THE ETHICAL DILEMMA OF WARRANTLESS WIRETAPPING IN THE UNITED STATES OF AMERICA

FEBBIE FARSIDILLA BASUKI

UNIVERSITI SAINS MALAYSIA

2015

THE ETHICAL DILEMMA OF WARRANTLESS WIRETAPPING IN THE UNITED STATES OF AMERICA

by

FEBBIE FARSIDILLA BASUKI

A thesis submitted in fulfillment of the requirements for the degree in Master of Social Sciences

September 2015

The tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.

Justice Louis D. Brandeis
(*Olmstead v. United States* case)

ACKNOWLEDGMENTS

The researcher experienced several bumpy roads during the journey of writing this Master's thesis. However, with the presence of many people, she managed to complete this process. This opportunity is taken to show her gratitude towards those individuals.

First and foremost, great appreciation would like to be expressed to her research supervisor, Assoc. Prof. Dr. P. Sundramoorthy, for his bold lines of corrections, which you would never miss out but were tremendously helpful for the improvement of this thesis, as well as for his patience and guidance. The researcher humbly acknowledges Assoc. Prof. Dr. Azeem Fazwan Ahmad Farouk as her research co-supervisor for his kindness, also suggestions and ideas, which helped clear the doubts encountered during the writing process.

Immense gratitude is given to the well-respected panel of examiners of this research thesis, Prof. Dr. Mohd Kamarulnizam Abdullah, Assoc. Prof. Dr. Azrina Husin and especially Assoc. Prof. Dr. Mohamad Zaini Abu Bakar. Their much valued feedback and reviews have enabled the researcher to amend shortcomings and weaknesses of her thesis.

Appreciation also goes to the Dean of School of Social Sciences at Universiti Sains Malaysia (USM), Assoc. Prof. Dr. Nor Malina Malek, as well as to the School

officials, especially Mr. Abdul Aziz Razak, Mrs. Suraya Abdullah, Mrs. Roslina Mohamed Idros and Mr. Ahmad Zaki Talhah Mohd Zain. Without their assistance, this thesis would not have been submitted on time. Not to forget the helpful officers at the Institute of Postgraduate Studies in USM, special thanks to Mrs. Nurrul Hasyda Mohd Hasim, Mrs. Umi Salmah Abd Rani, Mrs. Fadhrumaizah Tajul Arof, Ms. Siti Asma Osman, Mr. Mohammed Nazri Mohd Feroz Khan, Mr. Mohd Faizal Md Fazil, Ms. Mahani Yusoff, Mrs. Fatimah Mahmood, Mrs. Dianna Shanti Davadas Michael and Mrs. Siti Hajar Saad.

Finally, gratefulness goes to my Creator for giving me the health to complete this research thesis. Thankfulness is surely granted to my parents, sister and family for their constant support, love and prayers. Special cheers to friends of the researcher for their joyful company and encouragement; amongst them are Atoillah, Syarilla Ell Suhaily, Ainatul Fathiyah Abdul Rahim, Sri Jeyanthirar Subramaniam, Jega Annamalaiyar and many others, who unintentionally are not mentioned here.

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABA	American Bar Association (U.S-based)
ACLU	American Civil Liberties Union (U.S-based)
ASEAN	Association of Southeast Asian Nations
CALEA	Communications Assistance for Law Enforcement Act of 1994
CIA	Central Intelligence Agency (U.S)
CNO	Computer Network Operations
COMINT	Communications Intelligence
CSEC	Communications Security Establishment Canada
D.C	District of Columbia
D/CIA	Director of the Central Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense (U.S)
ECHR	European Convention of Human Rights
ECPA	Electronic Communications Privacy Act of 1986
ECtHR	European Court of Human Rights
EFF	Electronic Frontier Foundation (U.S-based)
ELINT	Electronics Intelligence
EO	Executive Order
EPIC	Electronic Privacy Information Centre (U.S-based)
E.U	European Union
FAA 2008	FISA Amendments Act of 2008
FCC	Federal Communications Commission
FBI	Federal Bureau of Investigation (U.S)
FISA	Foreign Intelligence Surveillance Act of 1978
FISC	Foreign Intelligence Surveillance Court
FISINT	Foreign Instrumentation Signals Intelligence
FVEY / UKUSA	Five Eyes Alliance
GCHQ	Government Communications Headquarters (U.K)
HRW	Human Rights Watch (U.S-based)
HSA	Homeland Security Act of 2002
HUMINT	Human Intelligence

IA	Information Assurance
IETF	Internet Engineering Task Force
IPT	Investigatory Powers Tribunal (U.K)
NCTC	National Counterterrorism Centre
NSA	National Security Agency (U.S)
NSL	National Security Letters
NYCLU	New York Civil Liberties Union (U.S-based)
PAA	Protect America Act of 2007
PATRIOT Act	Providing Appropriate Tools Required to Intercept and Obstruct Terrorism of 2001
PET	Privacy Enhancing Technologies
PRISM	Privacy and Security Mirror
RFID	Radio Frequency Identification Device
SIGINT	Signals Intelligence
TELINT	Telemetry Intelligence
TSP	Terrorist Surveillance Program
U.K	United Kingdom
U.N	United Nations
U.S	United States of America
U.S.C	United States Code

