Human Rights Council

Protecting individual privacy while maintaining national security

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Teresa Peregrina Alba

Forum:	Human Rights Council
Issue:	Protecting individual privacy while maintaining national security
Student Officer:	Teresa Peregrina Alba
Position:	Deputy President

Introduction

Individual privacy can involve several issues among that of online privacy; due to the rising concern for this generation.

Providing protection for citizens serves as an obligation to Governments, as well as establishing the requirement of protection for themselves. This purpose can only be fulfilled with the necessary information that will authorise their acknowledgement of the occurrence of possible threats. This is mainly done through the usage of digitally stored information.

In 2013, declarations occurred involving the National Security Agency (NSA) by Edward Snowden; causing a statement of debate regarding the capability of governments to gather and retain information, having the determination of enhancing national security. However, some individuals believe that this could be considered a violation act to the civil rights of privacy, on the other hand others argue that, to sustain national security this measure is necessary. Consequently, it can be seen to be of major importance to assure that the rights to privacy of citizens are followed accordingly with the government's compilation of information to protect and strengthen national security.

Definition of Key Terms

Privacy

Privacy can be defined as the state of having freedom to oneself, which includes no public damage, confidential surveillance, or the usage of unapproved declarations of an individual's private data by means of a corporation and government. *("Privacy.", dictionary.com)*

National Security

National security has been seen to be reflected as the protection of individual's data as a defence strategy from possible attacks.

General Data Protection Regulation (GDPR)

The GDPR came into use on the 25th of May 2018, this concerns privacy regulations within countries of the European Union and the European Economic Area (EEA). The use of individual privacy is restricted regarding countries that are not within the EU and EEA; their objective is for the citizenry to gain awareness and authority of their usage of personal data and through the merging of the EU regulation, global trades and transactions demonstrate a simplification of the regulatory environment.

Data encryption

Data encryption can be defined as the security of an individual's data that is restricted to only the people who are aware of the decryption key. This approach to secure information is most commonly employed by organisations. The data that is encrypted is generally known to as ciphertext, and the data that in unencrypted is referred to as plaintext.

US prism

The Prism was founded in 2007, due to the change of the legislation regarding surveillance performed by the US. This programme has the objective of obtaining information from he most known companies throughout the world, these being Facebook, Apple and Google among others. However, they have the capability of receiving data concerning an individual's activity online, and further intruding into their private information, such as chats and emails.

General Overview

Past events

The terrorist attacks on the 11th of September, known more commonly as "11S", occurred due to the hijacking of four jet airliners that belonged to the US. Consequently, three managed to crash at their destined target, those being, the Twin Towers of World

Trade Centre located in New York and the The Pentagon located in Virginia. The fourth thankfully did not reach its set area for crashing, and instead made its way to a field, in which the jet landed, situated close by to Pennsylvania. This provoked the government of the United States to acknowledge the necessity of an enhancement towards their national security, and further causing an emphasis to fall upon the protection of national security instead of the privacy of an individual. Subsequently, experts have claimed that if they had known specific information, the attacks could have been avoided.

Use of technology

Through the enhancement of modern technology, major increment has occurred to the collection of personal data. Due to the facilitation of this process, agencies and nations perform this collection through thorough observations. This process became well known to the public, under the revelations of Edward Snowden concerning the incorrect usage of information of the NSA and US; these as well being private conversations held by the citizenry. These caused an outrage to the international community and for them to further question the legality of these actions, most importantly regarding the management of their information in relation to the right of privacy being violated, in order to combat terrorism internationally and for national security to be protected.

Cookie law

The Directive 2002/58 about Privacy and Electronic Communication, better addressed as Cookie Law Directive or formally E-Directive pertains the issues involving the protection of data and privacy in Europe. This Directive is applicable to the companies that have a link within the member states of Europe, (however this does not depend upon if the collection of information is present or not); these companies have the purpose of obtaining information concerning the citizenry of the European Union. The jurisdiction of the Cookie Law Directive is subjected towards the placement of cookies upon a EU citizen by any company. Nonetheless, the EU citizenry's data is satisfactorily protected causing their information to have the possibility of incorrect usage; thus proving that the E-Directive is not sufficiently productive. In the European Court of Justice (ECJ), the European Commission revealed that this Directive is counterproductive and is not able to secure the data of

