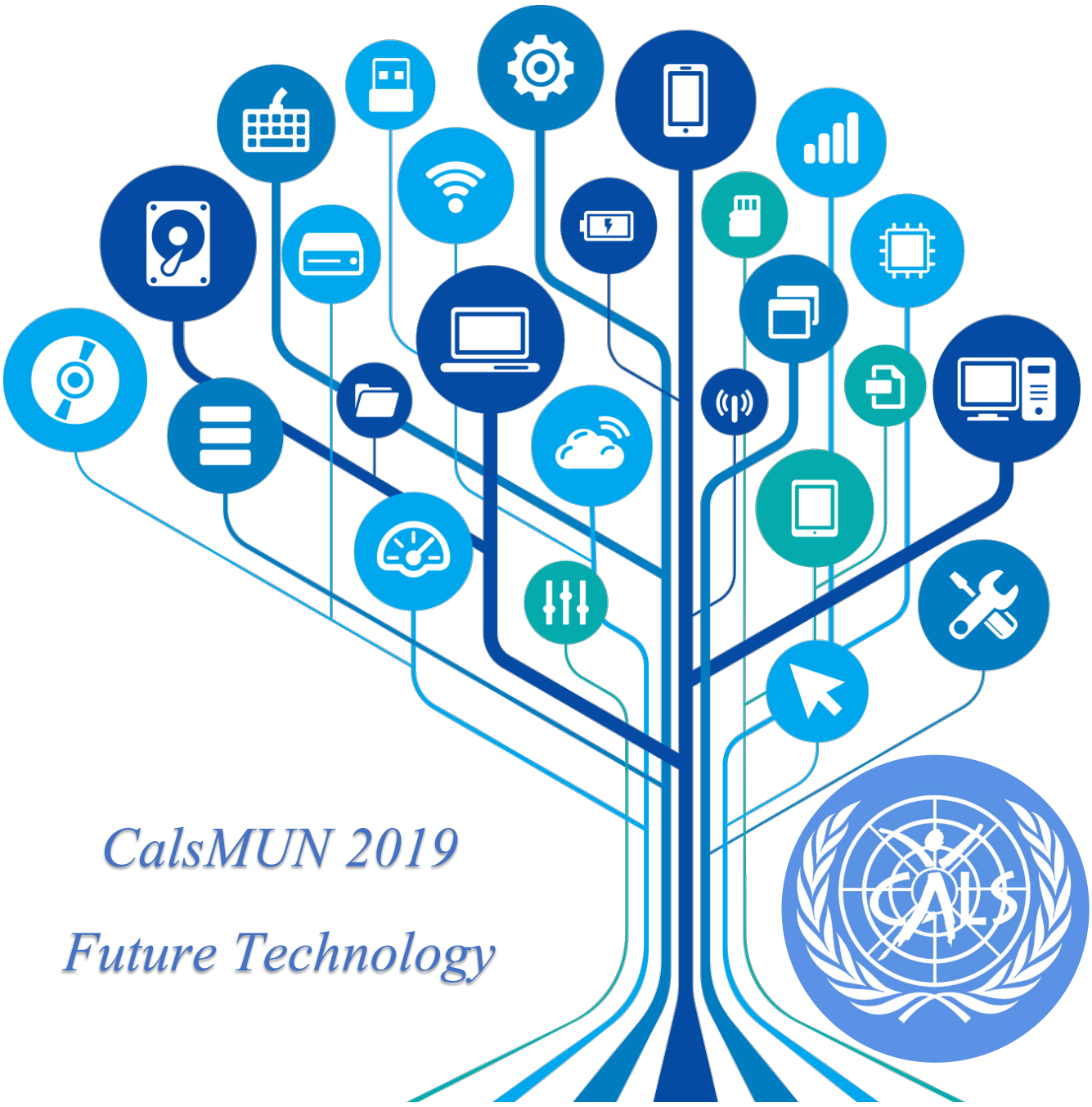

Research Report

Forum: General Assembly Sixth Committee

Issue: The border between online privacy and safety

Chairs: Raphael Ridder and Jonathan Thijs

Personal Introduction

Raphael Ridder

I am a student at the Stedelijk Gymnasium Haarlem (SGH), in my fifth year. I have participated in 21 conferences. I take part in the organisation of my schools very own HMUN as Head of Content. Furthermore, I am initiator of the annual TEDXYouth@Haarlem conference, whereof we will organise the second edition this year. I also am part of the Learning Across Borders organisation, the charity of the SGH. I was politically engaged from a young age, which my parents stimulated tremendously, by always encouraging me to question things and debate about issues we disagreed on. This interest has grown out into now a somewhat of an obsession, that I have been able to express in MUN and many other organisations I have been part of.

