International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V68I7P101

Volume 68 Issue 7, 1-6, July 2020

Original Article

Privacy vs National Security

Tajdar Jawaid

MS Cybersecurity, University of Dallas, TX, USA

Received Date: 14 May 2020
Revised Date: 27 June 2020
Accepted Date: 30 June 2020

Abstract *- There are growing concerns and anxiety about privacy among the general public, specially after the revelations of former NSA contractors and whistle-blowers like Edward Snowden and others. While privacy is the fundamental concept of being human, the growing tug-of-war between individual's privacy and freedom vs national security has renewed the concerns of where the fine balance should lie between the two. For the first time in history, technological advancement has made mass data gathering, analysis, and storage a financially and technologically feasible option for governments and private businesses. This has led to the growing interest of governments and security agencies around the globe to develop sophisticated algorithms using the power of Big-Data, Machine-Learning and Artificial Intelligence. The technology has enabled governments and private businesses to collect and store thousands of data points on every individual, which has put individuals' privacy under constant threat. This article analyses the individual's privacy concepts and their perceived link with national security. The article will also discuss the various aspects of privacy and national security, the arguments of both sides and where a boundary should be drawn between privacy and national security.*

Keywords *- Privacy, Human Right, National Security, Terrorism, Counterterrorism, Profiling, Cataloguing, Personal Data, Mass-Surveillance, Cybersecurity, Big-brother, Machine-Learning, Big-Data, AI, FISA.*

I. INTRODUCTION

There was a time when surveillance on anyone, be it is an individual, organization or enemy state, was considered to be a very difficult, sophisticated, time and resource-consuming operation. There were numerous laws, financial constraints, and technological hurdles. For instance, if surveillance is required on an individual, the security or law enforcement agencies have to create proper justifications to get the necessary warrants and relevant court permissions, allocate massive resources, break in into the premises of the target to install bugs for surveillance, physical spies are needed on targets to monitor and photograph all movements and interactions, wiretap phones, listen to conversations, collect evidence and so on. All these constraints, on the one hand, make the job of surveillance and intelligence gathering difficult, but on the other, they ensure greater privacy to the individuals and deter the governments and their agencies from initiating these activities without a justifiable cause. In the past few years, the advancement in technology has made a massive paradigm shift in surveillance. Technology has now made intelligence gathering not only financially viable but very attractive options for governments around the globe. Since 9/11 and the resulting war on terror, there was a strong desire among the security and law enforcement communities to find out ways to gather intelligence at a massive scale to avoid such incidents in future. This desire turns into a requirement of security and intelligence agencies that has given the birth of the concept of mass surveillance. Mass-surveillance programs have enabled governments and their intelligence agencies to monitor a large set of the population without their knowledge and consent. The rise of social media, internet-connected smart devices, IoT (internet of things) also have a deep impact on an individual's privacy. These concerns result in debates around what actually is considered to be private information in this time and age. The next section will focus on what actually privacy is in the current scenario, why it is important and why it is necessary to be protected.

II. BACKGROUND ON WHY PRIVACY MATTERS

Every human being has things that they want to keep very personal. It does not mean that it has to be to something illicit, unlawful or criminal in nature. In fact, most of the time, these are very innocent, totally harmless personal information in terms of religious, political or social views, some very personal choices, desires and feelings, sexual orientation, relationships, health-related information and so on. Still, individuals are not comfortable sharing it with anyone, even their closest ones. This is the actual essence of privacy. Disclosing these kinds of information is a personal choice and a fundamental human right. Privacy has been recognized as the fundamental human right under the United Nations Declaration on Human rights (UDHR) Article 12 [1], which states, *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.",* which was reaffirmed through the United Nation's International Covenant on Civil and Political Rights (ICCPR) article 17:1[2]. Accordingly, to the UN declaration and civil and political rights covenants, the law should protect and provide appropriate measures to ensure the protection of every individual's privacy.

