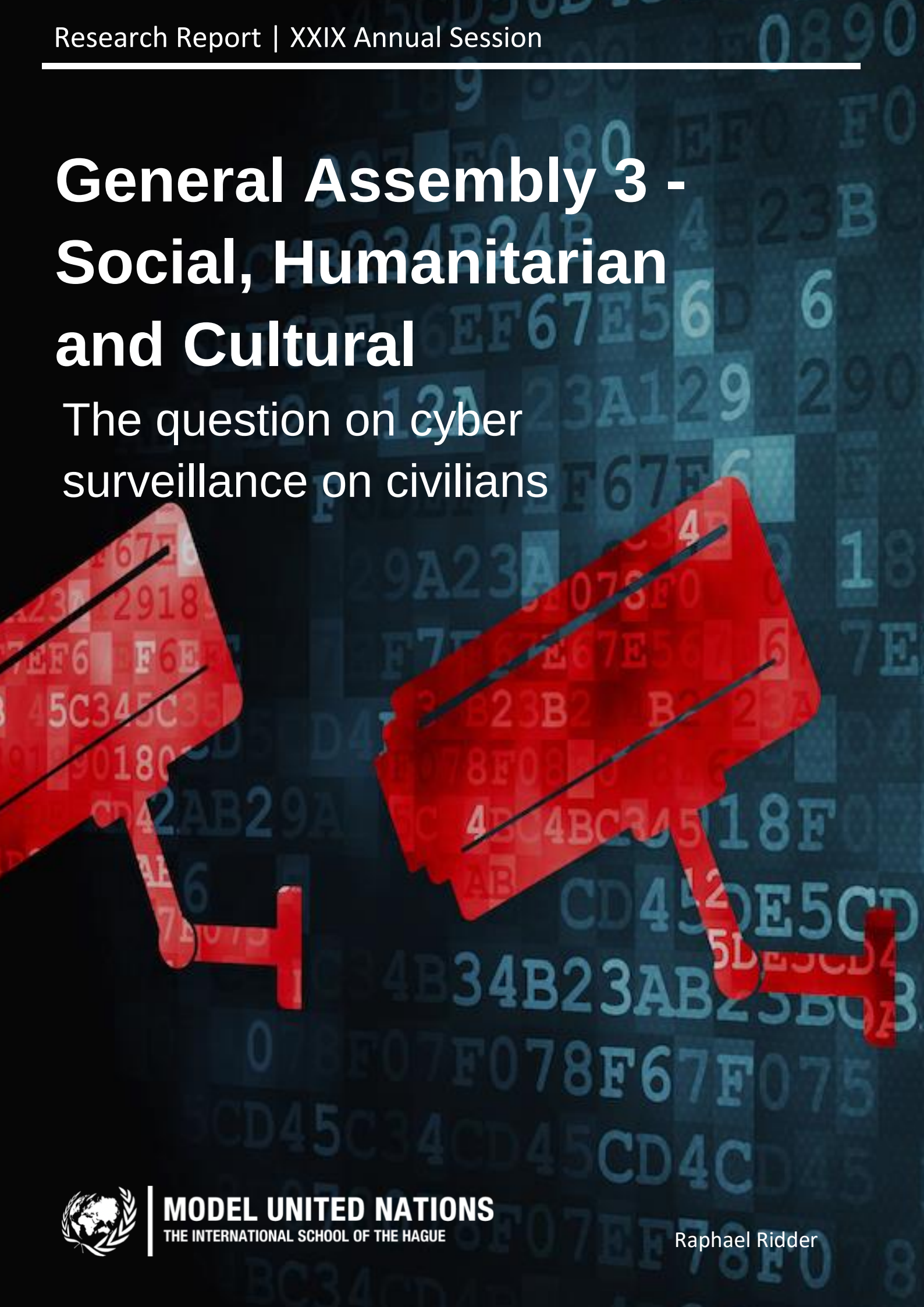
General Assembly 3 - Social, Humanitarian and Cultural

