Committee: Legal Committee

Issue: Assessing the security and privacy of digital footprints

Student Officer: Erika Koutroumpa

Position: Co-chair

PERSONAL INTRODUCTION

Dear delegates,

It is an honour and a privilege to be serving as a co-chair in the Legal Committee of the 3rd annual session of the ACGMUN conference. My name is Erika Koutroumpa and I am a junior at Pierce, The American College of Greece and this will be my first time as a student officer. Even though I have participated in 7 conferences, MUN has influenced me greatly and has played a significant role in forming my personality. I hope that those of you who will be attending a conference of such nature for the first time will enjoy it as much as I do, and will realise the magic that there is behind it.

That being said, this study guide will hopefully provide you with the necessary information to begin understanding the topic, as well as to build a strong foundation in order to be able to do even better and more wholesome research on the matter on hand, as well as your country's policy. I cannot stress how important it is also to conduct further research. In order to have a fruitful debate, you will need to have a good understanding of the topic, as well as your stance. The limited space of the study guide does not suffice to expound in all levels the topic. If you still have questions or if you need help in general, do not hesitate to contact me through my email, E.Koutroumpa@acg.edu.

Kind regards,

Erika Koutroumpa

TOPIC INTRODUCTION

The issue of the security and privacy of the digital footprints has started worrying the international community since the beginning of the 21st century, and especially in the past five years. Nowadays, we are well into the technological era, with new gadgets being invented nearly every single day. The internet is becoming more available at a very quick pace, especially in less economically developed countries with the help of projects of both governments and Non-Governmental Organisations (NGOs).

The web has a very specific reason why it has this great appeal to people from all over the world. It is a space that was created not long ago, with a seemingly endless amount of information and no governmental intervention yet. This gives people the ability to become more creative, start new projects and do something productive while helping others out through technology.

Sure, this very freedom and lack of restrictions aid people with unleashing their inner creativity and work in order to help the online community flourish, but it comes at a great cost indeed. The fact that there is no efficient and adequate legislation concerning intellectual property and safety on the web does not only mean that users are not protected from their data being used without their consent, but also that governments can use their traces in order to surveil innocent citizens.

There have been efforts by certain governments and even organizations in order to create applicable enactment in order to protect people's data and digital footprints; however, there is still a long way to go. Even though there have been treaties implemented by many countries across the globe, obedience to them is not compulsory for a great number of member states that have not ratified them, and hence they are often not applied. In addition, people have to be informed of their rights both in real life, but on the internet as well.

Hence, due to the lack of legislation and active measures, the privacy of citizens in the digital age is in jeopardy and the more Internet expands, the more this kind of issues will occur. The sooner this issue will be tackled, the better for both the individuals and the international community.

DEFINITION OF KEY TERMS

Digital footprints

The sum of all available information that exists on the Internet concerning a particular individual, as a result of all of their online activities. [1]

Active digital footprints

Active digital footprints consist of the data left when the user makes deliberate choices on the internet. A characteristic example would be any post made to social media accounts. When logging into project management or a similar site, the changes the person makes that are connected to that login name are also part of one's active footprint.[2]

Passive digital footprints

"Passive digital footprints are those left behind without intending to or, in some cases, without knowing it."[3] Consequently, it is the taking of any online information without an individual's consent. For instance, something that also counts as a passive digital footprint is when sites collect information about how many times someone visits a website. "They collect it when a device at your IP address connects with their website. This is a hidden process, and you may not realize it is happening at all."[4]

Privacy policy

"An internal statement that governs an organization or entity's handling practices of personal information. It is directed at the users of personal information. A privacy policy instructs employees on the collection and the use of the data, as well as any specific rights the data subjects may have."[5]

Cookies

[1] "Definition of digital footprint in English by Oxford Dictionaries", Oxford University, Oxford University, https://en.oxforddictionaries.com/definition/digital_footprint
[2] "What is a digital footprint? And how to help protect it from prying eyes (Norton Family Premier)", Norton Security, https://us.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html
[3] "What is a digital footprint? And how to help protect it from prying eyes (Norton Family Premier)", Norton Security, https://us.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html
[4] "What is a digital footprint? And how to help protect it from prying eyes (Norton Family Premier)", Norton Security, https://us.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html
[5] "Glossary of Privacy Terms (iapp)", iapp, https://iapp.org/resources/glossary