DILEMA ETIKA TERHADAP PENGINTIPAN TALIAN TANPA WARAN DI AMERIKA SYARIKAT

ABSTRAK

Kontroversi mengenai pengawasan komunikasi Kerajaan telah lama tercetus sejak berabad-abad yang lalu. Menemukan kelebihan yang seimbang terhadap pengawasan ini khususnya berkaitan keselamatan negara dan privasi individu sentiasa menjadi satu proses yang tiada kesudahan. Sejak kebelakangan ini, peningkatan serangan pengganas telah memberikan momentum kepada kerajaan untuk menggunakan pengesahan 'perang ke atas keganasan'. Hal ini membolehkan mereka menjalankan rentas-sempadan secara meluas dan besar-besaran atau dalam erti kata lain pengawasan komunikasi 'secara senyap'. Untuk memahami fenomena tersebut, penyelidikan ini mengkaji konteks berkaitan teknologi pengawasan secara khusus, iaitu pengintipan talian, di Amerika Syarikat (A.S). Negara ini dipilih sebagai skop kajian disebabkan penglibatan utama kerajaan dalam program-program pengawasan komunikasi tanpa waran sejak kebelakangan ini mula terdedah. Analisis kandungan telah dilakukan ke atas maklumat berkaitan isu subjek. Undang-undang sedia ada dan hasil pembelajaran untuk kes-kes mahkamah berkaitan pengintipan talian di A.S juga dianalisis untuk memahami sama ada mereka telah memberi sumbangan kepada penemuan keseimbangan yang ideal. Kajian ini juga menyimpulkan bahawa undang-undang semasa berkenaan pengintipan talian di A.S meletakkan beban yang lebih terhadap keselamatan kerajaan, manakala keputusan yang dibuat dalam kes-kes mahkamah di A.S berkaitan pengintipan talian menunjukkan keputusan yang tidak stabil dan telah memburukkan lagi keadaan yang

sebenar. Sudut pandang jelas yang digambarkan melalui peraturan-peraturan ketat yang juga harus dipatuhi secara konsisten oleh institusi hukum di A.S adalah penting. Perjanjian antarabangsa yang signifikan dan adil mengenai perkara ini juga memainkan fungsi yang penting untuk menyelesaikan dilema etika ini.

Katakunci: pengawasan komunikasi, pengintipan talian, kebersendirian individu, keselamatan negara

THE ETHICAL DILEMMA OF WARRANTLESS WIRETAPPING IN THE UNITED STATES OF AMERICA

ABSTRACT

Government communication surveillance created controversies since centuries ago. Finding a balanced advantage of this particular surveillance in regards to national security and individual privacy has always been a never-ending process. Recent increase in terrorist attacks gave governments the momentum to use 'war on terror' validations and enabled them to conduct extensive cross-borders mass or 'blanket' communication surveillance. To comprehend the phenomena, this research examines associated contexts of a specific surveillance technology, namely wiretapping, in the United States of America (U.S). This country is chosen due to its major involvement in warrantless government communication surveillance programs that were recently exposed. Content analysis was conducted on information relevant to the subject issue. Existing laws and outcomes of court cases regarding wiretapping in the U.S were also analyzed to understand whether they have contributed towards meeting the ideal balance. The study concluded that current U.S wiretapping laws put more weight on the national security scale, whereas the verdicts of wiretapping cases represent unstable decisions, which aggravate the situation. Clear standpoints portrayed through strong regulations that are consistently abided in judgment calls are crucial. Significant and fair international agreements on the matter are also essential to resolve this ethical dilemma.

Keywords: communication surveillance, wiretapping, individual privacy, national security

CHAPTER I. INTRODUCTION

This chapter intends to provide background information and facts on the research matter. Statement of the problem as well as questions and aimed objectives of this research are defined to highlight the importance and significance of this thesis. Important terms discussed in this study are also explained in the introductory chapter in order to comprehend them in the intended context.

1.1 Research Background

Ever since the World War I began in 1914, battle targets have always been changing (Petersen, 2012). It started off with humans as primary targets in war zones; to defeat more men or the opponent's leader was the ultimate goal. Then, not only humans were of concern but also war machines. Traditional attack and defense methods were no longer in trend, instead it became a battle of who owns more advanced war tanks, jet fighters, nuclear bombs, weapons of mass-destruction or other unconventional armaments. Having cutting-edge technology to innovate destruction tools that were ahead of those owned by opponents was crucial to gain victory in wars. Today, we have reached an era where information is the new battle strategy or battle target during warfare; it is claimed to be the time of 'clean and zero-blood war' (Mattelart, 2010). Control over worldwide information through communication is now vital for military purposes or international affairs. Fast access to critical confidential news like terrorist attack plots can afford additional time to develop the desired strategy, whether it may be for defense or ambush. Many

techniques can be pursued in achieving power and control over communication systems to attain information, one of them is surveillance.