The question on cyber surveillance on civilians



MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Raphael Ridder

Forum	General Assembly Third Committee
Issue:	The question of cyber surveillance on civilians
Student Officer:	Raphael Ridder
Position:	Chair

Introduction

The Internet, a place where we trade our privacy for services. Ever since the World Wide Web was created in 1991, there has been no binding law that was enforced on the Internet, partly because there really is no way to indicate a jurisdiction, making enforcing the law difficult. Now the internet seems a giant no-man's land without clear laws, partly because it is a fairly new forum not considered in all the basic laws that we daily enjoy. It is a place where borders cannot be established, upholding laws seems impossible and the possibilities seem endless. Corporations or governments could use the Internet to store all consumer's data, look through one's devices and restore things one might have thrown out, use the cameras on one's devices to look through and know the location of one's devices at any given moment.

In the digital era, people live their lives online, however not everyone is aware that everything one does online is monitored and stored. Big corporations will track online footprints from the moment their site is used for the first time. Hence, the consumers privacy is worth more to big corporations or governments than it is to oneself. On the web the users are not the costumers they are the product; big corporations create vast capital with their personal information.

By using these devices and online services daily we open ourselves up to mass surveillance and the inability of having privacy. However nowadays it seems impossible to live without these devices as a lot of us use theme for our work or school and without them we wouldn't be able to keep up. Hence, the Internet should have clear regulations that ensure that no party is violating privacy and so create a safe and private place for all people to use.

This further poses the questions of in what capacity governments are allowed to use the Internet as a means to protect, surveill, or censure their civilians. All nations have a secret service for cyber security, only the actions of said services are in no shape or form monitored or corrected. These services filter through the data of every single civilian; if the data is flagged, they might even visit said civilian to question them about their online actions.

Per example a chemistry teacher in The Netherlands had searched on how to make a certain type of bomb, as result the next morning two agents of the 'Algemene Inlichtingen- en Veligheidsdienst' (AIVD), the Dutch secret service, paid him a visit thinking he had terroristic intentions. This shows perfectly what an extreme impact the Internet has had on the way security and safety in nations is kept, however it also confronts us with the question how far can the government go to protect the safety of its civilians, are governments allowed to absolutely infringe their civilians safety to ensure safety, are these measures ethical or not. These are important questions that are brought up by such examples.

Definition of Key Terms

Censorship

Censorship is a practice in which the suppression or prohibition of any parts of books, films, websites, etc that are considered obscene, politically unacceptable, a threat to security, or inconvenient. There are many cases in which censorship is ethical or even encouraged, frequently when there is a threat to national security. However, sometimes it is used by a ruling party in order to stay in power or enhance their grip upon their civilians. This kind of censorship is used when certain information or even access to certain for a are deemed 'inconvenient' to the ruling party.

Deep Packet Inspection Technology

Deep packet inspection (DPI) is a form of computer network packet filtering that examines the data part and possibly also the header of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether or not to let it pass or flag it.

Digital Age

The 'digital age' or 'information age' is defined as the era of technological

development starting in the 1970's, heralded by the introduction of the personal computer. It signalled the rise of the ability to transfer information freely and quickly and is relevant to the topic at hand due to the era in which the Internet and social media has progressed in the last 50 years.

Internet Privacy

The privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences. Internet privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website under development. Risks may include phishing, pharming, spyware and malware. It corresponds with article 12 of the Universal Declaration on Human Rights (UDHR): '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'; however, it is still unclear if this will apply to the internet.

IP address

An IP Address or "identity protocol" address identifies one through one's computer on a local network. IP addresses are the way to identify users and their actions in the cyber sphere, which can lead to infringing on rights to privacy by corporations and national intervention.

Mass surveillance

Mass surveillance is the intricate surveillance of an entire or a substantial fraction of a population in order to monitor that group of citizens. The surveillance is often carried out by governments or governmental organisations, however, may also be carried out by corporations, either on behalf of governments or at their own initiative.

Malware

An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Pharming

An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.

Phishing

An Internet hacking activity used to steal secure user data, including username, password, bank account number, and security PIN or credit card number.