A packet of data sent by an Internet server to a browser, which is returned by the browser each time it subsequently accesses the same server, used to identify the user or track their access to the server.[6]

Browsing history

"A record of the information browsed by a user on a computer; especially (in a web browser) a record of recently visited web pages, stored with associated data."[7]

Net Neutrality

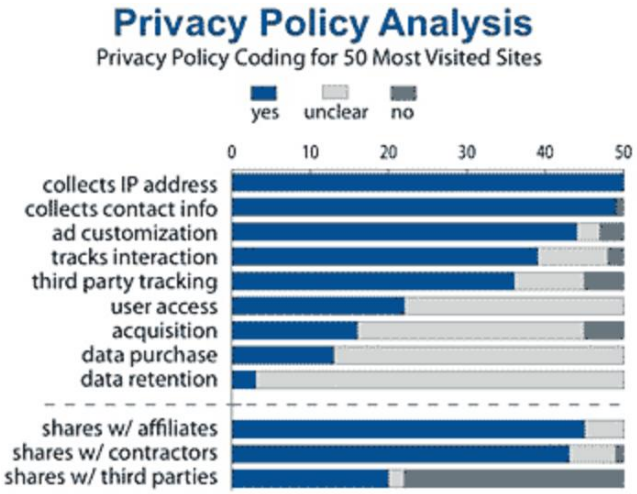
The principle that Internet service providers should enable access to all content and applications regardless of the source, and without favouring or blocking particular products or websites.[8]

BACKGROUND INFORMATION

Digital footprints have always existed, ever since the creation of the Internet back in 1983. However, their recent usage by third parties, as well as scandals like Facebook's illegal provision of users' data to statistics company Cambridge Analytica, have gathered lots of attention to the once overlooked digital footprints.

Usage of digital footprints in advertisement

Back in 2007, Dr. David Stiltwelt created an app for webpage Facebook called "myPersonality". What was so interesting about it was its ability to give results and comments based on the user's answers in its various psychometric tests. Certain users even allowed scientists to access their results, based on which an algorithm was created by the Cambridge Psychometrics team. It soon caused commotion all over the world, with people concerned with how this data could be possibly used by malicious third parties.[9]

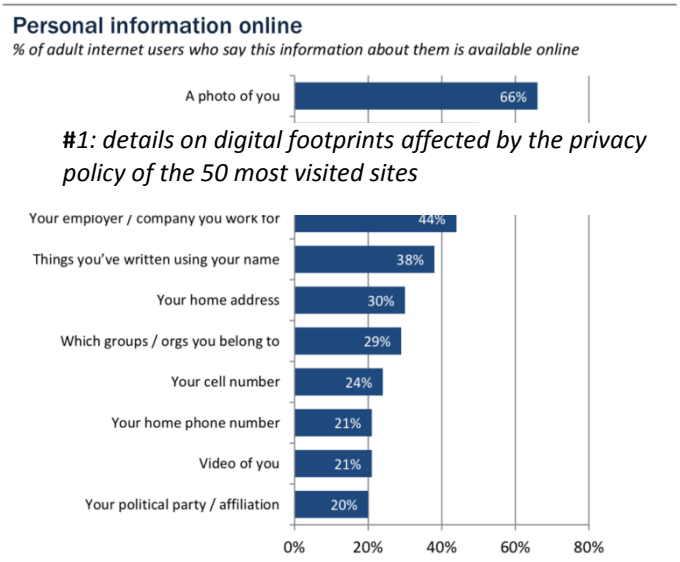


[6] "Definition of cookie in English by Oxford Dictionaries", Oxford University, Oxford University, https://en.oxforddictionaries.com/definition/cookie
[7] "Definition of browsing history in English by Oxford Dictionaries", Oxford University, Oxford University, https://en.oxforddictionaries.com/definition/browsing_history
[8] "Definition of net neutrality in English by Oxford Dictionaries", Oxford University, Oxford University, https://en.oxforddictionaries.com/definition/net_neutrality

Advertisers work in a similar way; collecting the data provided by the digital footprints, then analyzing it using algorithms and storing it for future reference. The main purpose of this practice is to create a consumer profile for each user and provide them with more targeted advertisements. However, in order for one's business to expand, another's rights to privacy should be violated. Something we must also bear in mind is that, most people are not aware that their digital footprints are being tracked, as well as stored for commercial use, making them completely ignorant of the dangers they might face[10].