EU habitants, in order to prevent this from being collected by the United States in forms that remain unspecified. This has been presented to the court due to the lodgement of numerous protests regarding the US companies of: Yahoo, Skype, Microsoft, Apple and Facebook. *(CLEI Policy Brief, Rocio Peregrina Alba).*

Right to privacy

Individual redress is also an important factor that has to be addressed in relation to Directive 95/46/EC and more specifically Article 28(4); as well regarding the European Charter of Fundamental Rights, in particular its Article 47. According to the Article 47, one is rightfully able to attain a trial and a legal remedy. In accordance with Article 28(4), if one feels as if their privacy is being violated committed, they may register a complaint. Since one can have an effective remedy, there is the right for their capability of decision making.

Current problems

The revelation of the data released by Snowden, as well contained information regarding US programme, entitled “Prism”; this permitted the free access of the texts and emails received by the customers. In 2015, the Congress held a vote upon the retrieval of data, to which resulted in the cease of the gathering of bulk data from the NSA. Due to this, investigators have gained admission to the records stored by the mobile phone companies, only with the warrant of the court. Furthermore, in this year, the surveillance of US information were revealed, causing the European Court of Justice (ECJ) to propose a cease to the Safe Harbour Agreement; which granted the transportation of commercial information from the consumers within the EU to companies of US. Consequently, there was an increment to the protection given to the citizenry of the EU.

Due to the leaks from Snowden, concerns have risen regarding privacy; causing the addition of data encryption for the products of several technology companies. The government of the United Kingdom renewed the encryption pertaining calls, as a consequence of the Manchester attacks in 2017; permitting the view of this information when demanded by investigators. Encryption as well became a subject in the United States, when the iPhone of an attacker of the December 2015 terrorist assaults, was obtained by an investigator; Apple

was instructed for the creation of a software that would allow getting through the encrypted password set. However, Apple did not agree and argued that this could provoke all their customers data to not be secure; causing the FBI to be forced to find an alternative to successfully access the phone, this being a hacking tool attained from an outside source. Brazil restricted the use of WhatApp for the second time during May of 2016, due to not granting access to the information required by a police investigation. The use of divisions continue to be provoked by further problems regarding the collection of data. As of 2016, the United Kingdom authorised a law concerning the obtainment of communications held from the citizenry of the UK, to be allowed from sweeping powers. However, the European Court of Justice (ECJ) claimed that this activity concerning this gathering of information is against the law. The Supreme Court of the United States held an agreement to judge a case respecting the need of a warrant from investigators to be able to know where an individual is located through the use of gaining access to the records of mobile phones.

Major Parties Involved

United States of America

The Director of National Intelligence issues a report yearly, which has publicised the total number of phone calls being, 151 million, realised by the citizenry in America in 2016; even though the ability to this action had been limited by the Congress just before. However large the amount may seem, the NSA used to have the capability to attain a larger fraction that would help analyse possible attackers through the usage of the system before 2016. The US legislation of the constitution according to the 4th amendment which revolves around the issue of the protection of the rights of their citizenry; ”the right of the people to be secure in their persons, houses…effects, against unreasonable searches and seizures, shall not be violated…”; this means that according to this legislation any individual has the right to regulate the data that is gathered and how it is processed. According to a poll conducted recently, the American citizenry did not reflect positively upon the attainment of personal information and its usage; the same as they did back in 2013. 38% of the results received from the poll considered that the employment of their data collected by organisations and the governments, among other groups, was having a positive effect upon the development of security. On the other hand, an opposing 53% believed that this collection of personal information was a violation to their privacy and security.

North Korea

North Korea's regime pursues to endure the government of the Kim Jong-un as supreme leader of the country by setting a strategy based on the use of the force.

To achieve these long-term goals, Kim Jong-un has been developing the country military capabilities including the development of nuclear missiles, regardless of the poverty and food shortage that many inhabitants are suffering in the country. Doing so, Kim Jong-un intends to gain international prestige by using this military power as a way to gain influence in the region, showing his nuclear power intends to intimidate neighbours and gain a stronger position in future negations.

Since Kim Jong-un´s arrival to the North Korea government in 2011, he has thrown the international community with continuous nuclear threats and power demonstrations, including six nuclear tests, and many interventions on the Korean Peninsula to the frustration of the international community.

