May to shut down the internet as we know it*. [online] The Independent. Available at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/theresa-may-internet-conservatives-government-a7744176.html [Accessed 20 Jun. 2017].

[5] Griffin, A. (2017). *Theresa May says the Finsbury Park mosque attack justifies her plan to crackdown on the internet*. [online] The Independent. Available at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/finsbury-park-mosque-attack-latest-theresa-may-internet-crackdown-justification-terrorism-web-a7797281.html [Accessed 20 Jun. 2017].

[6] Griffin, A. (2017). *Theresa May's internet plans could make it easier for terrorists, campaign group warns*. [online] The Independent. Available at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/london-attack-theresa-may-internet-regulation-terrorist-networks-jihadis-surveillance-privacy-a7773021.html [Accessed 20 Jun. 2017].

[7] Lee, A. (2017). *Theresa May's crackdown on the internet will let terror in the backdoor | Alex Lee*. [online] the Guardian. Available at: https://www.theguardian.com/commentisfree/2017/jun/20/theresa-may-crackdown-snoopers-charter-encryption-terror-backdoor [Accessed 20 Jun. 2017].

[8] Aliens, C. (2017). *Austria One Step Closer to Mass Surveillance*. [online] Deep Dot Web. Available at: https://www.deepdotweb.com/2017/06/15/austria-one-step-closer-mass-surveillance/ [Accessed 20 Jun. 2017].

[9] Carberry, S. *Watchdog: NSA needs to boost insider-threat protocols -- FCW*. [online] FCW. Available at: https://fcw.com/articles/2017/06/19/nsa-insider-audit.aspx [Accessed 20 Jun. 2017].

[10] Sheth, S. (2017). *Thousands of millennials straight out of high school work for the NSA with top secret information*. [online] Business Insider. Available at: http://www.businessinsider.com/reality-leigh-winner-nsa-leak-access-2017-6 [Accessed 20 Jun. 2017].

[11] American Civil Liberties Union. (2017). *Trump, Hypocritically, Moves to Make Temporary Surveillance Powers Permanent*. [online] Available at: https://www.aclu.org/blog/speak-freely/trump-hypocritically-moves-make-temporary-surveillance-powers-permanent [Accessed 20 Jun. 2017].

[12] Bossert, T. (2017). *Opinion | Congress Must Reauthorize Foreign Surveillance*. [online] Nytimes.com. Available at: https://www.nytimes.com/2017/06/07/opinion/congress-reauthorize-foreign-surveillance.html [Accessed 20 Jun. 2017].

[13] Oliver, J. (2017). *Government Surveillance: Last Week Tonight with John Oliver (HBO)*. [online] YouTube. Available at: https://www.youtube.com/watch?v=XEVlyP4_11M [Accessed 20 Jun. 2017].

[14] Burgess, M. (2017). *Google's using a combination of AI and humans to remove extremist videos from YouTube*. [online] WIRED UK. Available at: https://www.wired.co.uk/article/google-youtube-ai-extremist-content [Accessed 20 Jun. 2017].

[15] Guynn, J. (2017). *Facebook taps artificial intelligence in new push to block terrorist propaganda*. [online] USA TODAY. Available at: https://www.usatoday.com/story/tech/news/2017/06/15/facebook-using-artificial-intelligence-to-crack-down-on-terrorism/102887032/ [Accessed 20 Jun. 2017].

[16] Ghoshal, A. (2017). *AI is our best weapon against terrorist propaganda*. [online] The Next Web. Available at: https://thenextweb.com/artificial-intelligence/2017/06/19/is-ai-our-best-weapon-against-terrorist-propaganda/ [Accessed 20 Jun. 2017].

[17] Griffin, A. (2017). *Theresa May doesn't rule out regulating the internet like China*. [online] The Independent. Available at: http://www.independent.co.uk/life-style/gadgets-and-

tech/news/theresa-may-internet-regulating-regulation-china-general-election-london-attack-bridge-a7774221.html [Accessed 20 Jun. 2017].

[18] Stone, J. (2017). *Theresa May says the internet must now be regulated following London Bridge terror attack*. [online] The Independent. Available at: http://www.independent.co.uk/news/uk/politics/theresa-may-internet-regulated-london-bridge-terror-attack-google-facebook-whatsapp-borough-security-a7771896.html [Accessed 20 Jun. 2017].

[19] Nagy, B. (2017). Metadata: Australia's Cyber 'Sitting Ducks'. [online] The Diplomat. Available at: http://thediplomat.com/2017/02/metadata-australias-cyber-sitting-ducks/ [Accessed 24 Jun. 2017].

[20] Sveen, B. (2016). Data Retention Bill: Government departments ask AFP to access metadata after legislation enacted - ABC News (Australian Broadcasting Corporation). [online] Mobile.abc.net.au. Available at: http://mobile.abc.net.au/news/2016-10-04/government-departments-obtain-metadata-via-afp/7898648?pfmredir=sm [Accessed 24 Jun. 2017].