Spyware

An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.

General Overview

Before the digital age life moved much more slowly, news spread on paper, people talked in person or per letter and it was not until the invention of the telephone that people could make appointments on short notice. Since the launching of the World Wide Web the world stated to connect and through the easy immediate access and ability to talk to anyone anywhere anytime the world started to speed up. This also created an ideal platform for the dissemination of knowledge, where people are also encouraged to participate and use this for their own personal growth. Conjointly with the devices that allow people to use this platform anytime anywhere one cannot imagine a world without the Internet, what makes one even more vulnerable to exploitation through the Internet.

Human Rights

In article 12 of the Declaration of Humans Right it is stated 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.’ However, this article, which is binding to all UN member nations, is yet to be applied to the Internet. Logically this article applies to all privacy one could have, hence also the internet.

However, due to the fact that this article was written in a time before the internet existed, one could claim that this would not apply to the internet. It could be thought that the UDHR would evolve conjointly with the Human advancement, so this article would apply to

the internet. It would adapt an automatically cover all new aspects of the Human life. Only due to the increasing difficulty of Human life this is not so easy. One could therefore also argue that the UDHR is a stagnant legislation that is unchangeable and is applicable solely in the conditions it was written, only this would mean a possibility for adapting of the Declaration would be in order.

Concluding, the implementation of Article 12 is a sensitive issue, not solely by the sacristy of the Declaration itself, but also due to the extremely differing of opinions amongst the International Community (IC).

Mass Governmental Surveillance

In June 2013 Edward Snowden blew the whistle on the National Security Agency (NSA). He leaked classified information on the mass surveillance of hundreds of millions of people, whose phone calls, emails and searches were stored. There was a direct court order to Verizon to hand over all its telephone data to the NSA on an “on-going daily basis”. Furthermore, the NSA tapped directly into the servers of nine Internet firms, including Facebook, Google and Yahoo, which had as goal to track online communication in a surveillance program known as Prism. This surveillance clearly violates act 12 of the Universal Declaration of Human Rights with the key word arbitrary, which means based on random choice. Edward currently faces espionage charges in the United States of America (USA) but has been granted temporary asylum in the Russian federation.

In 2015 the China had a worse Internet connection to the rest of the world than in 2014; no other country’s Internet connection has deteriorated. All nations are improving their connection to the Internet and thereby the world. This deterioration of China’s connection has been because of the extreme censorship China is upholding. The most powerful monitoring body in China is the Communist Party’s Central Propaganda Department (CPCPD) that employs over two million workers that review Internet posts by using keyword searches. China has also recently instated the rating system, where citizens will be awarded point by what they search online or who their friends are and in accordance to their rate they will be granted more freedom and privileges. Moreover, the Chinese government also has the Golden Shield Programme in place colloquially known as the Great Firewall. This firewall makes large-scale use of Deep Packet Inspection technology to block access based on keyword detection. This makes all outside services, music or video content nearly impossible to reach for the normal Chinese people. All these efforts made by the Party strive towards Chinese digital sovereignty.

Corporate Abuse of the Internet

Not only governments practice mass surveillance, but also big corporations such as i.e. google. These corporations collect consumer's data and sell this to other companies. One's online information is worth vast amounts of money to big internet companies. Every site one visits is stored in one's online footprint and taken to the next site, etc. All these sites track the use of the internet of said users and adapt adverts to that information, possible links to different sites or their own products. The consumer is through this practice turned into the product, which is why one can use site free of charge, seeing that one's data provides enough profit.

However, since the implementation of the GDPR in Europe, European consumers have been protected against this 'surveillance' of big corporations and major corporations have been fined for non-compliance with this regulation. These big corporations now need explicit consent in order to track or store any data of its consumers.

Cybercrime

In this year and age cybercrime is the fastest growing area of crime, of course, due to the many aspects and possibilities for illegal activities. Many people are of yet not proficient enough to protect themselves against cybercrime, whether it is advanced cybercrime, sophisticated attacks against computer hardware and software, or cyber-enabled crime, 'traditional' crimes that have taken a new turn with the advent of the internet. This leaves especially older people, who have not grown up with the internet, vulnerable to many forms of cybercrime.