Users' awareness of the digital footprints

Although people are slowly becoming more and more aware of the traces that they leave behind, they do not really take any initiative so as to tackle this problem. In a 2014 pew center research, 60% of the participants stated that they often do not pay attention to the traces they leave online. As a result, colleges, potential employers etc. have managed through the extensive research that they conduct on their applicants to find traces of the digital footprint that reveal inappropriate behavior. Moreover, research by "On Device Research" shows that 8% of the people questioned that belonged in the age group 16-24 were rejected by potential jobs due to inappropriate online activity.[11]



#1: details on digital footprints affected by the privacy policy of the 50 most visited sites

#2: graph showing results of research on active digital footprints

[9] "How to read a digital footprint (University of Cambridge)", Cambridge University, Cambridge University, 23 June 2015, https://www.cam.ac.uk/research/features/how-to-read-a-digital-footprint

[10] "Digital Footprints in the Context of Professional Ethics", Stanislava Neuruté Kligiené, Vilnius University, 2012, https://files.eric.ed.gov/fulltext/EJ1064289.pdf

[11] "From Diaries to Digital Footprints - The Changing Nature of Primary Sources in the Digital Age", Mark Johnson, University of Arizona, 2013, https://nau.edu/uploadedFiles/Academic/CAL/History/History-Social_Studies_Education/From%20Diaries%20to%20Digital%20Footprints.pdf

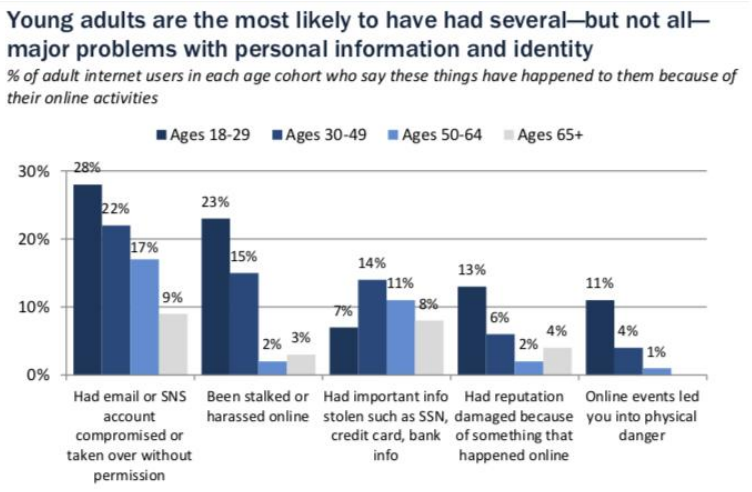
Digital footprints used by the states

Nevertheless, companies are not the only ones who have access to digital footprints. Many countries across the globe have also been observed to store such information and use them freely. For instance, the National Congress Library of the United States of America (USA) in 2010 started storing all tweets posted on social media platform "Twitter", during which time period it had 167 terabytes of online information.[12]

Other countries in the world, such as China, use digital footprints in order to surveil people and entire ethnic groups that they consider as threats because of their different beliefs. For example, the Chinese Government made citizens in Xinjiang region, with one of the biggest Muslim populations in the country, download a surveillance app called Jingwang, which means "web cleansing" or "clean net" in order for the government to observe and control any suspicious activity. According to the Human Rights Watch, accusations of digital surveillance have also been made for the USA and the United Kingdom (UK). The people monitored are not only from the respective countries, but they are from all over the world, while they are also often not suspected of any crime. The inadequate legislation gives, once again, leeway for breaches in the human rights of privacy and freedom of speech.[13]

Usage of digital footprints in cybercrime

The data can also be accessed by other internet users just as easily. With information like home address, phone number, birth date and bank account balance being available to a wider range of people whom most of the times do not have the best of intentions, leads to more and more people becoming victims of cyber-crimes, and in most cases phishing, fraud or identity theft.



#3: graph on issues provoked by young adults' digital footprints.