1.1.1 The Age of Surveillance

Surveillance in the context of this study is basically the act to observe a person, an object, an area or situation at a present or pre-recorded state with the intention to obtain information that would otherwise be impossible to achieve. According to Petersen (2012), surveillance is a very context-sensitive field (p. 18) but can be generally defined as a method to keep watching over a certain individual or a group of people, and/or a specific item or a group of things, and/or a specific space or broad zones in order to identify its characteristics, activities, patterns, trends, events, etc. (p. 10). "The act of monitoring the behaviour of another either in real-time using cameras, audio devices or key-stroke monitoring, or in chosen time by data mining records of Internet transactions", this was how David Wall defined surveillance (Wall, 2007, p. 230).

There are two approaches that can be used to further define surveillance, the neutral concept and the negative concept (Fuchs, 2010). Neutral concepts of surveillance claim that surveillance either has positive impacts or both negative and positive impacts; whereas negative concepts claim surveillance to have damaging impacts like the domination, violence, exploitation, oppression and coercion by power structures as well as the injustice of society. As cited in (Fuchs, 2010, pp. 2-3), several experts identified their own understanding of the **neutral** surveillance concept:

- Christopher Dandeker: Surveillance is "(1) the collection and storage of information, presumed to be useful, about people or objects; (2) the supervision of the activities of people or objects through the issuing of instructions or the physical design of the natural and built environments; and (3) the application of information-gathering activities to the business of monitoring the behavior of those under supervision and, in the case of subject populations, their compliance with instructions, or with non-subject populations, their compliance with agreements, or simply monitoring their behavior from which, as in the control of disease, they may have expressed a with to benefit". This is an example of a neutral concept that shows surveillance has positive impacts.
- Gary T. Marx: "Surveillance can serve goals of protection, administration, rule compliance, documentation and strategy, as well as goals involving inappropriate manipulation, restricted life opportunities, social control, and spying. To varying degrees, surveillance is a property of any social system – from two friends to a workplace to a government." This is an example of a neutral concept that shows surveillance has both negative but also positive impacts.
- Anthony Giddens: Surveillance is "the coding of information relevant to the administration of subject populations, plus their direct supervision by officials and administrators of all sorts". In other words, surveillance is relatively related to nation-states and to the agencies that are assigned to conduct the act.

On the other hand, there are **negative** surveillance concepts that are usually shaped by individuals who ground their opinions on reasonableness and seek for freedom, justice, peace and happiness amongst all people. As cited in (Fuchs, 2010), Kevin Haggerty stated that this negative perception of surveillance is often owned by scholars, because they "are trained in a tradition of critique" (p. 3). According to the most influential theorist on this concept, Michel Foucault, surveillance is "permanent, exhaustive and omnipresent" (p. 6), "a form of disciplinary power" and a "general formula of domination; it includes penal mechanisms, it encloses humans into institutions such as schools, orphanages, training centers, the military, towns, factories, prisons, reformatories, houses of correction, psychiatrists, hospitals, asylums, etc. in order to control their behavior and to partition, rank, normalize, punish, hierarchize, homogenize, differentiate and exclude" them (p. 5). John Fiske added that all surveillance is "totalitarian, for it allows its victims no say in the way it operates and we must not allow the general benignity of its uses to mask the fact" (p. 11).

Surveillance is also portrayed as the '***Panopticon***', which was introduced by Jeremy Bentham through his book written in 1791 and popularized by Michel Foucalt. A *panopticon* method involves putting an individual in a central point, where he/she can be monitored for behaviors to see if those behaviors are in accordance with the rules or not, but cannot see who is monitoring (Mattelart, 2010). It is a top-to-bottom approach; how the authorities see the citizens and how the few see the many. An inverse panopticon term '***Sousveillance***' has been invented by Steve Mann in 1998 (Mann et al., 2003). Unlike panopticon, sousveillance offers a bottom-to-top approach; it is how citizens see those in authority or employees see those at the top

management officials in organizations. Sousveillance challenges panopticon by repositioning the situation of surveillance.

With time, surveillance evolved from having a centralized system into a global decentralized form. So no longer is the surveillance power owned and controlled by one central point, but by several diverse dispersed agents of surveillance. Not only one main database holds data obtained from surveillance, now there are usually several of them located in different areas but are interconnected (Fuchs, 2010). William Bogard did not support this current state of surveillance, he stated that even though surveillance now is "less subject to spatial and temporal constraints (location, tie of day, etc.)", but it is also "less organized than ever before by the dualisms of observer and observed, subject and object, individual and mass" showing that "the system of control is deteriorating" (Fuchs, 2010, p. 8).

