Athens Journal of Law - Volume 2, Issue 4 – Pages 211-224

The "Right" to Privacy? - The Debate over the United States Government's Control over its Cyberspace[1]

By Emanuel G. Boussios[*]

This research note centres on a critical issue in the United States, that is, in the name of anti-terrorism the state utilises sophisticated cyber-surveillance machinery to protect its citizens' while at the same time promising to protect their civil liberties. The examination here of this issue seeks to go beyond the dichotomy of 'liberty vs. security' but to how open the United States government should be about its cyber-intelligence capabilities and how these apparatuses are possibly infringing upon its citizens' freedoms. The freshness of the controversy stems from Edward Snowden's claims the U.S. government (and its Allies) acted criminally by aiding and abetting its own agents to collect information on its populace in the absence of lawful means. This case has brought a range of legal and ethical questions on democratic states' cyber-intelligence gathering including calls for legislation to directly deal with 3 key issues: reduced privacy, increased government secrecy, strengthened government protection of special interests. This research will further discuss the demands of cyber-intelligence reforms put forth by Edward Snowden and whether these demands are in fact practical in modern, high-technology societies such as the United States.

Keywords: *Cyber-intelligence, Cyber-terrorism, Homeland Security, Surveillance, Privacy*

Introduction

This research oscillates around a crucial issue in the United States stemming from the activity of the state-owned or state-controlled entities overseeing our activity in cyberspace in an effort to protect against terrorists, while at the same time, promising to protect their civil liberties. Of course this political discourse lends itself to an important debate internationally, but in this paper it will be more narrowly discussed in the context of the current debate being held in the United States. Most recently, President Barack Obama signed into law the highly contentious Cybersecurity Information Sharing Act of 2015 (CISA). The CISA, craftily placed *within* the 2016 spending bill, encourages businesses and the federal government to exchange cyber threat information in the interests of national security. Privacy advocates, such as the ACLU, view the CISA's inclusion within the 2016 spending bill as "sneaky backdoor politics," since, by design, this minimises debate on the Act's very details,

[*] PhD Visiting Scholar New York University, Assistant Professor SUNY- Nassau Community College

[1] The author expresses much appreciation to the Faculty Resource Network (FRN) for the opportunity given to Dr. Emanuel G. Boussios to conduct this research at NYU New York.

https://doi.org/10.30958/ajl.2-4-1 doi=10.30958/ajl.2-4-1

while The White House justifies the CISA's passing as a necessary "victory at all costs" measure given the existential threats of cyberattacks[1]. There are too many critical issues to be covered in one paper, but the core of the debate is on the constitutionality of state actions,[2] and the shifting boundaries in which the state can act in the name of *security*[3], in an effort to protect its people—and hence the nation-state— from its enemies. A second piece of this debate is which state actors and agencies can control the mechanisms by which this sensitive cyber information is collected, stored, and if needed, acted upon. The most salient case in regards to this debate is that of Edward Snowden revealing the U.S. government's abuses of this surveillance machinery. Snowden claims the U.S. government (and its Allies) acted criminally by aiding and abetting its own agents in *collecting information* on its populace in the absence of lawful means (i.e. proper warrants), and more specifically infringing upon the privacy of its citizens, business, and even politicians by the use of deep packet inspection, and smartphone location tracking.. Although this case is far from its legal conclusion (Snowden, as of this writing, is still in asylum in Russia), it has brought a range of legal and ethical questions concerning democratic states' cyber-intelligence gathering. Edward Snowden's revelations in June 2013 prompted major debates around the topics of privacy, national security, and mass digital surveillance. This paper will discuss cyber-intelligence reforms put forth by Edward Snowden and whether this is in fact practical in modern, high-technology societies such as the United States.

The debate of states' use of surveillance in the name of security is not unique to American society or even to ancient city-states. For example, the use of spies by government agents to counteract insurgencies has been the norm, a tactic used by leaders of the earliest nation-states. For many the history of surveillance can be traced back to antiquity[4]. For example, in medieval Europe a feudal lord could keep watch over his domain from the top of his watchtower, while for others an emphasis on the visual represents the very essence of modernity[5]. According to Fussey "while the development of administrative

[1] According to Penton and Singh (2015), "Cyberattacks are increasingly exponentially in the United States and around the world. Attacks in the United States in averaging over 550,000 a week and over 25,000,000 a year."

