Special Conference Plenary (SPC1 & SPC2)

Protecting civil privacy while maintaining national security

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Jules Mateo-Nerlich

Forum	Special Conference Plenary (SPC1 & SPC2)
Issue:	Protecting civil privacy while maintaining national security
Student Officer:	Jules Mateo-Nerlich
Position:	Deputy President

Introduction

It is in human nature to want to keep things to ourselves. In the year 1890, an article was published which mentioned the first ideas about the right to privacy with innovations such as newspapers and photographs which had slowly started to invade public life. This right was before this article only ever known as the 'right to be let alone.' This right was implemented and thought about as technological advances were being made around the world, including the spread of newspapers and cameras which in an unprecedented manner displayed the quiet private lives of people to the entire world (Litt).

In 2021, 65% of the world population is active online on the internet (Lin). Our private information is all to be found online and accessible to anyone that has the capabilities to accessing this information. The right to national security is a crucial one and now more than ever criminal activities (such as hacking, conspiring crimes and recruitment to terrorist organizations) are being done online. To access to chat dialogues, search history, IP addresses, online purchases and downloads or whatever other means needed to track a criminal, a breach of the right to privacy is being committed. This also may happen to innocent civilians whose privacy is being breached without them knowing.

Any government knows certain information about most of their citizens no matter how hard they actively try to keep their life online private. These include their full name, age and date of birth, place of birth, social security number, place of residence and duration of residence (if they have moved from one place to another) and marital status. With this information alone a government can't tell if a person is a potential threat to their country. This is why intelligence agencies gather data left by an individual's digital footprint on the internet to assess potential threats. It is known that major tech companies (such as Microsoft, Apple, Google and Facebook) have assisted the American National Security Agency in their efforts to spy on individuals to search for incriminating evidence and/or potential threats (Dennis). Sometimes these efforts lead to positive outcomes, due to potential threats being singled out, culprits being found and avoiding future crimes however, sometimes this is not the case and

innocent people's privacy is being breached without them knowing. This is why the lingering question still hangs: Which is more important, civil privacy or national security and is it more important to jeopardize civil privacy if that means a greater chance of increasing national security? As it stands, it is near impossible to reach one without breaching the other.

Definition of Key Terms

Civil Rights

Civil rights are seen as basic rights to prevent discrimination in any given circumstance. For example, the right to a promotion in a workplace is not a civil right. What is a civil right is that if a woman is applying for a promotion that she will not be discriminated because of her being a woman. Other civil rights (include the right to vote, the freedom to religion and the right to privacy.

Civil Privacy

Article 12 of the Universal Declaration of Human Rights states that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations). On top of this, 130 countries across the world have statements written in their constitution regarding the right to privacy. Privacy is in which an individual is not being watched or disturbed by other people. A breach of privacy (when such breach is unwanted) is directly violating a basic human right.

Digital Footprint

A digital footprint is the trail left behind online of someone's internet activities. There are two types of digital footprints. First of all, an active digital footprint is one where someone chooses to leave this footprint behind. They do this by publishing things about themselves online by means of for example social media and/or websites. Then, there is a passive digital footprint. This is the digital footprint someone leaves behind without knowing or thinking about it. This is done when information is collected about someone online when using the internet. Commonly, digital footprints are known as cookies, where most websites will ask you for consent to be able to record your data. This data can technically be accessed by anyone and if often used for background checks by employers and also by law enforcement and intelligence agencies.

National Security

According to the UN, national security is “the ability of a state to cater for the protection and defense of its citizenry” (Osisanya). Nations use many different methods to achieve national security. Some of these include diplomacy (persuasion), military strength and presence, intelligence and governmental agencies and law enforcement (Holmes).

National Security Threat

A national security threat is anything that potentially could cause damage to a nation’s security. It is anything that causes harm to the civilians, economy and/or institutions within that nation. There are many different types of national security threats, these include terrorism, cybercrime, foreign hostile governments, diseases, natural disasters, and the proliferation of weapons in hostile states (“5 Threats to National Security and How Government Protects Its Citizens”).

Terrorism

Terrorism is a threat or an action which poses risk to a government or to the public and is used to intimidate and influence them. Terrorists always have a motive which could be political, religious, racial or ideological, this makes them different to other crimes. To be a terrorist, one does not have to commit the attack, assisting or planning a terrorist attack are both also crimes which are prosecuted under the term ‘terrorism.’