[12] "How Tweet It Is!: Library Acquires Entire Twitter Archive", Matt Raymond, Library of Congress, 14 April 2010, https://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/

[13] "Countries Should Protect Privacy in Digital Age - Human Rights Watch", Human Rights watch, Human Rights Watch,20 September 2013, https://www.hrw.org/news/2013/09/20/countries-should-protect-privacy-digital-age

Lastly, one of the most affected groups by cybercrime is children. A United Nations International Children's Emergency Fund (UNICEF) 2017 article that had as a case study the country of Malaysia supports that 26% of school kids have been cyberbullied, mostly between the ages 13 and 15, while 80% of victims raped by an internet acquaintance were aged 10-18.[14] Children are often not adequately informed about the proper usage of the internet and on how to protect their digital footprints. With more and more information available on social media nowadays, the job of predators is facilitated.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Canada

Canada is one of the countries actively taking part in resolving the issue. One of the most important legislation passed is the Personal Information, Protection and Electronic Documents Act (PIPEDA), a federal privacy law affecting the private sector, which is updated regularly. The PIPEDA includes clauses controlling the type of consent needed to be given by internet users, business transactions and contact information, data breaches, as well as special subcategories for minors.[15] The PIPEDA is very similar to the GDPR, with the latter having a stricter age framework and allowing data portability from one data controller to another.[16]

People's Republic of China

Even though the web in China came years later compared to other world superpowers it is developing rapidly, now being one of the main sectors of the Chinese economy. Ever since the very beginning of the Chinese internet, the government has tried to restrict access to unwanted websites. This is achieved through the Great Firewall, which prevents access to unsuitable web pages of political content, such as links to various human rights organizations, anything that has to do with the Tiananmen Square incident, articles criticizing the former Premier

[14] "For every child | digital safety", UNICEF, UNICEF, December 2017 https://www.unicef.org/sowc2017/index_101887.html

[15] "Online Privacy Law: Canada - Planning D-Day (April 2003) - Library of Congress Information Bulletin", Tariq Ahmad, Law Library of Congress, December 2017, https://www.loc.gov/law/help/online-privacy-law/2017/canada.php

[16] "Privacy Tracker | GDPR matchup: Canada's Personal Information Protection and Electronic Documents Act Related reading: GDPR matchup: The Children's Online Privacy Protection Act - Inside the ePrivacy Regulation's furious lobbying war", Timothy M. Banks, iapp, 2 May 2017, https://iapp.org/news/a/matchup-canadas-pipeda-and-the-gdpr/

Wen JiaBao, as well as inappropriate apolitical content[17]. A new cybersecurity law put into effect in June 1st 2017 increased restrictions, hindering the development of private internet companies and further promoting the federal services[18]. During the past year, the Chinese government has also been surveilling religious and ethnic minorities, many members of which have been persecuted. As mentioned before, users were also forced to download Jingwang (meaning web cleansing in Mandarin), an app which searches devices' files for blacklisted content.[19]

Turkey

Following the coup of 15 July 2016, the internet of Turkey has been characterized by instability. Websites such as WhatsApp and YouTube have been repeatedly suspended for national security reasons, while Wikipedia has permanently been banned due to sensitive political content regarding Turkey's part in the Syrian war. Virtual Private Networks (VPNs) have also been banned in order to ensure that blocked content will not be accessed, while people have also been arrested for online activity that gives off a pro-Kurdish sentiment, including journalists or other individuals who are against the ruling party.[20]

United States of America

Progress on this sector in the United States is a bit slow, as there have not been talks initiated in order to implement any stricter internet privacy laws in order for its citizens to be adequately protected. Relevant cases are mostly being judged based on civil and Tort law, and often regarding other sectors of the government or the economy. The modern way of approach on the issue is based on US Federal law of 1970.[21] However, they have recently become more sensitive on the topic, especially after the testimony of Mark Zuckerberg, creator of "Facebook", before the American Congress. According to reports, the data of 85 million users were harvested by Cambridge Analytica, an analytics company working on the Trump election campaign, in order for them to be targeted with advertisements.[22] Through