There are numerous technologies used to conduct surveillance, some of which might not even be exposed or publicly known yet, but below are a few examples (Petersen, 2012, pp. 14-15):

- **Acoustic surveillance** – this category include the usage of audio technologies that operate within the range of human hearing; infrasonic and ultrasonic technologies that operate outside the range of human hearing; and sonar technologies that operate in frequencies both inside and outside human hearing ranges and is usually used in marine surveillance
- **Visual surveillance** – this category can also include light, radar and aerial surveillance; technologies such as infrared, ultraviolet, satellites,

drones can be used; a popular technology used for this category is the closed-circuit camera television (CCTV)

- **Scientific surveillance** – this category include technologies that differ according to the purpose of a specific scientific study like the surveillance of chemical reactions, biological phenomena, human development, animal and plant life, genetics, etc.
- **Personal data surveillance** – this category uses databases to gather and store individual personal details like from identification cards, health records, store or facility member cards, birth or family certificates, etc.; this category can also include biometrics surveillance that uses human body scanning technologies like fingerprints, eyes or facial recognition devices

Surveillance technologies are developing faster than the laws are being drafted to regulate the technology itself or to balance their benefits against their potential harms. Surveillance is also used by competitive businesses for unethical purposes. Seemingly benign technologies, when used covertly to gather information of a competitive nature, may give an unfair or illegal advantage to the surveyor (Petersen, 2012, p. 22). However, it is undeniable that these tools are useful in several situations such as securing spaces like residential areas, shopping complexes, entertainment arenas, corporate or institutional buildings, etc. In addition, they also aid in criminal investigations, search-rescue operations, nature or wildlife observations, weather forecasting and scientific researches.

1.1.2 The Usage of Wiretapping for Communication Surveillance

This research focuses specifically on communications surveillance, which is accessing communication networks to monitor and/or record oral, written, or any other form of data transmitted through the network wires. This type of surveillance can be classified under the umbrella of acoustic and electromagnetic surveillances (Petersen, 2012, pp. 14-15). To conduct communications surveillance there are various methods that one can opt for, such as '*spy bugs*' or small microphones that can be attached near the target to eavesdrop any surrounding sounds. Another common device that can be used is the wiretap, which is the center of discussion in this study.

The definition of wiretapping itself is to covertly intercept and monitor conversations or sound waves flowing through telecommunication lines like telephone cables with the use of electronic or mechanical devices (Petersen, 2012). A wiretap is the device used for wiretapping; it basically catches patterns of electrical current fluctuations in a phone line and interprets them as sound (Harrison, 2002).[1] Earlier on, a wiretap involved physically linking circuits to direct the audio signals from the targeted communication line to a recording/listening post. But since telephone these days use digital technology, a computer system can ease wiretapping executions. Wiretaps are not only capable of intercepting communications on telephones but are also able to intercept communications on Internet-based services such as electronic mails (*e-mails*), social media platforms, chats and forums, online instant messengers, online

[1] Further technical information on wiretapping is discussed in Appendix A.

banking services, etc. (Duthel, 2014). The Internet made it easier for wiretapping and the increasing amount of Internet users benefitted such activities to target a larger crowd or also known as mass-surveillance (Bigo et al., 2013). Another communications surveillance method can be the collection of communication metadata[2] like Internet login records or phone call records, which does not include the actual content of the phone call. Authorities can gather communication metadata simply by obliging communication service providers to cooperate with them and pass on clients' records without the involvement of any wiretaps.

Wiretapping is indeed not a new phenomenon; only the technologies or methods used these days and in the past differ. Wiretapping began to increase in the 1890s after the invention of telephone recorders. One of the early wire-tappers was the 16th President of the United States of America (abbreviated as U.S throughout this research thesis), Abraham Lincoln. During the American Civil War, he listened in on telegraph conversations (McMahon, 2014). While earlier in the late 15th century, Queen Elizabeth I of England created a secret service division and imprisoned Queen Mary I of Scotland by intercepting her communication (Petersen, 2007). The U.S Kennedy administration also made use of wiretapping to monitor activities of Martin Luther King Jr. in 1966 (Garrow, 2002). Wiretapping was formerly targeted on specific suspected individuals, at least mostly, but now it can target just about anyone.

[2] Metadata are details of a communication such as the source, destination, time, duration of a phone call and at times the approximate location of the phone, but not its actual content (Jones, 2013).

With the current rise of cybercrimes happening globally, people became more cautious on what they post as well as on what they send and receive on the Internet. However, many people still seem to feel confident that communicating through their phone lines is secure, and they mostly might be, but only because no one is really interested enough to listen in. If their conversations were worthy enough to be tapped, it can easily be accomplished these days.

1.1.3 The Rise of Warrantless Wiretapping

The *spy world* has existed since a very long time ago. Surveillance was already popular in the late 15th century and according to Armand-Jean du Plessis, the Cardinal-Duke of Richelieu and Fronsac in France at that time, "secrecy is the first essential in affairs of the State" (Petersen, 2007, p. 23). Surveillance is a subset of the larger process of intelligence-gathering, and thus a key tool in intelligence operations (Petersen, 2007, p.4). Those days however, surveillance technologies were only available to a limited number of authorized people like government officials, law enforcers and the intelligence community, but nowadays they are accessible to public (Petersen, 2012, p.80).