China

The government within China, published a document relating to the protection of personal information known as, Standard GB/T 35273-2017, released as of May 1 2018. This document outlays how the collection of data is occurring and being shared, however it contains harsher requirements than the GDPR within the European Union.

European Union

The EU published the General Data Protection Regulation (GDPR) implemented upon 25th of May 2018; replacing the Data Protection Directive taken into force in 1995, which was "designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data". The replacement of this directive occurred in coherence with the modernisation of technology and to assure that current privacy legislations are being applied effectively to this.

Brazil

The President of Brazil, Dilma Rousseff, had a discussion in September 2013 with the United Nations regarding the importance of internet freedom and surveillance:

- "In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy;
- The right to safety and security of citizens in one country can never be guaranteed by violating the fundamental human rights of citizens of another country." *(President Rousseff)*

Brazil has ensured that the actions committed concerning the digital realm are exposed by both journalists and digital activists. Moreover this country, has taken the steps by developing Brazilian Digital Bill of Rights which pertains the principles concerning network neutrality and freedom of self-expression; this enables the citizenry to attain their civil rights online as well as off. However, doubts have arisen as to whether particular parts of this law has the ability to properly protect the rights of the user.

United Kingdom

The UK National Security Council (UK NSC) is the primary governmental body for maintaining the national security, international peace, and overall nationwide defence. Among its primary function is to advise and assist the UK Government on national security and foreign policies. It was formed on May 12, 2010 by Prime Minister David Cameron, and its inception, it has been the main cabinet for coordinating national threats and security responses.The UK National Security Council is supported by the National Intelligence office in order to produce independent assessments for the national security and intelligence issues of strategic importance.

The National Security Council has been quite successful bringing more clarity to decision making for opening up the process of governmental deliberation facilitating the decision making process. The success of the National Security Council has been mainly due to the direct involvement and commitment of the Prime Minister. The prime minister himself has been chairing sessions regularly and participating actively in the discussions, has reinforced the authority and confidence of the NSC.

The UK national security policy is covered by a veil of secrecy, but these good mechanisms and practices have favoured these processes for breaking down departmental barriers to get an active cooperation among governmental organisations to get a new national security doctrine, the Fusion Doctrine, that improve the collective approach to national security to project the national economy and nationwide goals.

Timeline of Key Events

Date	Description of Event
25th May 2018	The GDPR is enforced
May 2018	Standard GB/T 35273-2017 is published by the Chinese government pertaining the protection of personal data
May 2016	WhatsApp is banned for the second time in Brazil
14th April 2016	General Data Protection Regulation (GDPR) is approved
2016	The United Kingdom authorised a legislation concerning the obtainment of communications held from the citizenry of the UK
2015	The NSA is restricted from gathering bulk data
December 2013	Resolution 68/167 is adopted by the UN General Assembly, containing information regarding the effect of activity surveillance upon an individual.
June 2013	Edward Snowden reveals information regarding the NSA and their usage of private data that is published in the Guardian newspaper
May 2011	The European Union Directive is adopted; that allows an enhancement to a user's privacy online, through the use of being able to decline cookies. The laws of each country were updated in order to comply with this Directive.
12th May 2010	UK National Security Council is formed by David Cameron, being the main element for coordinating national threats and security responses

2007	The US prism is founded, having the objective of acquiring information from the most known companies throughout the world, these being Facebook, Apple and Google among others
11th September 2001	The Pentagon and the World trade centre of New York are attacked by Al-Qaeda terrorists.
1998	The Safe Harbour agreement is published
1995	The European Union directive Protection Directive is published respecting the usage of personal data within the EU. This is a key part of the human rights law and privacy within the EU
23rd March 1967	The International Covenant on Civil and Political Rights is comes into force.
10th March 1948	The Universal Declaration of Human Rights is published regarding the rights that any individual is entitled to.
5th march 1946	The Five Eyes is created due to the validation of the UKUSA agreement

UN Involvement, Relevant Resolutions, Treaties and Events

Below is listed the UN involvement, that regards main events and resolutions.

- Universal Declaration of Human Rights (UNHDR), all the document is in relevancy though in specific its articles 12 and 19.

- International Covenant on Civil and Political Rights (ICCPR), certain articles are applicable, these being articles 17 and 19.

- Guidelines for the Regulation of Computerised Personal Data Files, (A/RES/45/95), published in 1990.

- Developments in the field of information and telecommunications in the context of international security, (A/RES/68/243), published in 2013.