Jonathan Thijs

Hey! I am Jonathan, sixteen years. I live in Leiden (near to The Hague in the Netherlands) and I go to the Stedelijk Gymnasium Leiden. My free time is mostly spent on debating and on other activities around the field of politics. For example, I participate in 'regular' debating tournaments, I am active at a youth organization of a Dutch political party and I am eligible for the next elections of a layer of our government called the Provinciale Staten, with the hope of increasing my activity in those circles as well. However, I have set my eyes on studying something more scientific and exact – areas I am fond of as well – in a year, after a high school filled with debates. Furthermore, I play the piano, do water polo and like baking and cooking around. I will not be there the Saturday, as I unexpectedly have to be at a finale from another debating tournament, but the Sunday I will be present. Looking forward to the conference!

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 so making enforcing the law difficult. Even at this time the Internet is a place that one can use as one sees fit. People could use the Internet to store all our data, look through our devices and restore things we might have thrown out, use the cameras on our devices to look through and know the location of our devices at any given time.

In the digital era, people live their lives online, however not everyone is aware that everything the do online is being monitored and stored. Big corporations will track your online footprint from the moment you use their site. Hence, your privacy is worth more to these big corporations than it is to you. 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 things 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.

Definition of Key Terms

Cookie

A small text file created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk. They are a way to track your preferences throughout surfing the web. Cookies commonly are given as examples of ways that websites remember a person and can be hard to mitigate if one wishes to be 'forgotten' on the Internet.

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

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 30 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.

IP address

An IP Address or “identity protocol” address identifies one through their 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 of governmental organisations, but 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 wasn’t until the telephone that people could make appointments on short notice. Since the launching of the World Wide Web the world stated to connect and thru 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 us to use this platform anytime anywhere we cannot imagine a world without the Internet, what makes us even more vulnerable to exploitation through the Internet.

Government surveillance

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, has yet to be applied to the Internet. As such is the mass surveillance that multiple governments practice illegal according to article 12 on privacy of the Declaration of human rights.

In June 2013 Edward Snowden blew the whistle on the National Security Agency. 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 world than a year before; 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.

Cybercrime

In this year and age cybercrime is the fastest growing are 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

Organisations

European Union (EU)

Within the EU there has been created an organ the European Union General Data Protection Regulation (EUGDPS) that is an independent authority. It ensures the upholding of the data protection laws.

Human Rights Watch (HRC)

The Human rights watch is a NGO that is the largest organisation that advocates for Human rights. They have taken it upon themselves to create dialog on the abuse of human right on the Internet.

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.

Countries

People's Republic of China (PRC)

The People's Republic of China is a country where the Internet and the press is mostly controlled by the government and as such create a digital sovereignty. Recently they have instated the rating system that arbitrarily violates their citizen's privacy.

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 towards better Internet Privacy, however the current president said he would prioritise national security over respecting peoples' privacy on the Internet.

Timeline of Key Events

Date	Description of Event
10th of December 1948	The Universal Declaration of Human Rights (UDHR) was adopted, stating 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 regulation.
14th of April 2016	The European Parliament adopted the Regulation.
25th of May 2018	The General Data Protection Regulation (GDPR) was enforced

Previous Attempts to Resolve the Issue

The UN has until now not made any major steps towards the solving of this issue. However, within the EU there has been made significant progress to solving the issue. On March 2012, the European court of Justice proposed the European Union General Data Protection Regulation (EUGDPR) that protects users from unauthorised data storage and tracking. It is also there to ensure that all corporations follow the European laws data protection laws and are able to fine all non-compliant corporations. With this organisation instated the EU is far ahead of the International community.

Possible Solutions

A solution might be to educate people about their digital footprint, seeing that there still are a lot of people who are not aware that they are being tracked and their data is being stored. With knowledge these people will be able to fully understand the Internet and take control and seeing the impact of their Internet use.

A second solution might be an international variant of the EUGDPR that ensures that all organisations throughout the entire world will be forced to respect their users' privacy. Such an organisation must be a third party and cannot be controlled by a group of member states.

A third solution might be defining the legality of surveillance. Many nations already have digital surveillance in place, however with regulations that will legalise some supportive forms of surveillance you will be able to ensure that less privacy will be violated.

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*, www.privacyinternational.org/node/55.

Theintercept. "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.

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 (EUGDPR)
   https://www.eugdpr.org

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