Committee: Special Conference on Global Reform and Ethics

Issue: Ensuring individual privacy in the digital era

Student Officer: Alkistis Giavridis

Position: Deputy President

INTRODUCTION

Technology. One, simple word and a huge, complex world, at the same time. It's worth taking a moment to look at what the human race has done in the past 25 years, what we have achieved through hard work, team spirit and dedication. We have reshaped the world of communications; we have created a whole new way of life; we endorsed the digital era. An era filled with countless benefits and profits, but also an era that brings new challenges and potential risks.

Thanks to Information Communication Technologies (ICTs), communicating with each other seems simpler than ever; we have easier and immediate access to information and most importantly, we have managed to create a whole new work sector. The reimbursements of technology could form an endless list, but what we should not forget is that due to the countless benefits of ICTs, today's human is also very reliant on technology - maybe more than he should be. And this reliance enhances the potential dangers that technology poses, not only to international security but also to individual privacy.

There have been countless cases where the fact that it is extremely easy to gain access to someone else's personal data and information has been exploited, through carrying out cyber espionage, surveillance as well as interception. Governments, for example, often claim that surveillance is a necessity in order to protect a society from certain dangers such as terrorist attacks, but often the actions to safeguard someone are not in compliance with maintaining the person's right to privacy. Privacy is one of our most vital human rights, a right that should not lose its value in cyber space. As a famous man once said, "Privacy is not something that I'm merely entitled to. It's an absolute prerequisite".

DEFINITION OF KEY TERMS

Domestic Surveillance

Surveillance refers to the observation, supervision and/or the monitoring of a specific person or a group of people, generally by the authorities, and is not only restricted

to visual observation. The adjective "domestic" is applicable when describing something that is not foreign or international, but only relates to one specific country, in most cases one's own country. In conclusion, domestic surveillance refers to the close watching over a specific person or a group of people by his/her/their own country.

Search Warrant

A search warrant is a legal document that gives police authorities the power to collect information about a suspect, in order to prove the person's guilt or innocence. Often this document needs to be used, as pieces of information or data are often protected by the Fourth Amendment that clearly 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".

Information Communication Technology (ICT)

The term ICT mainly deals with all types of technology used by both individuals and organizations to gain access to information. These types of technology range from radio, cellphones and television to satellite systems, wireless networks and computer hard- or software. The term is often used in association with education.

Intelligence

Intelligence refers to the gathering and analyzing of an enemy's or potential enemy's information that is sensitive and/or secret, mostly by a specific government. The dictionary of the United States military terms for Joint Usage defines intelligence as "the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operation and which is immediately or potentially significant to planning."

Internet Freedom

Even though there is not one, universally accepted definition for Internet freedom, the term mainly refers to free and unrestricted flow of information on the Internet, without interference from any government.

Cyber Espionage

Espionage deals with the action of spying, or hiring other people to spy, on a specific group of people, often governments, in order to get access to information and/or audiovisual material that is not disclosed to the public. When talking about cyber espionage,

though, we refer to the use of certain computer systems that facilitate the carrying out of the espionage.

Cyber Security

Cyber Security, also referred to as Information Technology (IT) Security encompasses all measures that need to be taken, in order to safeguard and protect computer networks and systems, as well as pieces of information and data from cybercrime.

Cyber Warfare

Cyber Warfare includes all sorts of virtual conflicts that are instigated by both state and non-state actors for political reasons, targeting the IT networks of an enemy or even a possible enemy. Cyber Warfare includes attack forms such as, but not limited to, sabotage, cyber espionage, denial-of-service attacks and lastly the spreading of Trojans, viruses, worms and malware.

BACKGROUND INFORMATION

Sony Pictures Hack

Starting in October 2014, there was a major hacking attack on the computer systems of the company "Sony Pictures". Several pieces of sensitive data were stolen in the attack, as well as private information about some of the company's recent film productions that was later on exposed on the Internet as well. The hijackers, using malware, also damaged and destroyed an utmost amount of data on Sony's computer devices. Reporters described the attack as an act of blackmail, that was carried out by a group of hackers, calling itself "Guardians of Peace" (GOP). In mid-December, the U.S. officially stated that the government that hired the group, and the government that therefore was responsible for the attack was the Democratic People's Republic of Korea (DPRK), also referred to as North Korea. The believed motive behind the attack is the Sony-backed movie "The Interview", that was to be released in October 2015 and had a rather provocative plot towards the DPRK, as it revolved around the assassination of North Korean leader Kim Jong-Un. After numerous warnings and threats by the GOP, saying that any cinema screenings of the movie would be attacked, several theaters refused to play the movie and in conclusion the theatrical release of "The Interview" was cancelled. Responding to this incident, President Obama stated that he believes that the cinema release should not have been canceled by Sony Pictures and added that "We cannot have a society in which some dictator some place can start imposing