General Overview

The D ilemma

States are faced with a major dilemma when dealing with this issue. Either they protect civil privacy at all costs, with a fear of a breach in national security. Or they do the opposite, minimizing the risk of threats on their nation whilst jeopardizing civil privacy, thus violating human rights. However, this is not as simple as it seems, as the right to security is also a human right. Article 3 of the UDHR states that “everyone has the right to life, liberty and the security of person” (United Nations).

Why Privacy Matters

We hear about mass surveillance a lot when it comes to privacy. ‘Someone is always watching you,’ is a statement that many people have heard before. But although that may sound chilling, a lot of people have the mindset that it isn’t that bad. That if they are not criminals and don’t have any criminal activity to hide then it doesn’t matter. That if they use the internet to watch videos, for work/school or social media rather than plotting major terrorist attacks or other criminal activities for that matter. They decide to believe that since they aren’t

doing anything the government isn't watching them and if they are then it doesn't matter. They say that privacy doesn't matter. Then at the same time, they have passwords to all their accounts (social media, email etc.) often having two factor authentication as well. They have locks on their house doors, bathroom doors. All of this with the purpose to keep what they deem private, private. The attitude that people have when regarding online privacy in regards to in real life privacy is very different. If you are in public you don't act the same whilst as home, because you know that people are watching. Online however, people act very different and go about as if no one is watching them or collecting their data. This is why privacy is so important. It allows us to be who we want to be, to think what we want to think and to do what we want to do without anyone judging us. Part of privacy is deciding who you share what information with. For that reason, people have passwords and may tell their best friend or partner something that they don't feel comfortable with sharing to the entire world, even though often not criminal (Greenwald).

One thing that separates privacy from other rights is that when the right of someone's privacy is breached, they can be blissfully unaware. This is not the case with any other basic human right. For example, for article 5 of the UDHR, which states "No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment" (United Nations), a person will definitely know if that right is being violated. The way that technology is advancing, with more and more people living their lives online, it's becoming easier and easier for governments and companies to spy on everyone. This could lead to a dangerous situation in unstable democracies in which anyone deemed to have 'weird' behavior online could easily be secluded from society.

Why National Security Matters

Essentially, the main goal of any government is to protect their citizens and uphold national security. This is done by ensuring that the safety, security and justice of all citizens of a nation is upheld by ensuring good policing, military and judicial system. National security does not always relate to military threats to a nation. Corruption, fraud, illegal immigration, diseases, running out of resources such as oil and climate change are all threats to a country's national security ("Importance of National Security").

There are many different ways to uphold national security as national security is not just one simple thing. To start off, to maintain political security (the protection of the sovereignty of the government) measures are put in place to protect the government from both internal (i.e corruption) and external (i.e terrorism, espionage, proliferation) threats. Next to uphold economic security (to make sure a nation's economy is thriving and not allowing any

government or people to have full control on a nation's economy), measures are put in place to tackle economic espionage (the unlawful acquisition on secret/important information regarding a nation's economy). Also, as mentioned previously, to hold a good economy, the hands of a country's economy should not be given to one person (for example, the president of a country) as that can be very dangerous for their economy.

To summarize, national security is the main focus of any government as it ensures a thriving society and pushes the country in the right direction. The safety of their citizens, economy and government all lie at the heart of most government's intentions.

Examples of breaches of privacy for a supposed benefit of national security – were all of them worth it?

Airport Security

Breaches of privacy for national security do not only happen online. Airport security is a very good example of a major breach in civil privacy to benefit national security. Since September 11th 2001, the United States (and most other countries) has implemented strict airport security within their airports to prevent the smuggling of weapons onto planes. In 2016, American homeland security conducted a study with 70 officials smuggling weapons (of which some were bombs) through airport security. The results were extremely shocking as it was deemed that 95% of the officials had successfully smuggled weapons which could have led to disasters through airport security (Matthews). Since then, American officials have claimed that they have implemented better and stricter rules in their airport security and have upgraded equipment. Even then, these results combined with the major breach in privacy were very shocking for a lot of Americans.