- Right to privacy in the digital age (A/HRC/RES/34/7), published in 2017.

- Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, (A/HRC/34/61), published in 2017.

Previous Attempts to Resolve the Issue

Safe Harbour agreement

The Safe harbour agreement was created during the years of 1998 and 2000 for there to be a prevention towards the collection of customer data from organisations from the US or EU. However, the European Court of Justice took the decision of overturning this agreement on the 6th of October 2015; this proposed the companies of the US to adhere with the legislations concerning privacy that protect the citizenry of the EU.

The Data Framework Decision

The Data protection Framework is over the usage of private information in relation to the legality of criminal offences, there is minimal protection of information present necessitated for the collaboration of the states within Europe. Although, the European Data Protection Supervisor (EDPS) has declared that there is an unsatisfactory level of protection within the last text of Framework Decision. Consequently the EDPS has suggested improvements to the processing of data, in order to guarantee the enhancement of protection.

Possible Solutions

As mentioned previously, the most important factor that is to be discussed is the circulation of laws pertaining national security and individual privacy; through the verification that this in relevancy with the use of modern technology; personal data will be more restricted, allowing governments and agencies to not attain this information with facility and further not avoid the current legislation.

Another possible solution would be to ensure that this legislation is being enforced, as there is no control realised over the gathering of data throughout the world; the creation of a body that would allow a restriction to such data would serve as a benefit, as this would allow for the legislations concerning privacy to gain importance. However, it must be ensured that this activity is classified, and thus permitting the general public gaining awareness of it; as this could easily be endanger the national security within any nation.

The renew of the collection of data must taken into consideration; as this collection is adequate to a certain extent, such as for national security, but not to be benefited by organisations whom use this information for commerce. Furthermore, in order for prevent the detainment of data, legislations that deal with the data that does not serve as a useful

purpose should be reestablished, and effectively analysing the intermission of data identification.

Moreover, the European Court of Justice (ECJ) argued that new measures should be attempted, taking into consideration that the Safe Harbour Principles are unable to successfully pertain the transfers of information. The provision of trade treaties EU-US under the legislations, would allow national security and the data protection to be possible. The creation of a Transatlantic Trade and Investment Partnership (TTIP) that is in relevance with the standards of the EU regarding the rights to privacy would be able to set international global agreements and thus successfully generate, in accordance with other nations, safe protection of data.

Bibliography

CHINA AS A NATIONAL SECURITY CONCERN, www.rand.org/content/dam/rand/pubs/monograph_reports/MR1121/mr1121.ch1.pdf.

Perez, Talia Klein. “Does National Security Outweigh the Right to Privacy?” Theperspective.com/, 16 Oct. 2017, www.theperspective.com/debates/living/national-security-outweigh-right-privacy/.

Strohm, Chris. “Privacy Vs. Security.” Bloomberg.com, Bloomberg, 20 May 2015, www.bloomberg.com/quicktake/privacy-vs-security.\

Davis, Lauren Cassani. “When It Comes to Personal Data, How Do Americans Balance Privacy and National Security?” The Atlantic, Atlantic Media Company, 3 Feb. 2016, www.theatlantic.com/technology/archive/2016/02/heartland-monitor-privacy-security/459657/.

Morris, Nigel. “Q&A: What Is Prism, What Does It Do, Is It Legal and What Data Can It.” The Independent, Independent Digital News and Media, 11 June 2013, www.independent.co.uk/news/world/americas/qa-what-is-prism-what-does-it-do-is-it-legal-and-what-data-can-it-obtain-8650239.html.

“标准号：GB/T 35273-2017.” 国家标准|GB/T 35273-2017, www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE.

Pak, Jung H. “Regime Insecurity or Regime Resilience? North Korea's Grand Strategy in the Context of Nuclear and Missile Development.” Brookings, Brookings, 2 Feb. 2018, www.brookings.edu/research/regime-insecurity-or-regime-resilience-north-koreas-grand-strategy-in-the-context-of-nuclear-and-missile-development/.

“OHCHR | Right to Privacy in the Digital Age.” *OHCHR | Convention on the Rights of the Child*, www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

“National Security Reviews 2017: A Global Perspective - United Kingdom.” *White & Case*, 9 Nov. 2017, www.whitecase.com/publications/insight/national-security-reviews-global-perspective-united-kingdom.