Privacy ensures the individual's right to the freedom of speech and expression, and it protects from race/religious/political/sexual persecution providing the right to freedom and choice to share or hide personal information from others. Privacy is a state of not being watched or disturbed without our knowledge and consent. Right to privacy ensures that we are free from state surveillance, free to have our own unique thoughts and views, free from being just a number, free from profiling and cataloguing based on various character traits, free to protest, free to vote, free to think, free be left alone and so on so forth. Privacy, in some view, is what keeps us separate from zoo animals who are continuously being watched and filmed without their will and consent. Privacy is a very basic human instinct and is recognized as a fundamental human right, and it gives the confidence of being in possession of our own personal information, thoughts, views and opinions without being judged. These basic concepts of privacy are now considered to be under threat as per organizations and movements like privacy international [3]. To protect this fundamental right, there are multiple laws enacted, which will be discussed in the next section.

III. PRIVACY LAWS AND REGULATIONS

The privacy-related issues and concerns in Europe go back as far as the 1970s and '80s, as government agencies and privates' businesses started to collect and store customer data. As a result, in Europe, common protection system was implemented, which was followed by EU Data Protection Directives in the 1990s (directive 95/46/EC) [4]. The privacy concerns increase with the growing governments and private business interest in gathering and storing personal information. To address these concerns in Europe, the EU Data Protection directives of 1990 were replaced by EU-GDPR (European Union General Data Protection Regulation) in 2016 [5].

In the United States, the fourth amendment considered to be the basis of most privacy laws, which states that, *"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"*[6]. In the US, multiple federal and state-specific laws were enacted to ensure the privacy rights of an individual. Some of these laws in the U.S. are, Children's Online Privacy Protection Act (COPPA) of 1998, The California Online Privacy Protection Act (CalOPPA), Electronic Communications Privacy Act (ECPA) of 1986, Communications Assistance for Law Enforcement Act (CALEA) of 1994, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, Data Breach Notification Laws, Family Educational Rights and Privacy Act of 1974 and Identity Theft and Assumption Deterrence Act of 1998 are the few. These and other privacy-related laws and regulations provided the required framework for governments and private organizations to implement stringent security to ensure the privacy of an individual. The control over privacy is getting weaker even though the privacy rights grew stronger. This is due to the fact that personal data are now much more exposed and easily available, which was not the case a few years back.

It is important to understand what constitute personal data and what comes under privacy. At a very high level, any information that defines and uniquely identifies a person is normally classified as personal data and should be protected by privacy laws and regulations. This means in an ideal world, any information that falls under personal data should not be harvested without the knowledge and consent of the data subject. What comes under private personal data and falls under privacy rights will be discussed in the next section.

IV. WHAT ACTUALLY COMES UNDER PERSONAL DATA

Technically anything considered to be privately related to personal data which a person is not willing to share with the world. But according to the European General Data Protection Regulation (GDPR) of 2016, personal data means any information about a natural person (living person) which identify a natural person directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Together with this, article 9 of GDPR prohibits the processing of the following categories of personal data, e.g. race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, genetic data, biometric data, health data, concerning a natural person's sex life, sexual orientation etc. without explicit consent of data subject. The GPDR has provided a clear and concise definition of personal data or PII data, for which organizations have to have legitimate business and lawful purposes and data subject consent to process and store. In comparison, article 12 to 17 of the GDPR gives multiple rights to data subject related to their personal data, such as a right of access, right to be forgotten, right to restrict processing, right to data portability, right to object to processing [5].

In digital and internet context, the personal data includes but is not limited to a person's name, gender, race, beliefs, address, photographs, videos, friends and family members details, health-related information, physiological information, biometrics, phone numbers, IP address, location data like GPS coordinates or Cell-ID locations, and so on. Any digital trace and information which uniquely identified a person is considered to fall under personal data [5].

The next section will discuss the link between individual privacy with national security.

V. THE INDIVIDUAL PRIVACY VS NATIONAL SECURITY

In 1984 George Orwell wrote a novel called *"Big-Brother"*. The basic premise of the novel was that every citizen would be continuously watched, listened to, tracked, profiled and catalogued by the government. This fictional work has envisioned the environment where there was no concept of citizen's privacy at all [7]. In the aftermath of September 11, 2001, the United States government passed the USA Patriot Act on October 26, 2001, which has given new dimensions to the privacy of an individual by linking it to national security [8]. This perceived link between national security and citizen's privacy trend has been followed by multiple governments around the globe. The United Kingdom has introduced one of its own bills in 2016, which gives immense powers of surveillance to its security agencies with the bill called Investigatory Powers Act [9]. This kind of counterterrorism laws has given enhanced power to the security and intelligence agencies to allow surveillance by all possible means, e.g. digital communication monitoring, which includes (phones, emails, text messages etc.), investigating any suspect without tipping off, obtaining business records, cross-border information and intelligence sharing, obtain search warrant anywhere, monitor electronic trespassers enhance the punishments etc. These laws aim to equip the intelligence and security agencies with the necessary tools to intercept and obstruct terrorism. These counterterrorism measures have resulted in several covert indiscriminate mass-surveillance programs from governments around their citizens. However, the full extent of these programs and their invasiveness to citizens privacy-first surfaced after the revelations made by former NSA whistle-blower.