[2] In the United States, there are several Amendments that constitute an American citizen's right to privacy. The First Amendment which is held upon privacy beliefs – "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." The Third Amendment which states privacy within the home –"No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." Lastly, the Fourth Amendment which holds privacy of the citizen and their possession –"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[3] According to Griffin (2016) 50), "Trawling the internet for information about people is a seizure under the Fourth Amendment."

[4] Sennet (1990).

[5] Heidegger (1977).

surveillance has been viewed not simply as a mere feature of modernity, but as an enabling mechanism that has facilitated its development."[1] Despite its long history in civilised society, the very existence of surveillance has been viewed by many as a social problem due its ease of abuse by government and its agents. Several scholars[2] have suggested that one way of explaining this is that while surveillance has always been present, it has not always been a mechanism of control. Current public discourse on surveillance in Western societies, including the U.S. and the UK, is about the *encroaching* nature of this form of social control. According to Griffin[3] , "Alas, America has become a surveillance state." Public opinion in both the U.S. and U.K. has indicated that an overwhelming majority of the citizenry consider government surveillance of the *public's internet communications and telephone*, to be an important issue[4]. The EU and UK public think some surveillance technologies are effective and should be used in combating national security threats, and should be used, but acceptability varies according to whether the surveillance is of communications or bodies, blanket or targeted. It is common practice for government security agents to use all of these surveillance technologies. Surveillance of physical bodies (smart CCTV[5]) and targeted surveillance of digital communications (smartphone location tracking) are more accepted by the public than blanket surveillance of digital communications (deep packet inspection)[6].

Literature Review

Over the last several decades, most Western societies have seen a tremendous advancement in technology (progressing far beyond the simplicity of CCTV's) and a tremendous increase in the actual use of surveillance. With computerisation, surveillance is becoming more subtle and, at the same time more intense, spreading from material space to cyberspace. Scholars have argued[7] that the real 'superpanopticon' exists in electronic environments – in the 'wordwide web of surveillance.'

Most individuals in Western nations have accepted the fact that they are being observed in some capacity in public spaces, but would be surprised to know that information is being collected in the public and the "private" realm

[1] Fussey (2008).
[2] Fussey (2008).
[3] Griffin (2016) 38.
[4] Madden (2015).
[5] CCTV's features digital cameras which are linked together in a system that has the potential to recognise people's faces, analyse their behaviour and detect objects. Deep packet inspection detects and shapes how messages travel on a network. It opens and analyses messages as they travel, identifying those that may pose particular risks. Smartphone location tracking analyses location data from a mobile phone, to glean information about the location and movements of the phone user over a period of time.
[6] Bakir et al (2015).
[7] Lyon (2001)

and what is being done with that information. There are three general security-oriented technologies, each with its own mechanism of surveillance: smart-closed circuit television (CCTV), deep packet inspection, and smartphone location tracking[1]. Recent controversial Supreme Court rulings have reset the boundaries of the government's power in regards to deep packet inspection and smartphone location tracking[2]. According to Hunton and Williams[3] surveillance practices "pervades all societal sectors that stretch 'well beyond the state'; surveillance is a fact of modern life and not intrinsically anti-social or repressive". According to Lyon[4], surveillance societies are defined by their double-edged character; surveillance technologies can be used to provide benefits, empower consumers and workers and enable the promotion of citizenship rights[5]. Traditionally, privacy has been used as a counterpoint to resisting and challenging surveillance but others argue a post-privacy[6] challenge to surveillance exists that addresses the latter as a social question to do with power. Yet, cyber *in*security affects all, and "raises collection, storage, and release questions… when one writes, edits, drafts, and emails stuff, the pile has to be stored somewhere. Surrendering information to a trusted third party erases privacy"[7].

Discussion

This paper examines what is perhaps the most commented upon and certainly the least visible form of technological surveillance in modern society—that of cyber-surveillance. The examination of the cyber-surveillance debate in this paper seeks to go beyond the dichotomy of 'liberty vs. security'[8]

---

[1] Bakir et al (2015).

[2] Hunton and Williams (2014). On June 25, 2014, the United States Supreme Court issued a unanimous opinion in *Riley v. California*, holding 9-0 that law enforcement personnel cannot search detained suspects' cell phones without a warrant. On February 26, 2013, the United States Supreme Court decided in *Clapper v. Amnesty International* that U.S. persons who engage in communications with individuals who may be potential targets of surveillance under the Foreign Intelligence Surveillance Act ("FISA") lack standing to challenge the statute's constitutionality.