censorship here in the United States". The company itself responded to the whole situation, saying that the only reason they finally decided to temporarily cancel the release of the movie was to keep civilians safe from any form of attack. They also added that it was not their choice after all, as the theaters were the ones that refused to show the film. Only two days after the first threats by the GOP, the group made new demands, pointing out that the whole movie should sort of "vanish". Anything in association with it such as teasers, trailers and scenes of the movie should be completely obliterated and the movie should never be "released, distributed or leaked in any form of, for instance, DVD or piracy" (GOP). Finally the movie was released, 2 months after the initial release date, on December 24th 2014 in numerous theatres and on other digital platforms such as YouTube, Google Play and Netflix.

The commercial use of 'Cookies'

'Cookies', also referred to as 'magic cookies', are small text files that are collected on the user's PC and are sent back and forth between computer systems and computer servers. The main idea behind cookies was the personalization of online search engines, in other words to make internet browsing more practical and time-saving, as they could be used for multiple purposes such as remembering shopping lists when online shopping or making the computer "remember" passwords in form of a cookie. In that way, when attempting to log into e.g. a social network, the user did not have to retype their password again every single time they logged into the system.

In the past years, cookies have often been used for so-called "commercial purposes". This means that companies use the information on the cookies, such as recent searches and browsing habits, and with that information choose specific products that the user is most likely interested in and advertise them via Internet banners. Digital marketing provider corporations such as DoubleClick therefore use the data that the cookies provide and link certain Internet users with certain advertisements. Another goal of such companies is to ensure that not the same banners keep popping up on a person's screen. This is achieved through keeping record of the number of times that a certain banner has been shown to the customer at the websites that uses advertisements of DoubleClick customers.

Although cookies offer numerous benefits, such as creating a more personalized web experience for the user, many claim that they are facilitating invasions of privacy for numerous reasons. First of all, when visiting websites with ads, third party cookies are often placed on the user's PC, with the result that the third-party cookies are then saved by Internet servers that have the ability to access the user's data. While most of those third

parties involved use the information to advertise and sell more products, there is always the danger that the information might be sold to an individual or a group with malicious purposes for example hacking into a person's Internet accounts. Also others dislike the general idea of their browsing activity being saved and passively monitored, as they consider that browsing habits are something very private and personal that should not be used for the sake of advertisement.

Leaks by Edward Snowden

Verizon

The first revelation of Edward Snowden disclosed that the U.S. National Security Agency (NSA) was collecting the mobile phone records of millions of U.S. citizens. An article, published by the Guardian in June 2013, exposed a top secret court order by the foreign intelligence court forcing the communication technology company Verizon to hand over "all call details or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls". This so-called "metadata information" includes caller ID, receiver ID, call duration as well as the time and place the call found place. The order was untargeted and widespread, in other words the NSA basically had the possibility to monitor any U.S. citizen's phone call, no matter if that person even was suspected of any crime.

PRISM

Soon after the Verizon revelations, two other articles followed, revealing another surveillance program that was being used by the NSA, called "PRISM". Due to the Guardian and the Washington Post, the program allowed the NSA to directly access the servers of nine prominent Internet services including Facebook, Google, YouTube, Skype and Yahoo, and compared to Verizon, PRISM did not only disclose metadata information but also the content of conversations on those Internet services. On the other hand, the New York Times, along with several other newspapers, believes that the program only collects and analyzes data that was legally requested by the NSA. Due to the Obama Administration, the program does exist, and is also legal under Section 702 of the Foreign Intelligence Surveillance Act (FISA) that was amended in 2007 and later on renewed in 2012. The companies that were supposedly a part of the program all denied the allegations made about them. Many stated that they had nothing to do with such a program, that they didn't even

know it existed and lastly that the only case where they give away users' data is when there is a specific, legitimate court order about specific identifiers. Apart from the NSA, the British intelligence and security organization Government Communications Headquarters (GCHQ) also allegedly used PRISM to gather information from the world's biggest Internet firms, and has been using the program since June 2010.

EU offices and its computer systems

Due to further revelations by former NSA contractor Edward Snowden, in June/August 2013 the German newspaper "Der Spiegel" reported that the NSA has also been spying on computer networks of the UN in New York and on European Union (EU) internal networks in New York and Washington D.C. In addition, the intelligence agency was supposedly digitally eavesdropping on the EU Council of Ministers and the European Council in Brussels as a result of the cracking of the UN encryption system and the furthermore hacking into a private communication network that was being used by EU diplomats. While there have been numerous attempts by the U.S. to deemphasize and downplay the incidents, German Chancellor Angela Merkel, whose phone was also allegedly monitored by the NSA, responded to the spying actions, pointing out that allies should work together and not spy on each other, and that due to the latest incidents a relationship of trust needs to be rebuilt between Germany and the U.S..