A. The Snowden's Leaks: "A Case Study"

The startling revelations by former NSA contractors like Edward J. Snowdon have raised new and legitimate concerns around the privacy invasion in the name of national security. The scenario which was presented in Orwell's novel that a state act like *"Big-Brother"* by initiating the mass indiscriminate surveillance, tracking, profiling and cataloguing of its citizens seems to become a reality by Snowden's leak [10].

a) The mass-indiscriminate Surveillance

The Snowden leaks raises concerns over mass-indiscriminate surveillance of all citizen communication over the internet. This includes obtaining all phone records, emails and text messages from service providers, all social media posts, blogs and vlogs etc. The leaks also reveal that in many cases FISA process has been bypassed for the collection of citizens' private information [10].

b) Gather and Store all communication

The leaks also discuss the creation of big data centres with virtually unlimited or expandable storage capacities. They are created to gather and store all digital communications over the internet for later analysis [10].

c) The Meta-Data

The government stance is that they only collect the meta-data about communication, which does not contain the actual communication itself. But Snowden suggests that it is not entirely true. There are programs that gather and store actual communications, e.g. phone calls, emails, text messages etc. [10].

d) The Prism Program

Snowden's leak has revealed the details about the Prism Program. The prism program provides the most detailed search capability on an individual through access to social media platforms like Apple, Google, Amazon, Facebook, Twitter, etc. These social media platforms provided real-time search API's to NSA. These API's then combined into a single search interface, which can pull all the information about any specific person on various search criteria from the servers of the above companies. This includes data from all social media posts, connection details, friends and family details, emails, texts messages, photographs, internet searches, in fact, anything or everything stored on their platforms about an individual [10].

e)Zero-day Exploits (the backdoors)

Zero-day exploits are unknown, bugs and backdoors. Sometimes deliberately created specifically for surveillance purposes in mobile, desktop operating systems, applications and software. Through these zero-day exploits, any internet-connected device camera mic can be remotely activated without the device owner/user noticing it or the mobile applications track gather and transport personal data like phone records, contact details, emails, text messages on the servers without ever being noticed. Through these exploits, a person effectively can be watched or heard, tracked through their device's GPS, all without their knowledge and consent. Although all big names like Apple and Google are opposed to this request from security and intelligence agencies. But according to Snowden's leak, that was also a part of the prism program [10].

B. A Problem without a clear Solution

Terrorist incidents like 9/11 are considered to be the failure of security and intelligence agencies. Incidents like this have been the primary motivation behind the laws like the USA Patriot Act and the British government's Investigatory Powers Act. These kinds of laws indicate there is a clear shift in how governments see the privacy of their citizens. Privacy that was once considered the basic human right is now on a direct collision path with national security.

The primary responsibility of any state is to protect the life and livelihood of its citizens, maintain law and order and protect its national infrastructure and interests. Therefore, in order to achieve these objectives, the security agencies have to equip with the necessary tools and technologies supported by the law to gather the

intelligence which will help prevent the repetition of incidents like September 11, 2001.

There are also debates about the trade-offs between security and privacy. Too much privacy may hinder the ability of security agencies to gather required intelligence on targeted individuals. Also, too many prerequisites like gathering evidence to obtain necessary court orders may put security at compromise. On the other hand, unlimited and unrestricted powers to invade citizens' privacy by government agencies in the name of national security may increase the risk of power misuse, which increases the trust deficit between the general public and governments.