[3] Hunton and Williams (2014).

[4] Lyon (2001).

5 Lyon's point here is that surveillance can also be less concerned with 'care' and more with 'control.' Surveillance plays a coordinating role in aiding an individual's passage through the shopping mall, customs or the workplace. This coordination process is more and more being defined by a risk calculus, which is increasingly taking on an amoral character – less concerned with inclusiveness and questions of justice.

[6] Power and surveillance have a complex social relationship; not always to be characterised in oppressive terms in that 'few people feel constrained, let alone controlled, by surveillance regimes' (*See* Lyon (2001) 7). However, surveillance effects 'life chances and social destinies' in forming a kind of 'superpanoptican' (*See* Lyon (2001) 151) whereby surveillance societies can only be understood in recognizing how ideologies and beliefs 'underpin' the work of organizations and, therefore how they use surveillance technologies.

[7] Griffin (2016) 39.

[8] Fussey (2008).

to discuss how open the United States government should be about its cyber-intelligence capabilities and how these apparatuses are possibly infringing upon its citizens' freedoms. This debate is hardly new, however, the freshness of the controversy stems from legislation introduced in response to 9/11; Homeland Security Act (HSA) of 2002 and Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Cyber policy is highly contentious— the contest of security vs. privacy, the public good vs. corporate profits, interagency power struggles, budget fights, and the "simple" matter of setting daily priorities in a 24-hour day—all enter into and complicate issues that appear cut-and-dry at first glance. As of this writing, the discourse surrounding cyber-intelligence gathering[1], includes the controversial Cybersecurity Information Sharing Act and the Cyber Intelligence Sharing and Protection Act[2]. Each piece of legislation further exacerbates three conditions in the United States: reduced privacy; increased government secrecy; strengthened government protection of special interests[3]. The Cybersecurity Information Sharing Act (CISA) was packaged within the $1.1 trillion spending package that Congress passed in late 2015. The CISA will significantly reshape the relationship between the consumer, company, and government and how such data is collected and stored. These are some of the more significant changes with the passing of CISA[4]: sharing of cyber threat information by the federal government[5] cybersecurity best practices guidance[6], immunity; sharing of cyber threat information by businesses;[7] and privacy protections.[8] The

[1] Other such debates, on intelligence gathering, can be seen in the discourse surrounding ID cards (in particular for illegal immigrants) and even public camera surveillance.

[2] Both laws would similarly provide for the sharing of certain cyber threat intelligence and information (i.e. Internet traffic information) between the U.S. government and technology and manufacturing companies.

[3] Talamian (2008).

[4] Hoffman et al (2016).

[5] CISA broadly authorises the federal government to share, among federal agencies as well as businesses and the public, unclassified "cyber threat indicators" and "defensive measures" – technical data that indicates how networks have been attacked, and how such attacks have been successfully detected, prevented, or mitigated (collectively, "cyber threat information"). Classified cyber threat information, in contrast, may be shared outside the government only with entities that have appropriate security clearances.

[6] CISA requires the federal government to release periodic "cybersecurity best practices" that are tailored to the particular challenges faced by small businesses.

[7] CISA enables businesses to share cyber threat information with seven specified federal agencies. These agencies include the Department of Defense (including the NSA) and the Office of the Director of National Intelligence, as well as the Department of Homeland Security. Businesses will also enjoy immunity from any lawsuit that may arise out of such sharing. However, CISA also provides that sharing of cyber threat information with the federal government will not constitute the waiver of any applicable provision or protection provided by existing law, including trade secret protection.

[8] To address privacy and civil liberty concerns, CISA requires that the federal government retain, use, and disseminate cyber threat information in a way that protects any personally identifiable information contained within cyber threat indicators from unauthorised use or disclosure. Businesses are required to develop "technical capability" to assist in the identification and removal of personal information. It remains to be seen how this scrubbing requirement may be implemented in light of the inherent difficulty in efficiently and quickly

"immunity" provision both raised the concerns of privacy advocates and was viewed as essential to enabling the sharing of cyber threat information with the government by businesses. Privacy advocates have expressed alarm with the CISA in allowing businesses to monitor their information systems and all information stored on, processed by, or transiting the information system, as long as the monitoring is for the "purpose" of protecting the information or information systems. Since liability protections were of significant concern to businesses, the law is protective by granting businesses full immunity from government and private lawsuits and other claims that may arise out of CISA-compliant monitoring in which businesses may engage.