Computer Hacks in Hong Kong, China

After fleeing to Hong Kong in May 2013, the whistleblower Edward Snowden revealed to the South China Morning Post that the NSA had also been carrying out hacking attacks on Chinese educational institutions, mobile systems and businesses. The former NSA contractor proved those allegations by presenting information that he could have only received either by a foreign security officer or by having physical access to Chinese computer systems. Snowden claimed that the NSA has been targeting Chinese systems for several years now and that a huge number of NSA's hacking operations, in particular 61,000, were directed at Chinese mobile phone companies and a popular research institute, the Tsinghua University in Beijing.

XKeyscore

According to documents leaked by Edward Snowden, the NSA used another program called "XKeyscore" that basically gave them access to all aspects of a person's

Internet activity. This includes the content of conversations, browsing history as well as metadata information. The agency described the system as their "widest-reaching" program for the development of intelligence from the Internet and in general computer networks. XKeyscore does not require any form of authorization such as a warrant, and it gives its users access to the complete database of a person's information, so basically everything that the person has ever done on the Internet. In an interview, Snowden claimed that due to XKeyscore he had the ability to wiretap any person whose email address he knew. Analysts using XKeyscore do not need any prior authorization, they can access someone's data by just filling in a simple onscreen form, where they broadly explain the reason of the search, that is not even viewed by any type of court or the agency's personnel before being processed. The NSA claimed that those allegations were not true and that only a limited number of employees had access to XKeyscore, and only at times when it was necessary in order for them to fulfill their assigned tasks. The agency added that such programs are necessary so as to protect the nation and the people that live in that nation from potential dangers.

The monitoring of 35 world leaders

In October 2013, new documents were leaked, in particular a confidential memo, showing that the NSA was asking government officials to give out any contact information of heads of states, worldwide. After having received over 200 numbers by a U.S. government official, it was revealed the NSA was monitoring the phone calls of 35 world leaders. These revelations enhanced already existing tension (as a result of the monitoring of German Chancellor Angela Merkel's phone calls) between the U.S. and its allies, and after such a scandal, the countries' relationship of trust and cooperation has been seriously harmed. As a response to the allegations called by Mrs. Merkel, the White House press secretary stated that the U.S. "is not monitoring and will not monitor" the German chancellor's phone device. What raised a lot of suspicion about the agency's justification was the fact that it did not refer to any of the NSA's past actions, concerning the monitoring of several heads of states.

MAJOR PARTIES INVOLVED

The Public Sector

One of the major parties that are involved in the issue is the Public Sector. Public bodies in cooperation with the private sector are usually the ones that disrupt individual privacy as they use surveillance programs, mostly in an invasive matter, that give them access to a vast amount of personal data of their citizens. An example would be, as stated in the section above, the mass surveillance of the U.S., using programs such as PRISM, Verizon, XKeyscore and other systems to gather information. Governments often justify the use of surveillance systems, saying that observation of their citizens is necessary in order to identify and later on prevent criminals and terrorists from attacking innocent civilians and therefore ensure national security in the long run. Especially after the Paris attacks in January 2015, whose impact is comparable to the ones of 9/11, many heads of states drastically enhanced surveillance powers. The French government heightened its national security system "Vigipirate" to the highest possible level and also approved a new anti-terror law, the "French-Style Patriot Act", whose goal is the improvement of the state's Internet surveillance as the Internet is often used for terrorist purposes such as spreading ideology as well as planning and financing attacks.

Society

Responding to the measures taken after the Paris attacks, hundreds of people demonstrated, claiming that the proposed law is a violation of one of their basic Human Rights, the right to privacy. Furthermore, the NSA revelations caused public outrage and masses of people complained as they felt that the NSA has violated the principle of sovereignty by first of all spying on civilians and secondly not informing them about it, thus taking away another right of them, the right to voice their opinion about the incident. Civilians therefore expect that some kind of balance should prevail, so that security does not exist at the cost of individual privacy.

Internet Corporations and Telecom Providers

Internet Corporations and Telecom Providers in the private sector also play an important role in this matter, in two different ways;

Firstly, there are companies in the so-called "cybersecurity" industry, such as Hacking Team, Gamma Group and Trovicor, which supposedly safeguard and protect software while defending clients from cyber attacks. Some claim that in reality, these companies sell programs that function as "digital mercenaries" and their main goal is,

allegedly, not to provide security, but to practice cyber crimes such as cyber espionage and offensive hacking.