Covid-19 Tracing Apps

The Covid-19 pandemic brought a lot of panic to the world and required innovative ways to slow down the virus and minimize the risk of infection whilst not completely crippling the economy. Some of these methods saw countries around the world implementing mandatory lockdowns, travel restrictions, curfews, shutting down entertainment (concerts, theatres etc.), closing nightclubs and restaurants, closing schools and urging people to work from home. Also, pretty much all over the world wearing a mask when entering a public place became the norm. Countries also implemented ways to minimize the spread of the virus through contact tracing. This was done at first by a positively tested person letting everyone know that had been in contact with them, so that their contacts would also be placed in quarantine to minimize the risk of infecting more people (a measure of upholding national

security). Certain governments (including China, Israel and South Korea) have started enforcing citizens to download a tracking and tracing apps which would alert them if they had been in contact with someone that was positive and then lead the person to go into mandatory quarantine. In essence this is a good measure to prevent the spread of a virus however, it is a major breach in privacy. With these apps, the government can see where you go, who you meet and at what time this all takes place. Countries in the EU can't use such tracking apps as they violate the GDPR but still have resulted in using apps that work via Bluetooth. These are supposedly private safe as they don't reveal your location, just the people you were in contact with. A lot of people still don't know whether these tracing apps are useful, especially since they can't be mandatory in the EU, and whether the breach of privacy is worth it. Concerning these apps, time will tell.

Major Parties Involved

European Union

The European Union has made great steps towards strict privacy and security laws by enforcing the General Data Protection Regulation (GDPR). The GDPR is the toughest set up regulations regarding privacy in the world. It concerns all EU citizens as well as companies collecting data from EU citizens. Any breaches of the GDPR can result in heavy fines leading up to tens of millions of dollars. The GDPR was put into effect on May 25th 2018 (Wolford).

Germany

Germany is seen as one of the strictest countries in the world regarding data protection laws. In 2009, Germany passed a law which saw it illegal to store telephone calls and data gathered on the internet in large amounts (Mutalip Laidey).

Spain

Alongside with Germany, Spain is another country that is regarded as one of the strictest in the world regarding data protection. Spain is the country in the EU that has fined the most people due to violations of their data protection protocols (Mutalip Laidey).

France

Following the Charlie Hebdo terrorist attack in France on January 7th 2015, France's prime minister at the time Manuel Valls, implemented new counter terrorism measures as a response to this attack. These measures included cyber patrols. These measures saw 3000 people get employed to keep tabs and basically spy on people who were deemed a threat.

These regulations sparked a lot of controversy. On one side, the country was shook following the terrorist attack and people claimed anything should be done in order to help prevent another in the future. On the other hand, this mass surveillance frightened a lot of people due to the major breach in privacy.

United States of America

The United States of America came under fire in 2013 when classified documents of their National Security Agency (NSA) were leaked by former employee and whistleblower Edward Snowden. These documents showed that the USA had implemented mass surveillance programs on their citizens, both from telephone records and internet usage.

Timeline of Key Events

Date	Description of event
December 15th, 1890	"The Right to Privacy," by Warren and Brandeis was published, the first official instance of this right being mentioned.
January 1st, 1983	The internet was invented, allowing computers to have a way to communicate with each other. There wasn't a standard program which all computers ran, meaning that computers could only communicate with ones running the same program as them.
April 30th, 1993	The World Wide Web (WWW) was made available to the public. It allowed all computers to communicate with each other. This made sharing and accessing information online easy and possible.
June, 2013	Edward Snowden Leaked thousands of documents from the American National Security Agency (NSA). These documents revealed that the NSA was recording the phone records of tens of millions of Americans as well as tracking online communications and online usage.
May 25th, 2018	The General Data Protection Regulation (GDPR) was put into place after having been introduced two years prior. This is the strictest set of regulations concerning data protection ever created. It concerns all countries within the European Union as well as all companies that collect data from EU citizens.

Possible Solutions

One possible solution to this issue could be to create a system in which law enforcement have regulations in place that do not allow them to breach someone's privacy online without letting them know and without a good reason. This could be in the form of a warrant, which police use to access houses or property of suspects (which also is a breach of privacy). Having such regulations will minimize the breach of privacy of innocent civilians whilst also being transparent and letting people know that their online activity is being watched and for what reason.

Also, another solution is to implement a regulation across all countries that is similar to the GDPR which is in place in the European Union. Having such regulation will allow for strict rules on privacy whilst upholding National Security (as has been proven in the EU).

Bibliography

Works Cited

"5 Threats to National Security and How Government Protects Its Citizens." *EKU Online*, 19 Aug. 2020, safetymanagement.eku.edu/blog/threats-to-national-security/. Accessed 10 Aug. 2021.

"A Brief History of the Internet." *Usg.edu*, 2019, www.usg.edu/galileo/skills/unit07/internet07_02.phtml. Accessed 8 Aug. 2021.