[17] "How web-connected is China? - ChinaPower Project", Chin Power Team, China Power, 28 December 2015, https://chinapower.csis.org/web-connectedness/
[18] "China - Freedom House", Freedom House, Freedom House, 2018, https://freedomhouse.org/report/freedom-net/2018/china
[19] "China - Freedom House", Freedom House, Freedom House, 2018, https://freedomhouse.org/report/freedom-net/2018/china
[20] "Turkey - Freedom House", Freedom House, Freedom House, 2017, https://freedomhouse.org/report/freedom-net/2017/turkey
[21] "Abuse and Misuse of Personal Information", John Stephenson, American Legislative Exchange Council, November 2015, https://www.alec.org/app/uploads/2015/11/Abuse-and-Misuse-of-Personal-Info-Final-03202013.pdf
[22] "Mark Zuckerberg to testify before Congress today. What you need to know - PBS", Saher Khan, PBS News Hour, 10 April 2018, https://www.pbs.org/newshour/politics/mark-zuckerberg-to-testify-before-congress-today-what-you-need-to-know

this, the company allegedly violated a 2011 consent decree with the Federal Trade Commission, something that was denied by Zuckerberg.[23]

TIMELINE OF EVENTS

Date	Description of event
24 October 1995	Directive 95/46/EC of the European Parliament on the protection of individuals with regard to the processing of personal data and its free Movement
26 July 2000	US – European Union (EU) Harbor framework is deemed as legally adequate by the EU commission
10 October 2008	Biometric Information Privacy Act legislation in Illinois
29 November 2011	Federal Trade Commission (FTC) agreement with Facebook on data protection and handling
6 October 2015	The European Court of Justice rules the EU-US harbor agreement as invalid in Maximilian Schrems vs Data Protection commissioner case
15 December 2015	Agreement between the European Parliament and the European Council and finalization of the GDPR
1 June 2017	New internet restrictions imposed by the Chinese government
10 April 2018	Zuckerberg congress testimony and apology for the mishandling of 85 million users' data

RELEVANT RESOLUTIONS, TREATIES AND EVENTS

UN declaration of human rights, article 12 (10 December 1948)

[23] "Mark Zuckerberg Tells Senate: Election Security Is An 'Arms Race' - NPR", Camila Domonoske, US National Public Radio, 10 April 2018, https://www.npr.org/sections/thetwo-way/2018/04/10/599808766/i-m-responsible-for-what-happens-at-facebook-mark-zuckerberg-will-tell-senate

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

According to this specific article of the Declaration of Human Rights, it is clear and of great importance that the rights of all people, no matter the minority they belong to, should be protected by the member states. Even though it does not specifically refer to the law on the internet, it is still legally binding in all aspects of everyday life and taken well into consideration.

European Convention on Human Rights, Article 8 (3 September 1953)

1. "Everyone has the right to respect for his private and family life, his home and his correspondence."

2. "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

As seen in the above clauses, the right to internet privacy is considered as of fundamental importance. States are the only ones who can intervene, however this applies only to matters of national security and/or to protect the citizens. Still, it is important to pinpoint that each country considers different matters as important in order to intervene with a person's privacy.

OECD Guidelines on the protection of privacy and Trans-Boarder Flows of Personal Data, part 3 (23 September 1980)

16. "Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure."

18. "Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."

As it has been made obvious by the above-mentioned articles, the safe transition of data from one state to another should be of utmost importance. What is more, according to the guidelines, under no circumstances must the Member States create national legislation aiming to restrict the process of the transborder flow of personal data.

Council of Europe Convention for the protection of Individuals with Regard to Automatic Processing of Personal Data, chapter 3 (28 January 1985)

This convention recognizes the right of people to privacy and to the safety of their internet data, as well as the obligation of the states to protect it and handle it according to the country's national jurisdiction. One of the most important articles of the convention is article 5, in which it is highlighted that internet data ought to be handled by the state lawfully, with the clear and informed consent of the user, except for cases where there is a legitimate reason to do the opposite.

EU Data protection directive (24 October 1995)

The EU Data protection directive could be characterized as a first attempt at protecting users' privacy while protecting the free economic movement system used by the EU in its economy. This directive calls for the creation of common legislation between the countries of the Union.

U.S E.U & U.S. - Swiss safe harbor framework (26 July 2000)

In order to bridge the differences in legislation due to the EU directive of 1995, the United States of America signed a common framework, also known as the safe harbor agreement. Forthwith, on 6 October 2015, the European Court of Justice issued a statement deeming the 26 July 2000 EU decision on the adequacy of the convention as invalid, replacing it with the FTC Privacy Shield Framework.