This is still a debatable subject as to what level of privacy invasion and compromises are acceptable to achieve security objectives. What kind of powers should be vested in intelligence communities to curb the next big attack. Are there any other counterterrorism alternatives and solutions which could give the required level of information to intelligence communities to ensure security without invading the privacy of the individuals? Should governments wait for any incident to have happened before they allow the security and intelligence agencies to be able to do the surveillance on the suspected individuals? An analysis of recent terror-related incidents reveals that the majority of the suspected terrorist who carried out the attacks are already known to the law-enforcement agencies, and in some instances, the red flags were already raised against them. Still, those individuals successfully carried out the attacks [16]. This in itself raises questions around mass-surveillance programs effectiveness, their lack of ability to provide actionable intelligence etc. These and many similar questions are part of the wider debate on this subject, without a clear-cut and agreeable solution to date.

a) The Increase in terrorism

Since the war-on-terror started post 9/11, which resulted in various mass-surveillance programs, the actual number of terrorism-related incidents has been increased globally.

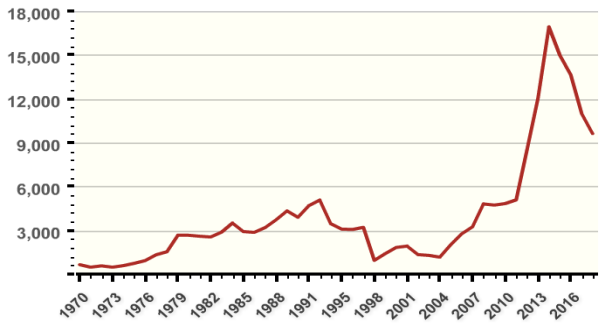

Fig. 1 University of maryland (2020). global terrorism database [14]

Figure 1 of the University of Maryland, Global Terrorism database shows a record number of increases in global terrorism-related incidents since 9/11 [14]. This is an indication that these programs are not as useful as it is perceived in the view of intelligence communities, at least not in their current shape and form to combat terrorism.

b) The general-public trust and opposition

Since Snowden's leaks, the approval ratings from the public has been decreased. In a survey in 2015 conducted by the PEW research centre, 52% of Americans were concerned about government surveillance of Americans personal data and communication [15].

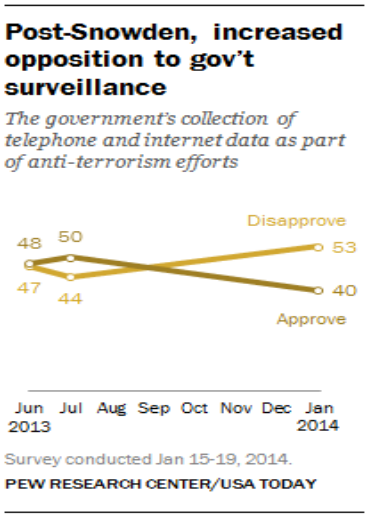

Fig. 2 PEW research Jan 15-19, 2014 [15].

The PEW research in 2014 shows that post-Snowden, the opposition to government surveillance has increased [15].

C. The False Trade-off between Privacy vs National Security

There is a general perspective that there are trade-offs between privacy and security. However, these perspectives are often based on arguments that are not fully supported by substantial facts and figures.

a) Good People vs Bad People View

There are views that are sometimes enforced by the influencers like the technology giant Google. Its CEO Eric Schmidt once said, *"If you have something you don't want anyone to know, maybe you shouldn't be doing it"* [11]. This particular mentality shows that privacy is a concern for only bad people who are doing bad things, e.g. involved in criminal activities, terrorism etc. They completely ignore the importance of privacy or the fact that privacy is not about being good or bad but a basic human right.

b) Nothing to Hide, Nothing to Fear

This is again on the similar lines of good and bad people view. This view again argues that essentially the reason to hide personal data from the government is because of the fear of something wrong with it. Again, people with these views completely ignores what privacy actually means [12].

c) The cost of Security is Privacy

If the next 9/11 can be avoided by giving up my privacy, I am up for it. Again, the cost of security does not have to be paid by giving up the fundamental human right to privacy.

Civil liberties and anti-terrorism policies

Percent who favor each as a measure to curb terrorism	Sept 2001 %	Aug 2002 %	Dec 2006 %	Aug 2011 %
Requiring that all citizens carry a national ID card at all times	70	59	57	57
Extra airport checks on passengers who appear to be of Middle-Eastern descent	--	59	57	53
Government monitoring credit card purchases	--	43	42	42
Government monitoring personal phone calls and emails	--	33	34	29

Fig. 1 PEW research centre aug 17-21, 2011 [15]

Pew research in 2011 on the tenth anniversary of 9/11 reveals that 54% of Americans were not in favour of giving up civil liberties as a method to curb terrorism [15]. The next section will discuss where the possible boundary can be drawn between Privacy vs National Security.

