Research Report I 30th Annual Session

Special Conference 1 on Shifting Power Dynamics in a Globalised World

Protecting civil privacy while maintaining national security

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Sam de Jong

Forum	Special Conference 1
Issue:	Protecting civil privacy while maintaining national security
Student Officer:	Sam de Jong
Position:	President of SPC1 & SPC2

Introduction:

As defined by the Cambridge dictionary, 'Privacy' is "someone's right to keep their personal matters and relationships secret" and "a state of being alone". Personal matters can be expanded upon by including 'Personal Information'. The first definition given by the dictionary is the one we will be focusing on in our committee during MUNISH 2020. The United Nations Universal Declaration of Human Rights, as well as over 150 national constitutions, mention the right to privacy, such as article 12 of the Universal Declaration of Human Rights, which reads:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks." (United Nations General Assembly, 1948)

Even though a declaration is not actually valid in a court of law, the integration of articles of the declaration into national constitutions make them valid and allow people to retain rights from the documents. Because most people agree upon the values stated in these documents, we can actually validate them within our society. It is everyone's role to inform themselves upon their rights, as it is the only way to defend them. As a member of our global population, every individual is also responsible for the rights of other individuals. The governments hold onto these laws to protect their inhabitants.[1]

The right to privacy is one that conflicts with many of our society's other priorities, for example that of national security. National security includes protection of the land, the people, the economy and the government. Measures that can be taken to improve national security are often seen as privacy invasive. What these measures could include will be elaborated upon in the general overview and further.

[1] (Amnesty Switzerland, 2016)

Definition of Key Terms

Data subject

An identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used (General Data Protection Regulation, Art. 4 Definitions).

Expectation of Privacy

In the United States, the Fourth Amendment protects people from unwarranted searches of places, but also seizures of people or objects, when they stand in relation to one's privacy. During the Katz v. United States, Justice Harlan used a two-part test to prove a violation of their clients 'Expectation of Privacy'. To pass the test, an individual first needs to have exhibited an actual expectation of privacy. Secondly, this expectation needs to be recognized as reasonable by society. If both requirements are met, the Expectation of Privacy has been noted as valid, and violation of this expectation is seen as violation of the Fourth Amendment.[2]

Mass Surveillance

Mass Surveillance is a governmental programme that monitors all (online) activities of individuals, not only within a country but across the entire globe. This systematic interference collects data of all users, not only those who can be spied upon based on valid grounds.[3]

Netizen

A citizen of the internet.[3] Someone who actively makes use of information and convenience provided by the world wide web.

National Security

Regarded as a responsibility of a nation's government, national security is the protection of a country's inhabitants, institutions, land, economy. Possibly, the protection of a country includes military action, as well as other tools governors have to guarantee safety. "A country's national security is its ability to protect itself from the threat of violence or attack" (Collins Dictionary)

Privacy

Someone's right to keep their personal matters, relationships and personal information secret. (Cambridge Dictionary)

---

[2] (Cornell Law School)

[3] (Muqeet, 2018)

1. Independence in making certain kinds of important decisions
2. The individual interest in avoiding disclosure of personal matters

(Whalen v. Roe, 433 U.S. 425. 1977)

General Overview

In order to set frameworks that protect privacy of citizens worldwide, countries have since the early 1970s started to adopt comprehensive privacy laws. These are made to ensure that every nation has similar laws upon the right to privacy. Through the United Nations, opportunities arise to make an even more general framework for all countries to conform to. However, in the world right now, many law enforcement and intelligence agencies have been given access to data, nonetheless. Over 90 countries worldwide engage in illegal monitoring, even collecting data from citizens that were not accused or suspected of being involved in criminality. [4]

Privacy

Our main priority within this topic is to protect the privacy of civilians. Even when governments are required to take action in order to protect their country, the right to privacy needs to be respected. Now our question is to define the length of matters that this privacy is in relation to. Many might agree that personal information like address, phone number or social security number should not be public information. On the other hand, many people seem to have no issue in sharing some of this 'private' information in surveys, phone calls and even on social media pages like Facebook and Instagram.