UN resolution 68/167; the right of privacy on the digital age (18 December 2013)

This resolution was based on the relevant report of the special rapporteur and it highlights the importance of privacy, hence making it a fundamental human right. On those grounds, the resolution calls for all members to take measures to protect their people's digital privacy, with one of the suggested ways being the creation of relevant legislation.

The EU General Data Protection Regulation (GDPR) (15 December 2015)

The logical step after the E.U. data protection directive was the creation of official permanent legislation recognized by all Member States of the European Union. Hence, finalized on 15 December 2015, the E.U. general data protection regulation took its place, aiming towards the adoption of common legislation by all EU countries, the protection of EU citizens' right to privacy, as well as the reformation of regional organizations' approach towards data privacy

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Digital Footprint Project

The UNI Global Union/ UNI Europa, in collaboration with the Foundation for the European Progressive Studies (FEPS) and the University of Hertfordshire, has created the Digital Footprint Project. Its aim is to properly comprehend the implications of the digital revolution, as well as to understand the digitalized labor market in the EU while proposing a new policy and legal ground to equate the digital with the traditional labor market.[24]

Predator on my Phone

Back in 2017, UNICEF started an initiative in order to ensure children's safety and access online. As a result, they collaborated with popular Malaysian media outlet R.AGE to begin the "Predator in my Phone campaign", whose aim was to use social media against the sexual predators who abuse its power in order to lure in young victims. The result was for the Sexual Offences Against Children Act to pass, something of great importance, since there were no previous legislation[25].

EU Data Protection Laws

[24] "Digital Footprint - UNI Europa, the voice of 7 million services workers." UNI Europa, UNI Europa, https://unieuropaprojects.org/digital-footprint/

[25] "For every child | digital safety", UNICEF, UNICEF, December 2017 https://www.unicef.org/sowc2017/index_101887.html

The European Union recently came up with an act whose aim is to protect the data and information of internet users from companies both from and out of the EU. This series of laws ensures the right of deleted information to be forgotten as well as the usage of a user's data only under certain legal obligations and agreements, whilst also including a series of laws that aim towards children protection on the internet.[26]

International principles on the application of human rights to communications surveillance

On 10 July 2013, a set of international principles in order to protect citizens from internet surveillance violating their human rights were made public by a broad group of civil rights activists in Geneva, also endorsed by the Human Rights Watch (HRW).[27] The demands of these principles are that surveillance on the internet should be legal, non-discriminatory and with valid reasons, take place only when considered absolutely necessary and only when less evasive techniques have previously failed.[28]

POSSIBLE SOLUTIONS

In order to find possible solutions, delegates should include clauses that cover all aspects of the issue, both the abuse of privacy by governments and companies or cybercriminals.

Firstly, one of the most important measures that need to be taken is the creation of an internationally recognized treaty, which will be supported and signed by every nation across the world. As explained previously, various Member states have made guidelines on rules of conduct on the internet in order to ensure the safety of the digital footprints. However, they are not legally binding and do not apply for all. The legislation ought not to be limited to laws about companies only but government interference as well. Hence, the creation of needed statute recognized by all states with stricter penalties could be proposed.

Furthermore, since the problem is not widely known yet, another possible solution would be to spread awareness to the public and to inform them for their

[26] "Help and advice for EU nationals and their family - Your Europe, European Union", European Union, europa.eu, https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm
[27] Countries Should Protect Privacy in Digital Age - Human Rights Watch
[28] "INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE - Necessary & Proportionate", May 2014, Necessary and Proportionate coalition, Necessary and proportionate, https://necessaryandproportionate.org/principles

rights, through the means that the delegates will consider as the most effective. This could take various forms, such as media campaigns, school programs and seminars.

Lastly, measures for the prevention of this phenomenon could also be the implementation of advanced technology in order to both detect and prevent cybercrime. This could be achieved through the creation of a stronger net infrastructure that will be more difficult to be breached, the foundation of an international IT board for cybercrime prevention and international conferences for the sharing of prevention techniques and ideas.