Many governments are already fighting against cybercrime, which has helped cyber-enabled crime to decrease in frequency. However, most governments are still not able to successfully eradicate all advanced cybercrime, seeing that this is mostly done by professionals that are extremely proficient in the cyber world.

Major Parties Involved

European Union (EU)

The Eu was the first intergovernmental organisation and the member states were the first to make clear regulation for the internet, which actually offered great protection for its

users. This regulation made it clear that citizens have the right to privacy on the internet and nor corporations nor governments are allowed to store data without explicit consent of the user. It does make clear that when clear indication of terroristic activity this privacy may be infringed. The EU has as result of the GDPR fined major corporations such as google exorbitantly. Within the EU a cyber security organ has been created: the European Union General Data Protection Service (EUGDPS). It ensures the upholding of the GDPR by the member states.

Human Rights Watch (HRW)

The Human rights watch is the largest NGO that advocates for Human Rights. They have taken it upon themselves to create dialog on the abuse of Human Rights on the Internet. They are great advocates for the implementation of Article 12 of the UDHR on the Internet.

People's Republic of China (PRC)

The People's Republic of China is a state where the Internet and the press is mostly controlled by the government and as such created a digital sovereignty. The government has deemed it vital to 'protect' it citizens from certain outside influences such as google or other such internet fora. The CPCPD is a body to place constant surveillance on its citizens. As an ultimate way of surveillance and censorship they have instated the rating system that arbitrarily violates their citizen's privacy.

Privacy international

Privacy International is an UK based NGO that challenge governments' powers by advocating and litigating for stronger protections. They lead research and investigations to shine a light on powers and capabilities, and to instigate and inform debate. They advocate for good practices and strong laws worldwide to protect people and their rights. They equip civil society organisations across the world to increase public awareness about privacy. They raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.

United States of America (USA)

The United States of America has been front and centre of the issue of privacy on the Internet ever since the Edward Snowden case. Former president Barrack Obama had taken some steps to better Internet Privacy, however the current president said he would prioritise

national security over respecting people's privacy on the Internet. Of course, this is an ethical statement, however this does blur the lines. It could also indicate prevention surveillance meaning privacy could be infringed even before any indication of wrongdoing has been alerted.

Timeline of Key Events

Date	Description of Event
10th of December 1948	The Universal Declaration of Human Rights (UDHR) was adopted, stating, in article 12, that the right to privacy as a fundamental human right.
4th of November 1952	The National Security Agency of the United States (NSA) was founded.
1975	First Personal computers are introduced, marking the beginning of the digital age.
2007	US Congress passes an anti-terror surveillance bill, allowing the PRISM program.
January, 2012	The European commission proposed a regulation to reform the data protection rules in the EU.
5th of June 2013	Edward Snowden releases NSA documents sparking huge controversy.
8th of April 2016	The European Council adopted the GDPR.
14th of April 2016	The European Parliament adopted the GDPR.
25th of May 2018	The General Data Protection Regulation (GDPR) was enforced

UN involvement, Relevant Resolutions, Treaties and Events

- Universal Declaration of Human Rights, 10th of December 1948 (Resolution Number)

Previous Attempts to solve the Issue

The UN is yet to make any major steps toward solving this issue. Until now all data protection legislation has been made on national level. However, the EU has made significant progress in solving this issue: the GDPR. It is a ground-breaking legislation in the field of internet privacy, by protecting its users from unauthorised data storage or tracking. It, furthermore, allows the EU to fine any non-compliant corporation, with the backing of the entire European market. It has already fined major corporations such as google for non-compliancy. With this legislation the EU is far ahead of the IC.

Possible Solutions

A first and probably the hardest solution one might consider is trying to establish a way to determine jurisdiction on the internet. In doing so one needs to consider all aspects of the internet and access points. The most important part would be what data belongs to which state, under which states sovereignty which sites lie, etc. It is the hardest solution one could implement but would reap the most benefit.