Much of the criticism of this Act (i.e. the ACLU) has been has been that privacy has been compromised given the NSA's expanded powers, while others, including The White House, feel it is a well-struck balance between the nation's need for cyber intelligence and defines, and privacy.

Proposed legislation such as the proposed Federal Computer Security Act of 2015, has taken federal oversight even further. The claim put forth by two prominent American lawmakers, Sens. Orrin Hatch and Tom Carper, is that several cyber-attacks on government agencies and organizations— including the IRS data breach, in which hackers stole the detailed tax-return information of over 100,000 U.S. citizens—have exposed "substantial vulnerabilities" within the federal government's database infrastructure[1]. This Act, currently under consideration in Congress, would direct the Inspector General of each executive agency that operates a federal computer system to submit reports on the security practices and software used by their respective federal agencies to safeguard classified and personally identifiable information. It would also require that the Government Accountability Office provide a report, including a financial analysis, on any impediments to agency use of effective security software and security devices. One of the most significant criticisms of this legislation is that oversight is largely limited to the executive branch, thereby bypassing Congressional oversight.

The Debate over the Public's Interest

Arguments over cybersecurity tend to be highly contentious and political wrangling over legislation is common. Marc Rotenberg, president of the privacy nonprofit EPIC, and renowned cryptographer Bruce Schneier both depict the history of the threat of cyberwar as one of 'continuous exaggerations' by the U.S. government'[2]. The suggestion is that the real threat comes from the efforts of agencies like the NSA to control the Internet, and big contracting firms looking for their share of the cybersecurity defines budget. Mike McConnell, former director of the NSA disagrees, arguing that the U.S. economy is enormously and increasingly vulnerable to cyber threats, and that

parsing personal information from large data sets that may contain relevant cyber threat information.

[1] Hatch, Carper Introduce Federal Company Security Act (2015).

[2] Farrell (2014).

the government needs to keep many of its countermeasures secret if it is to protect against these threats[1]. Undoubtedly, the extent of such (mass) surveillance has led to significant abuses of power, unfettered by the normal system of checks and balances. The extent of surveillance is not just limited to the federal government protecting against cyberattacks[2]. 'Open' internet advocates are highly sceptical that there is any real likelihood of attack[3]. Instead, they see the real risk as coming from a U.S. security establishment that wants limitless power to gather information and restrict individual freedoms. Security advocates depict open Internet advocates as dangerously naive, while open Internet advocates see security advocates as sinister power grabbers.

Snowden and the Debate over U.S. Cyber-Intelligence

In one of the most significant cybersecurity events in recent history, former NSA contractor Edward Snowden shared thousands of classified NSA documents with journalists Glenn Greenwald, Laura Poitras and Ewen MacAskill[4]. This ongoing disclosure of leaked documents has fuelled debates over mass surveillance, government secrecy, and the balance between national security and information privacy since it has revealed previously unknown details of a global surveillance apparatus run by the United States' NSA in close cooperation with Australia (ASD), the United Kingdom (GCHQ), and Canada (CSEC). For making these disclosures, Edward Snowden has been called a hero, a patriot, a whistleblower, a dissident, and a traitor. By Snowden revealing the surveillance techniques and a depth of information gathering by Western governments on its citizens, which was indeed staggering[5].

What we have come to know about these disclosures is that the NSA, working closely with the private sector, has been monitoring citizens' web activity and has collected massive quantities of data on email and phone contacts[6]. The National Security Agency acquired its name officially on 4 November 1952 and since that time this organization has endured much

[1] Farrell (2014a).

[2] The federal government retains an influence through its brokerage of advice and provision of funding to local jurisdictions. This can occur in a number of ways, such as setting policy objectives for local authorities (such as an obligation to tackle burglary, even if this has not been highlighted as a problem locally (*See* Fussey, 2008) or providing 'expert knowledge' of solutions to local problems. These are largely disseminated in the form of a series of crime-reduction 'toolkits' for a range of different issues faced by partnerships (*See* Fussey, 2008). Such toolkits include the use of CCTV's in suburban communities in combination with well-known neighbouring monitoring programs including NeighborHood Watch.

[3] Farrell (2014).

[4] Mass (2013).