BIBLIOGRAPHY

General Bibliography:

"Digital Footprints in the Context of Professional

Ethics", Vilnius University, Institute of Mathematics and Informatics, August 2011, https://files.eric.ed.gov/fulltext/EJ1064289.pdf

"Your Digital Footprint", Intel Lean Easy Steps, 2015, https://www.intel.com/content/dam/www/program/education/us/en/documents/intel-easy-steps/easy-steps-activity-digital-footprint.pdf

"From Diaries to Digital Footprints - The Changing Nature of Primary Sources in the Digital Age", Mark Johnson, Concordia International School Shanghai, 2013 Annual Western History Association on Methodologies for Teaching Frontiers, Borderlands, and Imagined Places, https://nau.edu/uploadedFiles/Academic/CAL/History/History-Social_Studies_Education/From%20Diaries%20to%20Digital%20Footprints.pdf

"How does Legislation affect Digital Footprints?" , Internet Society's Identity and Privacy , https://www.internetsociety.org/wp-content/uploads/tutorials/How_Does_Legislation_Affect_Digital_Footprints/presentation_content/external_files/How_Does_Legislation_Affect_Digital_Footprints.pdf

"How Tweet It Is!: Library Acquires Entire Twitter Archive", Matt Raymond, Library of Congress, April 14 2010, https://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/

"How to read a digital footprint", University of Cambridge, University of Cambridge, January 23 2015, https://www.cam.ac.uk/research/features/how-to-read-a-digital-footprint

"The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years", Key Changes with the General Data Protection

Regulation – EUGDPR, Key Changes with the General Data Protection Regulation – EUGDPR, https://eugdpr.org/

"Your Digital Footprint: What Is It and How Can You Manage It?", Rasmussen College, Rasmussen College - Regionally Accredited College Online and on Campus, www.rasmussen.edu/student-experience/college-life/what-is-digital-footprint

"Digital Footprint", Virtual Library, https://www.virtuallibrary.info/digital-footprint.html

"Glossary of Privacy Terms", iapp, https://iapp.org/resources/glossary

"Cybercrime", Merriam – Webster, https://www.merriam-webster.com/dictionary/cybercrime

"PHISHING | meaning in the Cambridge English Dictionary", Cambridge Dictionary, Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/phishing

"Digital Footprints", Pew Research Center: Internet, Science & Tech, February 4 2014, http://www.pewinternet.org/2007/12/16/digital-footprints/

"EUR-Lex Access to European Union law", EUR-Lex - 52011DC0681 - EN - EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

"Chapter 03: Your Digital Footprint Matters", John Wegener, Privacy and Security Online, http://www.users.miamioh.edu/viscokj/IMS201/website/chapter-03.html

"Cookie | Definition of cookie in English by Oxford Dictionaries", Oxford Dictionaries, Oxford Dictionaries | English https://en.oxforddictionaries.com/definition/cookie

"Data Protection", European Union, European Union, https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm

"European Convention on Human Rights", European Court of Human Rights, European Union, https://www.echr.coe.int/Documents/Convention_ENG.pdf

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

"U.S.-EU Safe Harbor Framework", Federal Trade Commission, Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework

"United Nations Official Document", United Nations, United Nations, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

"Countries Should Protect Privacy in Digital Age", Human Rights Watch, Human Rights Watch, April 17 2015,https://www.hrw.org/news/2013/09/20/countries-should-protect-privacy-digital-age

"GDPR matchup: Canada's Personal Information Protection and Electronic Documents Act", iapp, May 2 2017", https://iapp.org/news/a/matchup-canadas-pipeda-and-the-gdpr/

"For every child | digital safety", UNICEF, UNICEF, December 2017 https://www.unicef.org/sowc2017/index_101887.html

"Digital Footprint - UNI Europa, the voice of 7 million services workers." UNI Europa, UNI Europa, https://unieuropaprojects.org/digital-footprint/

"Mark Zuckerberg Tells Senate: Election Security Is An 'Arms Race' - NPR", 10 April 2018, Camila Domonoske, US National Public Radio, https://www.npr.org/sections/thetwo-way/2018/04/10/599808766/i-m-responsible-for-what-happens-at-facebook-mark-zuckerberg-will-tell-senate

Figures

"Anonymity, Privacy and Security online", Pew Research Centre, 5 September 2013, http://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

"Report: Widespread data sharing, 'Web bugs'", Kathleen Maclay, Phys.org, 2 June 2009, https://phys.org/news/2009-06-widespread-web-bugs.html