Some countries actually do legalize wiretapping, for example the Performance Management and Delivery Unit (PEMANDU) in Malaysia proposed such an idea. The proposition was supported by Dato' Sri Ahmad Shabery Cheek, the Malaysian Communication and Multimedia Minister at the time; though he noted that to ensure a smooth execution, the associated legal matters have to be crucially studied before it is implemented (NST.com, August 2013). Likewise, the Russian President, Vladimir

Putin, stated such activities are essential in fighting terrorism, but he too advised "to limit the special services agencies with certain rules" (Isachenkov et al., 2013).

This paragraph introduces the standard procedures in the U.S for conducting a **legal** wiretapping operation or rather known to authorities as **legal interception** (Duthel, 2014). First of all, just like any authorized search and seizure for crime investigation purposes, a court warrant for the execution of wiretapping needs to be obtained and to accomplish that a 'probable cause[3]' needs to exist (Kaplan et al., 2012). The warrant is usually valid for thirty (30) days but an extension can be requested. After the completion of the wiretapping process, the conversation recordings or data gathered from the wiretap are then sealed by the judge, who authorized the wiretap, and are kept for a maximum of ten years (Boucher et al., 2001). Then, there is 'particularity', which is the requirement that the warrant shall particularly describe the communications or persons to be tapped to avoid any possible general or irrelevant conversations to be heard (Congressional Research Service, 2004).

Unfortunately, ever so often authorities neglect these procedures and find ways to circumvent them (Greene, 2014). These procedures are seen to be overly troublesome, time consuming and more prone to disclosure; as a result, warrantless wiretaps occur. To cut the hassle in obtaining a court warrant and save valuable investigation time, it became a popular trend amongst U.S law enforcement agencies to skip these legitimate administrative steps. Moreover, with no court processes, fewer parties will be involved and so the risk of public disclosures regarding the

[3] Further explanation on 'probable cause' is discussed in Appendix B (Probable Cause).

crime investigation will be less. The chance of the whole operation to stay undetectable or covert is higher.

In several cases, mostly concerning national security, wiretapping permits are easily obtained without being questioned and processed beforehand by the court or other entities authorized to approve such warrants (Duthel, 2014, p. 454). In fact, U.S law enforcers or its intelligence community are in the opinion that it is a normal or necessary thing to do. For example, a spokesperson of the U.S National Security Agency (NSA), an American intelligence agency, claimed wiretapping to be one of their duties, stating that the agency is "an element of the U.S intelligence community in charge of collecting and reporting intelligence for foreign intelligence and counterintelligence purposes […] engaging in the collection of signals intelligence […] through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire or other electromagnetic means" (Campbell, 2013, p. 2). U.S officials even mentioned that naturally "all countries engage in similar forms of espionage" (Lendman, 2013). More interestingly, Robert Décary, the then Commissioner of Communications Security Establishment Canada (CSEC), a Canadian intelligence agency, claimed that CSEC owns the right to spy on its citizens' electronic communications (Jones, 2013). According to the Wiretap Report 2013, wiretaps were used in the U.S to investigate major offenses including drug crimes, money laundering and homicide (Administrative Office of U.S Courts, 2013). General Keith Brian Alexander, a former[4] NSA director, also mentioned

[4] General Keith Brian Alexander retired in March 2014 after serving eight years at the NSA (Schwartz, 2014).

surveillance programs helped hinder around 54 terrorist attacks worldwide (Kelly, 2013).

As we can see from the examples above, those supporting wiretapping tend to associate it with national security. According to Jay Stanley, a senior policy analyst at the American Civil Liberties Union (ACLU), "national security is used to justify the existence and powers of intelligence services, but self-preservation, defense of prerogatives and reputation, and expansion of powers are truly mission number one" (Glaser, 2013).

Over the years, wiretapping did not only receive positive feedbacks. As a technology, wiretaps cannot be blamed, because basically the technology itself is something rather neutral and is neither meant to be helpful nor harmful. At most times, it is the purpose of implementation that is hardly neutral. The wrong purpose and unlawful execution of wiretapping can create negative impacts such as distrust, fear, curiosity, sexual gratification, unfair and illegal profit, exploitation and sales pressure (Petersen, 2007, p. 11). Individuals, especially those from human rights organizations and amusingly also several politicians, seem to oppose wiretapping practices. For instance, the former[5] Indonesian Foreign Minister, Mohammad Marty Muliana Natalegawa protested that such activities are unacceptable, illegal and immoral (Bachelard, 2013). Speaking for Indonesia as one of the targeted countries of U.S unlawful wiretapping operations, Natalegawa stated that "such action is not only a breach of security, but also a serious violation of diplomatic norms and ethics, and