[5] Jewkes (2015). "Among Snowden's revelations were that the NSA, together with the British Intelligence Agency GCHQ, collected the phone records of millions of citizens, accessed and collected data from Google and Facebook accounts via a program called Prism… carried out offensive cyber-attacks and infected more than 50,000 computer networks worldwide with malware designed to steal sensitive information, shared raw intelligence data with Israel in an information sharing agreement, bugged offices of the EU…"

[6] Scheuerman (2014).

controversy in an attempt to protect American communication systems, primarily those of the U.S. armed forces[1]. One such controversy was over the offshoot of the warrantless domestic spying program created by the Bush administration after 9/11. These NSA's initiatives were kept out of the public eye until the *New York Times* revealed them in December 2005. In spite of this revelation, Congress responded by indemnifying the big telecommunications firms that had cooperated with the NSA, effectively giving the agency a green light to continue with secret surveillance[2], leaving one to wonder what type of "agreements" were made outside of the public eye. It was the later efforts, such as the PRISM data mining program, that Snowden revealed in 2013.

By involving parties in the press and the government, Snowden said he hoped to serve the public interest: bringing attention to privacy issues while also mitigating security risks. His personal motivations[3] for leaking the NSA documents, Snowden said, was motivated more by "self-interest" than altruism, as he felt that he would improve societal wellbeing by revealing and ultimately dismantling the NSA's metadata collection programs[4]. Several scholars agree that "In the name of privacy or, put more succinctly, a deeper concern for the turf allotted to privacy, government should dump its bulk telephone meta-data about us."[5] Snowden added that he feels there are moral obligations to act when the law no longer reflects the morality of the society it governs. Snowden recommended two major policy changes: ending mass surveillance and better protecting whistleblowers[6]. On the first point, Snowden cited the

[1] The Central Security Service was established in 1972 to promote a full partnership between NSA and the cryptologic elements of the armed forces. NSA/CSS is unique among the U.S. defines agencies because of our government-wide responsibilities. NSA/CSS provides products and services to the Department of Defense, the Intelligence Community, government agencies, industry partners, and select allies and coalition partners. In addition, we deliver critical strategic and tactical information to war planners and war fighters. By its very nature, what NSA/CSS does as a key member of the Intelligence Community requires a high degree of confidentiality. Our Information Assurance mission confronts the formidable challenge of preventing foreign adversaries from gaining access to sensitive or classified national security information. Our Signals Intelligence mission collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations. This Agency also enables Network Warfare operations to defeat terrorists and their organizations at home and abroad, consistent with U.S. laws and the protection of privacy and civil liberties. See Scheuerman (2014).

[2] Scheuerman (2014).

3 In an interview with Edward Snowden, Perry and Taylor asked whether Snowden was reluctant to "break the law," here is an excerpt of Snowden's responses: "When legality and morality begin to separate, we all have a moral obligation to do something about that," he said. "When I saw that the work I was doing and all my colleagues were doing [was] being subversive not only to our intentions but contrary to the public's intent, I felt an obligation to act." Snowden spoke at length about the institutional failures in the U.S. government that allowed for the NSA activities in question to occur. "The courts were frozen out, the majority of Congress was frozen out, the populace was frozen out," he said. He added that he attempted to reintroduce this system of checks and balances—which failed in the case of the NSA—in his own methodology for releasing the documents.

[4] Xu (2015).

[5] Griffin (2016) 40.

[6] Jewkes (2015).

"ineffective" nature of surveillance projects and the ineffectuality of the NSA's data collection in producing any improvements in security. On the second point, he argued for the creation of independent agencies staffed by civil liberties advocates to handle cases like his[1].

Snowden's demand for ending mass surveillance is not practical especially in modern high-tech societies. An analogous situation may be occurring with the use of CCTV surveillance in urban communities. According to Jewkes[2] "some studies examined whether visual surveillance technologies such as CCTV were effective in cutting crime or whether they simply displace it to surrounding areas." The net result is that ending mass surveillance could increase cybercrime in these nations (displacement), thereby increasing public fears about personal safety. In addition in this current Internet age, ending mass surveillance could leave a nation open to massive cyberattacks, crippling its infrastructure and thereby undermining the nation's security. Eliminating mass surveillance as suggested by Snowden may induce a net negative result of absorbing displaced cybercrime from neighbouring communities/nations that utilise mass surveillance.