The second type of technology companies that play a major role in aiding the public sector are Internet Services such as Facebook, Google and Skype. Compared to the spy-tech firms, these Internet companies are accused of giving governments access to metadata information as well as the content of communications of their users, not always knowingly and willingly.

Non-Governmental Organizations (NGOs)

Lastly, NGOs are also an important body in the fight against excessive governmental surveillance, as they support civilians by hosting projects that have the goal of protecting peoples' rights –online and offline. The organization that has taken the lead in solving the issue is the Electronic Frontier Foundation (EFF), fighting in court to protect the right of privacy, next to many others, in the digital world. One of its many projects concerning the law and technology of government surveillance is the so-called "Surveillance Self-Defense project". It is designed to help individuals protect themselves from surveillance as much as they can, by educating them on the dangers of cyberspace and how they can avoid them.

TIMELINE OF EVENTS

Date	Description of Event
1995	The development of the cookies for the Internet by the Netscape Communications Corporation.
December 2003	A group of hackers, allegedly Chinese in origin, codenamed "Titan Rain" launched a cyber attack in November 2003, which went on for roughly 3 years. Military systems of the government were targeted by the group, as it tried to access sensitive data and information.
December 16, 2005	The New York Times discloses the NSA's surveillance actions for the first time, publishing an article that accuses President Bush of calling on the NSA to conduct warrantless domestic surveillance in order to track any terrorist activity. The spying actions are confirmed by the President one day later.

October 2007	China's Ministry of State Security accuses the United States and Taiwan of information theft from Chinese key areas
July 10, 2008	The FISA Amendment Act is passed by Congress, which legalizes some of the NSA surveillance actions revealed by Edward Snowden, due to a loophole that authorizes the conducting of digital surveillance of law-abiding Americans
April-October 2008	The journalistic organization WikiLeaks reports that "50 megabytes of email messages and attaches documents, as well as a complete list of usernames and passwords from unspecified (U.S. government) agency" were successfully stolen by a hacker Group in Shanghai associated with the People's Liberation Army
March 2009	An espionage system that was allegedly implanted by China-based hackers in the offices and embassies of government officials was discovered by Canadian researchers
August 2010	The Pentagon declares that along with land, air, sea and space, cyber space is the new domain of warfare
April 2011	Google reports that a phishing attack had been carried out on its email systems with the goal of accessing prominent people's passwords
June 5, 2013	The Guardian published a Secret Court Order proving that the NSA had been collecting the metadata of US Verizon users
June 7, 2013	Soon after the first Snowden revelation, another one follows exposing another surveillance program called PRISM, used by the NSA to monitor the content of conversations on renowned Internet services including Facebook, Apple, YouTube and others.
June 13, 2013	The newspaper New York Time reveals that Skype was running a program called Project Chess, that allowed the NSA to conduct spying activities on Skype users
June 21, 2013	The NSA's British equivalent, GCHQ, is exposed in a Guardian report

June 27, 2013	The Guardian releases a NSA Draft Report, revealing a timeline of spying actions that the NSA had carried out in the past
October 2013	The NATO takes several measures to improve the security of its networks, after they had suffered approximately 2,500 attacks in 2012 alone. The 58 million Euro project is completed by the end of October, and basically involves an upgrade of NATO's cyber defense systems
December 18, 2013	Resolution A/RES/68/167 about the right to privacy in the digital age gets adopted by the UN
March 2014	China and Pakistan allegedly practiced online espionage on India's armed forces systems and defense research organization mechanisms
November 2014	A hacker group, allegedly employed by the DPRK infiltrates Sony Pictures' networks, accessing and later on exposing sensitive information about the company's recent productions to the public
April 2015	The Russian Federation is blamed for the 2014 attack on the White House's and the State Department's email systems
July 2015	Office of Personnel Management (OPM) director, Katherine Archuleta, resigns a day after an immense data breach attack on the agency finds place. Social security numbers, next to other pieces of sensitive data of over 21 million people, including government officials as well as people from outside the government, were stolen in the attack

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

- http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

UN resolution on the right to privacy in the digital age – 21 January 2014

- http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/043/88/IMG/NR004388.pdf?OpenElement

Article 12 of the Universal Declaration of Human Rights (UDHR) "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." – 10 December 1948

- http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Article 17 of the International Covenant on Civil and Political Rights "No one shall be subjected to arbitrary interference with…" – 16 December 1966

- http://www.echr.coe.int/Documents/Convention_ENG.pdf

Article 8 of the European Convention of Human Rights (ECHR) "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." – 4 November 1950

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The European Union has been the trailblazer in solving this complex issue by drafting various documents that propose measures that need to be taken in order to protect the peoples' right to privacy. One of the documents, named "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" explicitly defines and analyzes all aspects of the issue of data protection, and how it can be achieved on national and international level. Apart from that, in January 2012 the European Commission also introduced certain changes to the EU's data protection rules of 1995, with the main intention of safeguarding the citizen's personal data as well as offering them an improved digital economy. Europe's Data Protection Directive also proposes several norms that serve for the insurance of citizen's data transfers, abroad.