[5] Mohammad Marty Muliana Natalegawa served as the Indonesian Foreign Minister in the Susilo Bambang Yudhoyono administration from 2009 until 2014 (Setiawan, n.d.).

certainly not in tune with the spirit of friendly relations between nations" (Kyodo News International, 2013). The former[6] U.S White House Press Secretary, Jay Carney, admitted that public revelations on the NSA controversial surveillance programs created economic and security tensions between the U.S and the aggrieved countries (Lendman, 2013). The European Parliament (Petersen, 2012, p. 61) also agreed that warrantless wiretaps contravene human rights conventions. A former Indonesian Coordinating Minister, Djoko Suyanto, added that it disrupts bilateral relations between the countries involved (Maryati, 2013). Such operations are unethical also because it increases the gap between advanced nations and nations with less advanced technology access. This caused plenty of civil liberty groups and organizations to provide awareness for civilians on the rise of improper government surveillance like warrantless wiretapping (McMahon, 2014).

Oddly, survey polls in the past years reflected that public has shifting opinion on wiretapping. A Los Angeles Times and Bloomberg survey poll conducted in April 2006 showed the majority of people considered the Terrorist Surveillance Program (replaced with the Privacy and Security Mirror or abbreviated as PRISM program[7]), which was an initiative by the former U.S President George Walker Bush, as an unacceptable way for the government to investigate terrorists. However, in another 2006 survey poll conducted by the Washington Post and ABC News involving 1000 randomly selected adults in the U.S, the majority of respondents (54 percent) had no problem if NSA were to intercept phone calls and e-mails of people inside and

[6] Jay Carney completed his serving period of three years as the U.S White House Press Secretary in the Barack Obama administration (Guthrie, 2014).

[7] Further explanation on what and how the PRISM program functions is discussed in a specific sub-chapter of this thesis (Section 4.1.1) on exposed U.S government communications surveillance programs.

outside of the U.S without a court warrant (Clement, 2013). In a 2011 survey poll conducted again by the Washington Post and ABC News involving 1001 randomly selected adults in the U.S, 77 percent of them were in the opinion that increased wiretaps and surveillance methods are effective in reducing the threat of terrorism (Craighill, 2011). Then in 2013, the question "Is it justifiable to violate certain civil liberties in the name of national security?" was posted on an online debate forum. Over a hundred online users participated in the poll with the result of 68 percent votes objecting that certain civil liberties shall be sacrificed for national security (Debate.org, n.d.). After analyzing the different questions used in these sample surveys, the researcher can conclude that the shifting public opinion on government surveillance is formed or perhaps influenced by the way the survey questions were worded; namely whether surveillance is posed as a bad or a beneficial thing. Though, it shall not be forgotten that an individual's perception of an issue, idea, concept or almost anything can also be influenced by other factors like the person's personality, expectation, experience, previous knowledge, political view, etc. (McLeod, 2007).

To sum up, there are two school of thoughts on how people view wiretapping (Eaton, 2014). The first thought is that the security of a nation needs to be prioritized. Hence, people or citizens of the nation should not feel burdened to give up a bit of their rights, in this case privacy rights, in order to achieve a greater benefit, namely national security with the goal to protect not only one but all other citizens. This thought is mostly owned by individuals supporting the totalitarianism and desiring few dominant powers to control the many others (Gregor, 2009). On the other hand, the opposing group questions whether it is worthy and constitutional to be giving a nation that much of a power. People with this school of thought, known as the

libertarians (Capaldi, 1983), are concerned on the invasion of individual privacy, especially freedom of expression (includes freedom of speech and association), that can be caused by government communications surveillance. To them, these kinds of activities are just a tool for governments to gain overly excessive power over its citizens and/or over other nations.

To prevent unethical government communication surveillance in the future, several resolutions were drafted such as one proposed to the United Nations General Assembly in November 2013 by Brazil and Germany. The approved General Assembly resolution 68/167 (United Nations General Assembly, 2013, p. 2) noted that "while concerns about public security may justify the gathering and protection of certain sensitive information, states must ensure full compliance with their obligations under international human rights law". Nations shall also "review procedures, practices and legislations on their communication surveillance". Another resolution (Sihite, 2013) was proposed in December 2013 by Indonesia with the support from Malaysia. The resolution was brought up during the 2014 Association of Southeast Asian Nations (ASEAN) Summit in Myanmar to prevent wiretapping and espionage amongst Southeast Asian nations.

1.2 Problem Statement

After the escalation in events of terrorist attacks, governments tend to increase the authority or power of their intelligence services and launched more 'blanket'[8] surveillance. The 'war on terrorism' or 'national security perseverance' is modestly used to justify the execution of covert operations like warrantless wiretapping by law enforcement authorities. With more U.S government communications surveillance programs being disclosed, a blurred line is created. It is also questioned by other parties how considerate these programs are to an individual's privacy.