Advocates of stronger cybersecurity warn that we are at risk of a "digital Pearl Harbor"[3] in which the U.S. power system, financial system and other parts of "critical infrastructure" could be attacked and seriously damaged by foreign hackers. In one such occurrence, a cyber-attack on the Office of Personnel Management resulted in 21.5 million federal-worker personnel records being stolen by hackers[4]. Some within the U.S. government think that deterrence [strategy against cyberattacks] is feasible, and face a dilemma[5]. The U.S. government would like to get everyone to believe that it has strength and depth in cyber-offense, so that it can deter others from attacking it[6]. This means means that the most that the United States can do to deter attackers is to deny them any benefits from attacking (what deterrence theorists call 'deterrence through denial'), creating strong defences that minimise the likelihood of successful attacks and hence slightly discourage attackers from trying to breach systems in the first place[7] (Farrell, 2014). Yet, the U.S. does not want to provide any *detail* about its capabilities i.e. be more transparent in its cyber-intelligence activities. If you have some idea of what a country's cyber weapons look like, you can defend yourself much better against them[8]. Because the U.S. can only talk in vague generalities about its capabilities, other states might think that it is deliberately inflating them for show (i.e. a form of 'game theory' strategy). The U.S. is obviously technically sophisticated and spends a great deal of money on cybersecurity. The President's Fiscal Year (FY) 2017 Budget seeks to invest over $19 billion for cybersecurity, and

[1] Jewkes (2015).
[2] Jewkes (2015).
[3] Farrell (2014a).
[4] Harch, Carpe Introduce (2015).
[5] Farrell (2014).
[6] Farrell (2014).
[7] Farrell (2014).
[8] Farrell (2014).

represents a more than 35 percent increase from FY 2016 in overall Federal resources for cybersecurity[1] (Fact Sheet: Cybersecurity, 2016). Even so, opponents may underestimate these capabilities. On the same point, the U.S. is mute on its offensive capacities in cyberwarfare. This is not an accident; and most U.S. senior officials have been only slightly more forthcoming. Other scholars disagree on the effectiveness of deterrence, and the need for this type of strategy. According to Farrell, "it [current operations] reflects the U.S. belief that traditional deterrence *does not* work in cybersecurity, and if it did, then the United States would gain benefits by publicizing how effective their weapons were and hence making it clear that the United States had a strong retaliatory capacity." Since U.S. officials believe that deterrence *does not work*, they are reticent in describing their attack capabilities. Explicit description could have many downsides (encouraging other states, for example, to arm up in cyberspace too), and few obvious upsides. While the United States does have strong offensive capacities, it sees no good reason to publicise them. Although this is understood and deemed necessary by the general public for very brief time periods during war, this fails to gain the confidence among the American public that abuse is *not* being taken place during times of peace.

Perhaps it is not necessary to end mass surveillance, or even to be more transparent on its cyber-intelligence operations, but it is essential to have greater accountability over these operations. This is attainable in a functioning democracy and would go to great lengths in better protecting the American public from illegal government overreach and do better in gaining the public's trust. Accountability is critical in gaining the confidence of the public and "checking" against abuse (i.e. checks and balances). In governance, accountability has expanded beyond the basic definition of "being called to account for one's actions"[2]. "[…] It is frequently described as an account-giving relationship between individuals, e.g. "A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them, and to suffer punishment in the case of eventual misconduct".[3] Accountability cannot exist without proper accounting practices; in other words, *an absence of accounting means an absence of accountability*.

It is important to note that given the range of cyber threats, this could have necessitated the current U.S. cyber-security arrangement. The main actors of this arrangement include the Department of Homeland Security (a civilian government role), the National Security Agency and Cyber Command (a military role), and the FBI[4]. Just as the culture and turf wars between these different organizations are difficult to manage, as one could imagine a comprehensive oversight arrangement is indeed difficult to arrange. Yet the

[1] Fact Sheet; Cybersecurity Plan (2016).
[2] Mulgan (2000).
[3] Schedler (1999).
[4]Gardiner and Mallicoat (2014)."The DHS monitors cyber operations to warn or alert about intrusions and coordinating response, the NSA and CC (under the Department of Defense) is responsible for protecting cyberspace in terms of security/cyberwar and works with DHS and the private sector to support cyber critical infrastructure, and the FBI is responsible for investigating cyberattacks against the public."

status quo allows for a mostly ineffective systems of checks and balances (within branches of government as well) to remain in place and the chance of continuous government overreach remains an immediate threat.