VI. PRIVACY VS NATIONAL SECURITY, WHERE SHOULD BE THE BOUNDARY?

There may be trade-offs between national security and privacy, but they should be based on the facts and figures. There should not be a complete blind eye by governments on the powers vested to its security agencies in the name of national security. There should be a proper system of checks and balances needed to be developed supported by the law in order to avoid the misuse of these powers.

a) The Internet and Digital Communication

After September 11, the NSA has initiated a domestic surveillance program known as the *"President's Surveillance Program"*. The program enforces all communication and internet service providers to provide all communication and call detail records of all their customers. NSA also recorded the emails of all customers of these telecommunication providers [13]. This trend has been followed by multiple governments around the globe. In fact, these internet and telecom companies have developed search portals that are made available to government agencies, which can be used to search for any communication details that happened over their network in real-time. Again, this level of information access is key in intercepting, tracing and locating a suspect before they carry out their attacks. Proper government oversight is needed to address privacy and misuse concerns.

b) The Encrypted Internet Communication

The security and intelligence agencies view encrypted internet communication technologies as a hindrance in their work. Which in many cases may be a legitimate concern. The counter-argument here is providing the cryptographic keys to agencies could make the whole internet communication unreliable and unsafe. The access to the cryptographic keys to government agencies could be a prime target for malicious hackers, put internet security at risk, compromise the human right to privacy and undermine the rule of law. These kinds of law enforcement access to encrypted communication should approach with caution [17].

c) Video Surveillance

In today's world, close circuit tv and security cameras are installed in a public and private place in all cities and towns, shops, bars, businesses, buses, trains and every step of the way. Every movement of a person is recorded and watched. This video surveillance, by definition, is also an invasion of privacy, but it is an acceptable norm around the world. These video surveillance technologies are now increasingly used with biometric technologies such as facial recognition, which can be used to profile, catalogue and identify an individual. These technologies are essential to provide security and deterrence but at the same time raises the concern over privacy invasion. The use of video surveillance technology, when clubbed with biometrics such as facial recognition and related algorithms, should have a proper law oversight to avoid any misuse of these technologies.

d) Big-Data Analytics, Machine-Learning and Artificial Intelligence

Big-data technologies has revolutionized the way data has been studied. Big data has enabled the systematic analysis of very large and complex datasets to extract meaningful information through various algorithms. The algorithms like pattern recognition and pattern matching identify trends and associations among seemingly unrelated and very large and complex datasets. The intelligence and law enforcement agencies use big-data technologies and algorithms on the citizen personal data, which they collected from different sources like internet communication service providers, social media platforms and various other means. Big-data analytics, together with Artificial Intelligence and Machine learning technologies, are used to improve the prediction of human behaviour through the process called psychographic analysis. It is a known fact that the majority of terrorists leave digital traces while communicating, planning and interacting over the internet. These technologies can be used to study, analyze and predict the behaviour of these individuals in order to combat terrorism and security threats. But at the same time, a misuse of these technologies can have a devasting impact, like it was revealed in the Cambridge Analytica scandal. The scandal reveals how these technologies have been used to influence the whole election process in various countries [18]. Further research is required to develop or refine the existing big-data algorithms to help intelligence agencies with the appropriate oversights to avoid unnecessary privacy invasion of citizens supported by the laws to curb the misuse of these technologies.

e) Store everything for later analysis:

As revealed in the Snowden case study, governments and private businesses create big data centres with virtually unlimited data storage capabilities. This result in storing all internet communication for an unlimited period

of time, to be analyzed later [10]. The blanket application of gathering and dumping everything by security agencies into these big data centres should be scrutinized by governments and relevant watchdogs. There is always a risk if a malicious hacker gets their hands on any such datastores what level of havoc they can pose to individuals, corporations and governments.

f) The FISA and Investigatory Powers Act

The U.S government has provided lawful backing to the security agencies through Foreign Intelligence Surveillance Courts (FISA). The FISA courts in the USA ensures that the security and law enforcement agencies can only do the surveillance on American citizens and permanent residents through a proper court order when there is a probable cause or a legitimate security concern [19]. Similarly, in the UK, the Investigatory Powers Act gives enhanced powers to the law-enforcement agencies to obtain communications and data about communications and other digital traces of an individual [9].