The circumstances of such government activities being disclosed as unreasonable and immoral create feelings of distrust, anger and fear from citizens. So far, it has been quite challenging to contest the ethical or legal aspects of wiretaps in the U.S, especially those conducted without warrants. Citizens essentially lack legitimate protection against these sorts of government actions. Moreover, authorities are given the ability to ward off anyone and anything challenging their wiretapping operations by pulling out the 'sovereign immunity' and 'state secrets' cards. Any public disclosure requests on the information acquired from a wiretap will ordinarily be repelled with the same explanations by authorities. Ethical issues on wiretapping are also being contested, such as (1) how are the information or materials obtained from wiretaps disseminated, (2) are all the obtained materials analyzed, (3) are all authorities involved in the wiretap allowed to analyze the obtained material, (4) what if sensitive parts of the information unrelated to national security threats are

[8] In this context, a 'blanket' wiretapping operation means the wiretap is conducted on a large group of people without targeting a certain individual or suspect(s). This type of wiretapping operation is usually conducted warrantless because it does not go through any court process.

overheard, and (4) how can modification or alteration on the obtained information be hindered to ensure originality, integrity, accuracy and trustworthiness when it is used as court evidence.

Furthermore, if warrantless wiretapping operations are conducted across countries, it does not only breach individual liberties but it can create a greater impact towards diplomatic relationships. Such abusive use of wiretaps may also widen the economic gap between developed nations and nations that don't have access to technology. Another issue is warrantless mass-surveillance or mass-wiretapping, which most certainly involves the privacy of innocent individuals. Current international resolutions or agreements on the matter are seen as too broad and general. The lack of power and vague frameworks of these arrangements make it hard for nations to abide by them.

This study aims to analyze whether the debate on government warrantless wiretapping has been resolved in the U.S. National laws, court cases, incidents and other relevant information on wiretapping are looked into to identify how they have impacted national security and individual privacy in the country as well as how the U.S government has handled this issue.

1.3 Research Questions

1. To what extent have the disclosures of government communications surveillance programs been received in the U.S?
2. To what extent have wiretapping laws evolved in the U.S in regards to the protection of national security and individual privacy?
3. What do court cases regarding wiretapping in the U.S indicate in terms of national security and individual privacy?

1.4 Research Objectives

- To describe the feedbacks on how the disclosures of U.S government communications surveillance programs have been received and handled in the country.
- To examine the debate on the progress of wiretapping laws in the U.S in regards to the protection of national security and individual privacy.
- To examine the debate on the rulings of court cases regarding wiretapping in the U.S in terms of national security and individual privacy.

1.5 Research Significance

This study aims to acknowledge whether a resolution to the ethical dilemma on balancing national security and individual privacy rights in association to government communications surveillance, specifically warrantless wiretapping, is achievable. If it is still not, this study shall expose the different influences or causes of why it is something relatively difficult to accomplish. The goal of this research however is not to specify a certain resolution towards the matter, but rather to explain what can be done to moderately diminish the aforementioned imbalance.

As one of the major agents of surveillance, the U.S is looked into to examine how the wiretapping world runs there. By exposing positive and also negative or less constructive measures carried out by the country to handle the matter, it is expected to provide insights for other countries on what actions can be adopted and what can be avoided. It is hoped that the results can intrigue other nations to enhance their legal framework or any decision making on the matter.

The study also aims to provide awareness regarding wiretapping not only to the public, but also awareness to governments and authorities with the attempt to contribute or influence a nation's policy by laying out facts that there are indeed negative criticisms on wiretapping. It is important to understand all relevant aspects of the issue in order to be able to have a clear standpoint. And from there, clear applicable legislations and legal procedures on the conduct of wiretapping or surveillance in general can be established.

1.6 Definition of Terminology

1.6.1 National Security

It is rather difficult, if not impossible, to find a general or standard definition of national security, because each state even each individual has their own definition. According to Buzan, before asking what a person is willing to give up to obtain more security, the person has to first identify his own concept of security (Baldwin, 1997). National security is so ambiguous that it is often referred as a confused or an inadequately explained concept. At times, the term is related to the goal of a state to excel in fields like economics, environment, food supply, military, human welfare, etc. According to Hart and Kennedy, a nation can have a strategy by combining military, political and economic aspects to achieve its ultimate objectives in the international system, which means each nation may have different strategies to deal with other nations (O'Connor, 2013). No theory can specifically set how much or what values have to be achieved for a nation to be considered as a secure or safe place, because surely every nation has different concepts and interests in what needs to be protected.

National interests are goals that are identified by a particular state (actor), because they are deemed to have positive impacts on the state and its citizens. Henry Kissinger and Robert Art pointed out that the identification of these interests is quite important for a nation to develop clear policies and strategies (Bartholomees, 2010, p. 3). Furthermore, it could "enhance the political, economic, security, environmental, and/or moral well-being of a populace and the state or national

enterprise to which they belong", as Robert D. Blackwill stated (Bartholomees, 2010, p. 4). National interests according to Hans Morgenthau are permanent regardless of the governing power, time or place. However, some others debated that national interests are "a diverse, pluralistic set of subjective preferences that change periodically, both in response to the domestic political process itself and in response to shifts in the international environment (Bartholomees, 2010, p. 5).