"Charlie Hebdo Attack: Three Days of Terror." *BBC News*, 14 Jan. 2015, www.bbc.com/news/world-europe-30708237. Accessed 12 Aug. 2021.

"Civil Rights vs. Civil Liberties." *Findlaw*, 20 Jan. 2021, www.findlaw.com/civilrights/civil-rights-overview/civil-rights-vs-civil-liberties.html.

Dennis. "Citizen Surveillance: What Does the US Government Know about You?" *Privacy.net*, 18 Sept. 2018, privacy.net/us-government-surveillance-spying-data-collection/. Accessed 9 Aug. 2021.

"Digital Footprints." *Family Lives*, Totally Communications, 2019, www.familylives.org.uk/advice/your-family/online-safety/digital-footprints/. Accessed 9 Aug. 2021.

"France Security Law Incompatible with Human Rights, Say UN Experts." *The Guardian*, 4 Dec. 2020, www.theguardian.com/world/2020/dec/04/france-security-law-incompatible-human-rights-un-experts. Accessed 12 Aug. 2021.

Greenwald, Glenn. "Why Privacy Matters." *Ted*, TED Talks, 2014, www.ted.com/talks/glenn_greenwald_why_privacy_matters?language=en. Accessed 10 Aug. 2021.

Holmes, Kim. "What Is National Security?" *The Heritage Foundation*, 7 Oct. 2014, www.heritage.org/military-strength-topical-essays/2015-essays/what-national-security. Accessed 12 Aug. 2021.

"Importance of National Security." *IPL*, www.ipl.org/essay/Importance-Of-National-Security-F3CSZRHEACFR. Accessed 12 Aug. 2021.

Lin, Ying. "10 Internet Statistics Every Marketer Should Know in 2020 [Infographic]." *Oberlo*, 8 Nov. 2019, www.oberlo.com/blog/internet-statistics#:~:text=Summary%3A%20Internet%20Statistics. Accessed 8 Aug. 2021.

Litt, Robert S. "Privacy, Technology & National Security." *Intelligence.gov*, 2011, www.intelligence.gov/index.php/ic-on-the-record-database/results/45-privacy. Accessed 3 Aug. 2021.

Matthews, Dylan. "The TSA Is a Waste of Money That Doesn't Save Lives and Might Actually Cost Them." *Vox*, 17 May 2016, www.vox.com/2016/5/17/11687014/tsa-against-airport-security. Accessed 9 Aug. 2021.

McPartland, Ben. "Liberty or Security: Or Can France Have Both?" *The Local*, 22 Jan. 2015, www.thelocal.fr/20150122/france-terrorism-surveillance-security-privacy-cnil/. Accessed 12 Aug. 2021.

Mutalip Laidey, Noorenda. "Privacy vs. National Security: Where Do We Draw the Line?" *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, vol. 9, no. 6, Dec. 2015. *ResearchGate*.

"National Security Threat List." *Www.wrc.noaa.gov*, 28 Nov. 2001, www.wrc.noaa.gov/wrso/security_guide/nstl.htm. Accessed 12 Aug. 2021.

Oberheiden, Nick. "Defending against National Security Threats." *The National Law Review*, 16 Feb. 2021, www.natlawreview.com/article/defending-against-national-security-threats. Accessed 12 Aug. 2021.

"On This Day: World Wide Web (WWW) Became Public Domain." *News18*, 22 May 2021, www.news18.com/news/lifestyle/on-this-day-world-wide-web-www-became-public-domain-3690710.html. Accessed 8 Aug. 2021.

Osisanya, Segun. "National Security versus Global Security." *United Nations*, www.un.org/en/chronicle/article/national-security-versus-global-security.

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/. Accessed 12 Aug. 2021.

Simmons, Dan. "13 Countries with GDPR-like Data Privacy Laws." *Insights.comforte.com*, 12 Jan. 2021, insights.comforte.com/13-countries-with-gdpr-like-data-privacy-laws. Accessed 12 Aug. 2021.

"Terrorism." *Www.cps.gov.uk*, 2020, www.cps.gov.uk/crime-info/terrorism. Accessed 11 Aug. 2021.

United Nations. *Universal Declaration of Human Rights*. , 10 Dec. 1948.

"What Is Privacy?" *Privacy International*, 23 Oct. 2017, privacyinternational.org/explainer/56/what-privacy. Accessed 10 Aug. 2021.

Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" *GDPR.eu*, 7 Nov. 2018, gdpr.eu/what-is-gdpr/. Accessed 10 Aug. 2021.