Though the FISA courts in the USA and Investigatory Power Courts in the UK are enacted to justify every surveillance need through probable cause, according to Snowden's leaks, the security agencies in the majority if not in all cases completely bypass these processes [10][18], or these courts pass orders in favour of law enforcement and security agencies without due scrutiny to ascertain the probable cause [19].

While, in some cases, understandably, the intelligence agencies may not have enough time at their disposal to go through the due process, sometimes a complete blind eye may compromise privacy and may be counterproductive to achieve security objectives. Hence it is necessary that these legal and lawful processes must be refined, strengthened and properly enforced.

VII. CONCLUSION

National security and privacy are deeply interconnected topics. Though technological advancement for the first time in history has enabled mass surveillance a viable technological and financial option for governments, it has also raised concerns over the right to privacy. As privacy awareness is increasing, the privacy laws and regulations are getting tougher, but the control over privacy is getting weaker. Privacy is a fundamental human right and must be protected. The debate between privacy and national security is complex as both sides have compelling arguments. There may be trade-offs between security and privacy still a proper government oversight is necessary to avoid mass indiscriminate citizen surveillance and to put a proper check and balances over the powers given to the security and intelligence agencies.

REFERENCES

[1] The United Nations website, Universal Declaration of Human Rights (UDHR), (1948) [Online]. Available: https://www.un.org/en/universal-declaration-human-rights/

[2] The United Nations website. United Nations Treaties. International Covenant on Civil and Political Rights (ICCPR). (1966) [Online]. Available:https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

[3] The Privacy Insertional website. [Online]. Available: https://privacyinternational.org

[4] The European Union website. Europa, Access to European Union Law. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of European Union L 281, 23/11/1995 P.0031 - 0050. (1995). [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[5] The European Union website. Europa, Access to European Union Law. Regulation (Eu) 2016/679 Of The European Parliament And Of The Council, General Data Protection Regulation. Official Journal of European Union L 119/1, (2016). [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

[6] The U.S. Congress website. Constitution Annotated, Analysis and Interpretation of the U.S. Constitution, Fourth Amendment. [Online].Available:https://constitution.congress.gov/constitution/amendment-4/

[7] George Orwell, Nineteen Eighty-Four, Penguin Modern Classics, 2004.

[8] The U.S. Department of Justice website. The USA Patriot Act: Preserving Life and Liberty. [Online]. Available: https://www.justice.gov/archive/ll/highlights.htm

[9] The United Kingdom Home Office website. Investigatory Powers Act. Home Office, United Kingdom. (2015). [Online]. Available: https://www.gov.uk/government/collections/investigatory-powers-bill

[10] Luke Harding, The Snowden Files, Penguin Random House. 2014.

[11] Electronic Frontier Foundation. Google CEO Eric Schmidt Dismisses the Importance of Privacy. (2009). [Online]. Available: https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

[12] Daniel J. Solove, Nothing to Hide. Yale University Press (2011).

[13] Electronic Frontier Foundation, (2014). NSA Spying. [Online]. Available at: https://www.eff.org/nsa- spying.

[14] University of Maryland. Global Terrorism Database. Incidents over time. (2020). [Online]. Available at: https://www.start.umd.edu/gtd/

[15] PEW Research Center. Civil liberties and anti-terrorism policies. (2011). [Online]. Available at: https://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

[16] Dr Lorenzo Vidino, George Washington University. (2018). [Online]. Available at: https://extremism.gwu.edu/dr-lorenzo-vidino

[17] Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner .Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. Computer Science and Artificial Intelligence Laboratory Technical Report. (2015). [Online].Available at: http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

[18] Carole Cadawalladr, Emma Graham-Harrison. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in a major data breach. The Guardian. (2018). [Online]. Available at: http://freestudio21.com/wp-content/uploads/2018/04/50-million-fb-profiles-harvested-by-cambridge-analitica.pdf

[19] David Wright, Reinhard Kreissl. European responses to the Snowden revelations: A discussion paper. Increasing Resilience in Surveillance Societies (IRISS). (2013). [Online]. Available at: https://www.irks.at/assets/irks/Publikationen/Unterlagen/IRISS_European-responses-to-the-Snowden-revelations_18-Dec 2013_Final.pdf