A second solution one might considers is transforming the GDPR into an international treaty, implemented within the entire IC. Of course, the GDPR is written based upon the Charter of the EU and therefore not directly transferable into a UN treaty. With this solution one needs to keep in mind to make signing and ratifying the treaty beneficial and attractive to members states in order for it to reach its full reach.

A third solution one could consider is establishing an organisation that would monitor and determine the severity of government surveillance, ultimately determining if the severity is necessary for the security risks. Moreover, creating internationally recognised and agreed upon actions in certain risk situations. This could, however, get difficult with the question of sovereignty, seeing that nations are not obliged to disclose any information on surveillance actions they are taking.

A fourth solution one might consider is to educate people about their digital footprint and the risk of the Internet. As of today, many people remain oblivious to the dangers the Internet holds and how horribly one is protected against said dangers. With knowledge one has more control and has a full comprehension of the impact of their daily Internet usage.

A fifth solution one might consider is ensuring Article 12 of the UDHR is applicable to the Internet. This would make protection against arbitrary infringement of one's privacy on

the Internet a basic Human Right, which would be a major step in this issue. This is of course, also one of the harder solutions, seeing the sacristy of the Declaration and needing practically all members states to agree to such a change.

A final solution one might consider is defining the legality of surveillance, meaning in what way may governments infringe on civilian's privacy for national security, how may governments infringe on said privacy. This would clarify the vague lines that define 'for national security'. It would be extremely difficult to find international consensus on this legislation.

Bibliography

"Arthur W. Diamond Law Library Research Guides." *International Internet Law - Research Guides*, www.library.law.columbia.edu/guides/International_Internet_Law.

"Edward Snowden: Leaks That Exposed US Spy Programme." *BBC News*, BBC, 17 Jan. 2014, www.bbc.com/news/world-us-canada-23123964.

"Universal Declaration of Human Rights." *United Nations*, United Nations, www.un.org/en/universal-declaration-human-rights/.

"What Is Internet Privacy?" *Techopedia.com*, www.techopedia.com/definition/24954/Internet-privacy.

"When It Comes to Internet Privacy, Be Very Afraid, Analyst Suggests." *Harvard Gazette*, 24 Aug. 2017, www.news.harvard.edu/gazette/story/2017/08/when-it-comes-to-Internet-privacy-be-very-afraid-analyst-suggests/.

Doctorow, Cory. "The Curious Case of Internet Privacy." *MIT Technology Review*, MIT Technology Review, 30 Dec. 2013, www.technologyreview.com/s/428045/the-curious-case-of-Internet-privacy/.

Jeavans, Adam Blenford & Christine. "After Snowden: How Vulnerable Is the Internet?" *BBC News*, 27 Jan. 2014, www.bbc.com/news/technology-25832341.

"Media Censorship in China." *Council on Foreign Relations*, Council on Foreign Relations, www.cfr.org/backgrounder/media-censorship-china.

Privacy International. “Cyber Security.” *Privacy International*, www.privacyinternational.org/topics/cyber-security.

Privacy International. “Data Protection.” *Privacy International*, www.privacyinternational.org/topics/data-protection.

Privacy International. “Government Hacking.” *Privacy International*, www.privacyinternational.org/topics/government-hacking.

Privacy International. “Identity and Privacy.” *Privacy International*, www.privacyinternational.org/topics/identity-and-privacy.

Privacy International. “Social Media Intelligence.” *Privacy International*, https://www.privacyinternational.org/node/55.

The Intercept. “NSA Deletes ‘Honesty’ and ‘Openness’ From Core Values.” *The Intercept*, 24 Jan. 2018, www.theintercept.com/2018/01/24/nsa-core-values-honesty-deleted/.

“Cybercrime.” *N2018-092 / 2018 / News / News and Media / Internet / Home - INTERPOL*, www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

Appendix or Appendices

I. “The right to privacy in the Digital Age”
http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

II. The EU General Data Protection Regulation
https://www.eugdpr.org

III. Privacy International
https://www.privacyinternational.org