Privacy over the years[5]

With the development of industries, the internet and globalization, the perspective on privacy has constantly been evolving and changing. Where it was once easy to decide who did and who did not get to know about you, it has become more and more difficult to contain this spread of information. The web allows anyone to find anything they want, about celebrities, but also about 'regular people'. At the beginning of the privacy debates, people were concerned about their bodies and homes, whether the British could or could not invade houses on unjust grounds. During the Twentieth Century, as telephones started to develop, wiretapping became a subject of debate. The Growth of Government Record Systems, including the 1935 Social Security System, gave a boost to the administration by governments of peoples' identities. The US Congress enacted the Federal Communications Act of 1934, in which section 605 provided: "*no person not being authorized by the sender*

[4] (Banisar and Davies, nd)

[5] (Solove, 2006) and Appendix III

shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person". This section in principle illegalised wiretapping in any way. During the Second World War, the American Federal Bureau of Investigation (FBI) got increasing permission to engage in wiretapping, in order to protect the national security of the USA.[6] The 1967 *Katz v. United States* gave rise to the 'Expectation of Privacy', which is further elaborated upon in the 'Key Terms' section. Soon came the rise of the computer. In 1974 the US Congress passed the Privacy Act of 1974, which limited the use of the Social Security Number by federal and local agencies to protect information and confidentiality. More Protection Acts arose, please refer to Appendix III. However, a big twist in the debate on privacy came on 11 September 2001, when the USA, and by that the entire world, got faced with the dangers of extreme terrorists. Quickly arose a new wave of privacy laws, upon which we will elaborate more in the 'Timeline of Events'-section, as well as 'Relevant Treaties'.

What data do governments need?

The processing of certain information about citizens can help governments to take down criminal activity. A very easy way to do this is for example by registering DNA and fingerprints of all citizens in large databases. Given the fact that fingerprints and DNA can often be found at crime scenes, having a register of these makes it easier to find the culprit. Often however, crime does not limit itself to one country. Therefore, another question that arises is the sharing of information over the border. In this case, national security could become a pressing issue. With threats of international terrorism, governmental issues and conflicts that go across the borders, sharing information can be as much of a support as a threat. Information that is related to these threats can go as detailed as specific conversations and interactions between people, as well as their internet searches and social media activity. In the ideal situation for national security, the governments can always know who is where with whom and what they are doing. Every conversation can be overheard, every written message can be read, everyone can be watched. Now we should ask ourselves in what range we can 'invade' an individual's privacy in order to keep them safe, without making people feel uncomfortable or unsafe.

Relation to national security

The information acquired through the web behaviour of consumers allow governments to have an insight on their general intentions and way of living. Potentially, this information can lead to discoveries that can protect the entire country

[6] (Whitfield and Landau, 1998)

by preventing certain things from happening. These things could include, (terrorist) attacks, leakage of classified information or international criminality. In theory, all these acts that could harm national security, are organised by multiple people. That means that to make something like that happen, people need to communicate about it. From that we can conclude that by verifying all interactions between all people, all these acts against national security can be foreseen and therefore prevented or taken measures against.

National Security

Every country has the individual responsibility to keep their citizens and economy safe. Many external, as well as internal effects can however make it harder for countries to fulfil that purpose. Externally, other countries threaten a nation's security by invading the country, politically influencing domestics or threatening with violence. Within the country citizens with mal intentions threaten security, as well as for example corruptive governors or loopholes in national laws.

Threats to national security[7]

There are numbers of threats to the national security of each country. Even though every country has their own issues, there are some common threats that most countries need to combat against. One of the main issues that became highly pressing in 2001 is the threat of terrorism. Starting in the USA, the entire world quickly engaged in the War against Terrorism. Until this day, terrorism remains of the biggest threats to the safety of citizens worldwide. Another common threat is that of espionage. It is usual for governments to rely on international information to base their decisions upon. However, espionage is a way to obtain information that is not usually public knowledge. Human resources, as well as technical means can be used to discover information about policy, financial state, defence, technological advances and industrial/commercial interest. This could harm military abilities or advantages of nations, it allows countries to destroy foreign economies, or could lead to theft and copying of classified documents or technologies. Lastly, so-called 'hostile actors' can, from within a country, access the country's Cyberspace and launch network attacks. These attacks can be related to terrorism, crime or espionage. Often, a combination of resources is used by attackers. This makes the protection of national security a complicated job.

Conflict

[7] (CPNI)

In modern day and age, with the development of high-level technology and the endless possibilities of the internet, combined with pressing threats to national securities, the limits of the citizens precious privacy are put under pressure. As it is the government's goal to make their citizens feel safe, it is a balancing game to see who the biggest enemy is. On the one hand, governments monitoring their citizens without a just ground makes inhabitants feel watched, unsafe and untrusted. Whilst on the other hand, not knowing whom in the neighbourhood might be planning a terrorist attack makes everyone fear for their lives.