Due to the ambiguity of the term security itself, there are guidelines (Baldwin 1997) to simplify the creation of a concept by questioning (a) whom should be secured, (b) what values should be secured, (c) how much security is needed (d) what threats should be avoided to be secure (e) what means can be pursued to ensure security (f) at what cost can security be ensured and (g) how long can security be ensured. It is also mentioned that the more security a person has, the less that person will value an increase of it.

The U.S government's take on the term national security is defined by its Department of Defense (DoD) into three main aspects, which actually received some criticism claiming them to be unclear and not quite cohesive (United States Department of Defense, 2015, p. 164):

> "A collective term encompassing both national defense and foreign relations of the United States with the purpose of gaining: a) a military or defense advantage over any foreign nation or group of nations; b) a favorable foreign relations position; or c) a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert."

Another suggested definition for the U.S national security is "the ability of national institutions to prevent adversaries from using force to harm Americans or their

national interests and the confidence of Americans in this capability" (Sarkesian et al., 2008, p. 2).

Under the Barack Obama administration, the first U.S National Security Strategy (NSS) was released by the White House in May 2010. It listed four main national interests including the U.S government plan of strategies to achieve those goals, such as the following (United States White House, 2010):

1. **Security** → The security of the state, its citizens, its allies and partners.

   Strategies (pp. 18-27):
   - *Strengthen security and resilience at home*
   - *Disrupt, dismantle and defeat Al-Qa'eda including its violent extremist affiliates in Afghanistan, Pakistan and around the world*
   - *Reverse the spread of nuclear and biological weapons and secure nuclear materials*
   - *Advance peace, security and opportunity in the greater Middle East*
   - *Invest in the capacity of strong and capable partners*
   - *Secure Cyberspace*

2. **Prosperity** → A strong, innovative and growing U.S economy in an open international economic system that promotes opportunity and prosperity.

   Strategies (pp. 29-34):
   - *Strengthen education and human capital*
   - *Enhance science, technology, and innovation*
   - *Achieve balanced and sustainable growth of home and global economy*
   - *Accelerate sustainable development*
   - *Spend taxpayers' dollars wisely*

3. **Values** → Respect for universal values at home and around the world.

   Strategies (pp. 36-39):
   - *Strengthen the power of our example in spreading freedom and democracy abroad*
   - *Promote democracy and human rights abroad*
   - *Promote dignity by meeting basic needs*

4. **International Order** → An international order advanced by U.S leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges.

   Strategies (pp. 41-50):
   - *Ensure strong alliances*
   - *Build cooperation with other 21st century centers of influence*
   - *Strengthen institutions and mechanisms for cooperation*
   - *Sustain broad cooperation on key global challenges*

The latest U.S National Security Strategy was released in February 2015. Even though it was also written during the Obama administration, it has added and removed some of its strategies to achieve the previous four main national interests (United States White House, 2015):

1. **Security** → To achieve security of the state, its citizens, its allies and partners.

   Strategies (pp. 7-14):
   - *Strengthen our national defense*
   - *Reinforce homeland security*
   - *Combat the persistent threat of terrorism*
   - *Build capacity to prevent conflicts*
   - *Prevent the spread and use of weapons of mass destruction*
   - *Confront climate change*
   - *Assure access to shared spaces (cyber security, space security, air and maritime security)*
   - *Increase global health security*

2. **Prosperity** → To achieve a strong, innovative and growing U.S economy in an open international economic system that promotes opportunity and prosperity.

   Strategies (pp. 15-18):
   - *Put our economy to work*
   - *Advance our energy security*
   - *Lead in science, technology and innovation*
   - *Shape the global economic order*
   - *End extreme poverty*

3. **Values** → To respect universal values at home and around the world.

   Strategies (pp. 19-22):
   - *Live our values*
   - *Advance equality*
   - *Support emerging democracies*
   - *Empower civil society and young leaders*
   - *Prevent mass atrocities*

4. **International Order** → To achieve an international order advanced by U.S leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges.

   Strategies (pp. 24-28):
   - *Advance our rebalance to Asia and the Pacific*
   - *Strengthen our enduring alliance with Europe*
   - *Seek stability and peace in the Middle East and North Africa*
   - *Invest in Africa's Future*
   - *Deepen economic and security cooperation in the Americas*

In terms of **security**, the U.S was still focused in the process of bringing wars outside the country to a responsible end, whereas now the government places more focus on its own defense and security. Although combatting terrorism, worldwide capacity building, mass destruction weapons prevention and cyber security are still listed as strategies, other security areas of concern were added in 2015 such as health security, space security, air and maritime security as well as concerns on climate change.

In terms of **prosperity**, the U.S has changed its attention from ensuring the quality and management of human resources in the country like education aiming for a sustainable development and economy nationally and globally to now ensuring the quality and management of its own resources in order to be able to shape and lead the economic order worldwide.