There is no doubt that some of the concern is because of the secrecy surrounding the government's cyber security initiatives. More specifically, a case occurred with the Bush Administration and the Department of Homeland Security releasing limited information about the cyber security measures they were taking—including its well-known use of Einstein 3[1] which was considered an excessive and illegal use of deep packet inspection by these agencies. In addition, problems exist here today whereby most of the details of the initiatives remain classified, generating continuing Congressional and public concern about overreaching[2]. Without explicit accountability laws in place, what are the constraints placed on the executive branch in carrying out its cyber protection responsibilities? Regular reviews of cybersecurity programs could help alleviate concerns about privacy and overreach. One such proposal recommends that cyber security programs be subject to regular Congressional reviews and also be required to publish regular reports, in unclassified form, about the status and recent actions under the deep packet inspection programs[3] such as Einstein 3. These cybersecurity programs could also undergo periodic legal review by independent experts with appropriate clearances to ensure that constitutional and statutory constraints are being followed much like the Federal Trade Commissions' authority to regulate corporate cybersecurity[4]. Similar to these suggestions is the report put forth by the Sans Institute[5] recommending is that if significant discrepancies are found, these reviewers would have the authority to temporarily stop the programs in question, or at the minimum, convene meetings with the officials overseeing these programs. These reforms would better enable these critical bi-partisan committees on intelligence, the House and Senate Select Committee on Intelligence, enhanced access to certain information. Improving such access would arm these committee members, for instance, with the ability to comb through covert action and activities information which the executive branch can currently restrict "as needed."

Conclusions

Edward Snowden revealed a wide range of concrete evidence showing the scope and the scale of cyber-surveillance in the West. Although the U.S. arguably is the most technologically advanced society in the world and people living in less high-tech prone places may expect that the eye of the Big Brother to be less digitised, the debate centres on the magnitude of activity of the state-

[1] Chi (2014).
[2] Chi (2014).
[3] Chi (2014).
[4] Stempel (2015).
[5] Chi (2014).

owned or state-controlled entities overseeing our activity in the World Wide Web. 'Open' internet advocates are highly sceptical of the likelihood of crippling cyberattacks, rather they see the real risk as coming from a U.S. security establishment that wants limitless powers to gather information and restrict individual freedoms. In contrast, security advocates see open Internet advocates as dangerously naïve in a world in which the risk of a digital Pearl Harbor is imminent.

Ending mass surveillance could open Americans to blunt and constant cyberattacks, however, shunning the moral and legal responsibility of checks and balances would give the appearance of totalitarian governing practices. There was heated debate in Congress over the Cybersecurity Information Sharing Act of 2015 (CISA). This act strongly encourages business and the federal government to share cyber threat information in the interests of national security. Although the heated exchanges over this legislation was welcomed, what was troubling to many (including the ACLU) was this bills' inclusion into the 2015 Capitol Hill spending bill, perhaps as an effort to *bypass* any additional dialogue over the bills' privacy protections. In consolation to some, the CISA requires the Attorney General and the Secretary of Homeland Security to jointly submit to Congress interim CISA policies and procedures by February 16, 2016, and publish final policies and procedures by June 15, 2016[1]. Since these policies and procedures are subject to Congressional reviews, this allows for needed dialogue over the necessities of such policies and whether they are excessive. It would appear that the political wrangling in Washington over the Cybersecurity Information Sharing Act and the Cyber Intelligence Sharing and Protection Act is suggestive of a passionate debate over governments' responsibility to be the moral authority in cyberspace, at the same time, have branches of government be more involved in keeping government security agents accountable for their actions[2]. The debate does not end here however. There are amendments needed on current laws regarding corporate cyber-laws over the ownership of consumers' data. The legal tug-of-war between Apple Inc. and the US government is one example of the need for such legislation. The conflict began with the FBI's attempt to use legal motions and public pressure to force Apple to write new software allowing this agency to access the iPhone used by one of the shooters in the December 2015 mass murder in San Bernardino. The debate, however, over who *owns* the data of individuals US citizens—corporations or the government— is still in its infancy.

Acknowledgements

The author thanks Jeff Goodwin of New York University and Theodore M. Roussis of Stony Brook University for their contributions to this research note.

[1] Hoffman et al (2016).
[2] The Supreme Court is due to litigate the CISA Act; Davis (2016).