Major Parties Involved

European Union

The EU law for data processing is known as the General Data Protection Regulation (GDPR), which is a federal-level data protection outline. The law protects data from consumer processes by companies. Even though it does not directly point to the processing of data by governments, it does give an insight on the European standards of privacy. This data includes for example information about the consumers buying habits, home- address and email, but also their account information. By registering passwords that consumers use to make an account for a certain companies' web shop, it might also become easier for (legal) hackers to get into the consumer's other accounts. The GDPR effectively says that companies shall limit the information they process about their data subjects: the data is adequate, relevant and not excessive. Another point is that the processor of the data is ultimately responsible for the safety of the information during processing. Lastly, the amount of time in which the date remains saved is set out in the GDPR.[8]

United States of America

Even though the popular American police shows like NCIS, Criminal Minds, Hawaii Five-0 and CSI might not give the most realistic view of federal investigations in the USA, they do give a sight of the tip of the iceberg. In the shows, an elite group of detectives solves massive criminal cases in a matter of days or even hours. A big source of information is the database that the shows have including every inhabitant of the country. They need the smallest bit of DNA, a fingerprint or a pixelated picture and within minutes they can identify and locate whoever they need. It seems great, as these high-profile criminals can be caught extremely fast, making life in America safer every day. On the contrary, knowing that any inhabitant can be found, might not be the safest feeling. In reality however, the USA implements so called Mass Surveillance, which collects data from nearly all of the nation's internet activity. According to governors, it is not an invasion of privacy, as the information will

[8] (Green, 2020)

not be viewed nor analysed without just grounds. Surveillance tools used by federal and local agencies, however, have the ability to localize phones and computers in specific areas without a problem. The collection of all this data might lead to unfair suppositions or flawed correlation. Authorities not only in the US can access citizens' banking and phones and might even affect their freedom of expression, for example their expression of political preference.[9]

Timeline of Key Events and Relevant treaties and UN resolutions

Date	Event	Explanation
1948	Universal Declaration of Human Rights	*"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."* Article 12, UN General Assembly, UDHM
16 Dec 1966	International Covenant on Civil and Political Rights	*"…provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. It further states that "Everyone has the right to the protection of the law against such interference or attacks."*
1967	Katz v. United States	The expectation of privacy is accepted as well as the requirement of a warrant before intercepting communications.
11 Sep 2001	9/11	Terrorist Attack New York, killing a total of 2977 citizens of the USA. From that point on George W. Bush announced the War on Terrorism, referring to the NAVO-pact for support.
2001	USA PATRIOT Act	"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism"-Act. 18 U.S.C. § 3127(3) as amended by the USA PATRIOT Act § 216.
2002	Homeland Security Act	Introducing in the USA a Department of Homeland Security, including 22 federal agencies and a privacy office. 6 U.S.C. § 222

[9] (Muqeet, 2018)

2002	Directive 2002/58/EC	Collecting, accessing and deleting of personal data within the electronic communication sector specified by law
2004	Intelligence Reform and Terrorism Prevention Act of 2004	Which aimed to improve the sharing of information between federal agencies, in order to develop a culture of free information sharing.
2006	Data Retention Directive (Directive 2006/524/EC)	Telephone and internet companies are required to trace the source and location of communications in order to track down serious crimes.
2013	NSA Surveillance revealed	NSA surveillance is revealed by Edward Snowden, a previous CSI detective. NSA uses technologies to track calls, messages, emails and social media of millions of Americans.
Dec 2013	UNGA Resolution RES/68/167	General Assembly expresses concerns about the privacy of citizens with the evolution of the digital age. Notices negative impact of mass surveillance and interception and calls upon States to review their practises upon privacy laws. States are required to fulfil their obligations to the Universal Declaration of Human Rights.
2014	GDPR and Right to be Forgotten	General Data Protection Regulation of the European Union (EU 2016/679) gives a legalisation to the common-sense privacy laws. The Right to be Forgotten allows a data subject to have their information removed without undue delay (which is about a month).
Mar 2014	UNGA decision 25/117	Protecting privacy in context of domestic surveillance as well as extraterritorial, mass scale collection of personal data and interception of digital communications.
May 2018	Updated GDPR	Requires people to give permission for their data to be processed.