Moreover, several NGOs such as the EFF, Privacy International and The Association for Progressive Communications have been proven to be significant bodies in addressing the matter, not only as they helped raise awareness about this problem, but also by drafting countless reports that underline the importance of the formation of norms, treaties and guidelines that clearly govern the use of ICTs, in terms of also respecting the autonomy of individuals. The EFF, for instance, has launched several projects, one of them being the "Surveillance Self-Defense project", whose main aim is to help individuals protect their personal information, through educating them on the potential risks that they will most likely encounter in cyber space.

POSSIBLE SOLUTIONS

First and foremost, we need to continue to raise public awareness about this issue. If there is no controversy and no countermovement against excessive cyber surveillance, governments will continue to exploit the vulnerabilities of technology and use them in order to gather sensitive data. This data and information gives them more power, as they can use it for basically anything, including commercial purposes that may harm the affected citizens.

Another key move that needs to be done in order to effectively tackle the issue is to use international law in order to regulate the government's interference into the citizens' private space. Several nations have often exploited the loopholes in legislation, which allowed them to legally employ warrantless domestic surveillance on citizens that were not even suspected of having committed any crime. As long as excessive cyber surveillance is legal and authorized in certain parts of the world, it is impossible to find a way to protect civilians' rights in cyber space. Therefore, we need to move towards the formation of International legislation that balances out a state's security measures and the invasion on individual privacy of its citizens. Apart from that, the whole surveillance process should go through with transparency, in other words the type and degree of surveillance measures should be explicitly defined and demarcated to the public. Furthermore, a regular renewal of the legislation regarding this topic should be considered, as technology nowadays advances rapidly. In that way outdated and therefore irrelevant legislation that could later on lead to the creation of new loopholes can be easily avoided.

In the digital era that we live in, it seems almost impossible to ensure security while not disregarding the fundamental right to privacy. Therefore, it might seem like a great challenge to find effective measures to tackle this serious issue, but we believe that by creating a climate of cooperation between the public sector, the private sector and the civil society anything can be achieved. As a wise man once said, "It always seems impossible until it is done".

BIBLIOGRAPHY

"All About Computer Cookies - Privacy Concerns on Cookies." *Allaboutcookies.org*. N.p., n.d. Web. 30 Aug. 2015.

Ball, James, and Spencer Ackerman. "NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls." *Theguardian.com*. N.p., n.d. Web.

"Edward Snowden: Leaks That Exposed US Spy Programme - BBC News." *Bbc.com*. N.p., n.d. Web. 30 Aug. 2015.

"EU Member States Approve Changes to Data Protection Rules." *RTE.ie*. N.p., n.d. Web. 30 Aug. 2015.

Gidda, Mirren. "Edward Snowden and the NSA Files – Timeline." *Theguardian.com*. N.p., n.d. Web.

Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *Theguardian.com*. N.p., n.d. Web.

Grisham, Lori. "Timeline: North Korea and the Sony Pictures Hack." *Usatoday.com*. N.p., 05 Jan. 2015. Web. 30 Aug. 2015.

Jegatheesan, Sowmyan And Usability. "Cookies – Invading Our Privacy for Marketing, Advertising and Security Issues." *Cookies – Invading Our Privacy for Marketing, Advertising and Security Issues* (n.d.): n. pag. *Arxiv.org*. Web.

Passeri, Paolo. "Category Archives: Cyber Attacks Timeline." *Hackmageddon.com*. N.p., n.d. Web. 30 Aug. 2015.

Perez, Evan, and Shimon Prokupecz. "How Russians Hacked the White House." *CNNPolitics.com*. N.p., n.d. Web. 30 Aug. 2015.

Peterson, Andrea. "The Sony Pictures Hack, Explained." *Washingtonpost.com*. The Washington Post, n.d. Web. 30 Aug. 2015.

"The Tech Terms Computer Dictionary." *Techterms.com*. N.p., n.d. Web. 30 Aug. 2015.