References

Bakir, V., Cable, J., Dencik, L., Hintz, A. & McStay, A. (2015) . "Public Feeling on Privacy, Security and Surveillance." Retrieved from: http://sites.cardiff.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf.

Chi, M. (November 12, 2014). "Cyberspace: America's New Battleground," Retrieved from https://www.sans.org/reading-room/whitepapers/warfare/cyberspace-americas-battleground-35612

Davis, J.S. (Feb. 17, 2016). "Scalia's privacy and cyber legacy -- and what's next?." Retrieved from: http://www.scmagazine.com/scalias-privacy-and-cyber-legacy--and-whats-next/article/474397/

Farrell, H. (March 12, 2014). "The political science of cybersecurity IV: How Edward Snowden helps U.S. deterrence," Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2014/03/12/the-political-science-of-cybersecurity-iv-how-edward-snowden-helps-u-s-deterrence/

Farrell, H. (January 23, 2014a). "The political science of cybersecurity I – why people fight so hard over cybersecurity," Retrieved from: https://www.washingtonpost.com/news/monkey-cage/wp/2014/01/23/the-political-science-of-cybersecurity-i-why-people-fight-so-hard-over-cybersecurity/

Fact Sheet: Cybersecurity National Plan. (Feb. 9, 2016) https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Fussey, P. (2008). "Beyond Liberty, Beyond Security: The Politics of Public Surveillance." *British Politics*, vol. 3, no.1, 2008, p. 120–135.

Gardiner, C. & Mallicoat, S. (2014). Criminal Justice Policy, Sage Publications, New York, 2014, p. 67-83.

Hatch, Carper Introduce Federal Computer Security Act. (August 11, 2015). Retrieved from: https://riponadvance.com/stories/510632623-hatch-carper-introduce-federal-computer-security-act/

Griffin, R.C. 2016. "Spying", in D.A. Frenkel (ed)) *Selected Issues in Modern Jurisprudence*, Athens Institute for Education and Research (ATINER), Athens, Greece, pp. 35-54.

Heidegger, M. 1977. *The Question Concerning Technology, in: The Question Concerning Technology and Other Essays*. Harper and Row, New York, 1977, p. 3– 35.

Hunton, H. & Williams, M. (2014). "Privacy and Information Security Law Blog: Global Privacy and Cybersecurity Law Updates and Analysis." Retrieved from https://www.huntonprivacyblog.com/tag/supreme-court/

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press, Buckingham.

Hoffman, A. Linsky, K. Segalis, B. (January 3, 2016) "Federal Cybersecurity Information Sharing Act Signed into Law" Retrieved from http://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law/

Jewkes, Y. (2015). Media and Crime. Sage Publications, New York, p. 222-242.

Madden, M. (2015). "Americans' Attitudes About Privacy, Security, and Surveillance." Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Mass, P. (August 3, 2013). "How Laura Poitras Helped Snowden Spill His Secrets." Retrieved from: http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?pagewanted=all&_r=0

Mulgan, R. (2000). "Accountability: An Ever-Expanding Concept?" Public Administration, vol. 78, no. 3, 2000, p. 555–573.

Pelton, J. & Singh, I. B. (2015). *Digital Defense: A Cybersecurity Primer*. Springer: New York.

Schedler, A. "Conceptualizing Accountability" (1999). In A. Schedler, L. Diamond, M. Plattner (eds.). *The Self-Restraining State: Power and Accountability in New De contacts*, Lynne Rienner Publishers, London, 1999, pp. 13–28.

Scheuerman, W. (May 21, 2014). "Snowden and the Ethics of Whistleblowing." Retrieved from: http://bostonreview.net/books-ideas/scheuerman-snowden-greenwald-harding-sagar

Sennet, R. (1990). *The Conscience of the Eye: The Design and Social Life of Cities*. W.W. Norton, New York.

Stempel, J. (August 24, 2015). "U.S. court declares FTC has authority to regulate cybersecurity," Retrieved from: http://venturebeat.com/2015/08/24/u-s-court-declares-ftc-has-authority-to-regulate-cybersecurity/

Talanian, N. (2008). "The 'War on Terror' and The Constitution," Retrieved from: http://www.constitutioncampaign.org/toolkit/war_on_terror.pdf

Xu, V. (May 15, 2015). "Edward Snowden Talks Ethics of Whistleblowing," Retrieved from: http://www.stanforddaily.com/2015/05/18/edward-snowden-talks-ethics-of-whistleblowing/