Possible Solutions

Now the question is of course what MUNISH Special Conference 1 is going to do to resolve the issue of protecting civil privacy while maintaining national security. In the past we have seen many countries make attempts at managing privacy within their borders. However, with the evolvement of terrorism and cyber-attacks, governments had to set priorities. With

the time that we have to prepare for the conference though, we can sit down and think of what will actually work in the long run.

Firstly, I think it important for you to think about the perspective of the inhabitants of your country. What are their general beliefs on privacy? How do they live? Does your government have faith in their inhabitants? For many religions and lifestyles, transparency is not that much of an issue. As this issue is very much about what the people will accept in matters of their privacy being invaded, you can use your own perspective and that of your friends. We know that it might be easier to compromise on the negative side of privacy than on that of national security.

Secondly, take a look at how willing countries are to share information. One country's effort and knowledge can help another country to protect themselves. However, sharing classified information with foreigners might put your own country in a dangerous position.

A third thing to consider is to eliminate the threats. We have seen these threats in the general overview: terrorism, espionage and cyber-attacks. Terrorism might only be preventable by invading the people's privacy, but espionage and cyber-attacks can very well be countered with solid online protection. Consider whether investing in that could be worth it.

Altogether, it is important to find a balance between these two important measures. As long as people understand why something is necessary and important, they often do not mind going along with it.

Bibliography

ACLU. "NSA Surveillance", *American Civil Liberties Union*, https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance. Accessed 28 June 2020.

Amnesty Switzerland. "Human rights in two minutes", 21 Dec 2016, https://www.youtube.com/watch?v=ew993Wdc0zo. Accessed 14 June 2020.

AVG Now. "History of Digital Privacy", https://now.avg.com/history-digital-privacy. Accessed 28 June 2020.

Banisar, David and Simon Davies. "Privacy and Human Rights: An International Survey of Privacy Laws and Practise", http://gilc.org/privacy/survey/intro.html. Accessed 28 June 2020.

Cambridge Dictionary. "Definition of Privacy", *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/. Accessed 14 June 2020.

CPNI. "National Security Threats", *Centre for the Protection of National Infrastructure*, https://www.cpni.gov.uk/national-security-threats. Accessed 28 June 2020.

Collins Dictionary. "Definition of National Security", Collins Dictionary, https://www.collinsdictionary.com/dictionary/english/national-security. Accessed 14 June 2020.

"Expectation of Privacy", *Cornell Law School*, https://www.law.cornell.edu/wex/expectation_of_privacy. Accessed 14 June 2020.

"Everything you need to know about the Right to be Forgotten", *GDPR.EU*, https://gdpr.eu/right-to-be-forgotten/. Accessed 28 June 2020

Green, Andy. "Complete guide to privacy laws in the US", *Veronis*, 29 March 2020, https://www.varonis.com/blog/us-privacy-laws/. Accessed 28 June 2020.

Green, Andy. "What is the EU General Data Protection Regulation?", *Veronis*, 29 March 2020, https://www.varonis.com/blog/what-is-the-eu-general-data-protection-regulation/. Accessed 28 June 2020.

Intersoft Consulting. "General Data Protection Regulation", Article 4, https://gdpr-info.eu/art-4-gdpr/. Accessed 28 June 2020.

Muqeet, Bilal. "Mass Surveillance Program Around the World", *Privacy End*, 23 February 2018, https://www.privacyend.com/mass-surveillance/. Accessed 28 June 2020

Solove, Daniel J. "A Brief History of Information Privacy Law", *GW Law Faculty Publications & Other Works*, 2006.

"The Right to Privacy in the Digital Age", *UNHCR Office of the High Commissioner*, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx. Accessed 28 June 2020.

United Nations General Assembly. "Universal Declaration of Human Rights". https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf. Accessed 14 June 2020.

Whitfield, Diffie & Susan Landau. "Privacy on the Line: The Politics of Wiretapping and Encryption", p. 161-62, 1998.

Appendix or Appendices

I. This page gives an overview of the national laws of all nations within the United Nations, which is now set to find articles on privacy. It can be used to find, pin, compare and save articles: https://www.constituteproject.org/search?lang=en&key=privacy

II. The full report on the survey research upon international practice of privacy laws and the threats of privacy can be found here: http://gilc.org/privacy/survey/intro.html

III. For the download version of the "Brief History of Information Privacy Laws": https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications

IV. Mass surveillance programs around the world: https://www.privacyend.com/mass-surveillance/