**Issue:** Reducing the infringement of the right on privacy in the digital age

**Forum:** Special Conference 1

**Position:** Deputy Chair

**Name:** Filip Hellman

# Introduction

For the past few decades, technology has been improving and developing at an astronomical rate. It has allowed for innovation in things such as medical treatment, law enforcement. data storage, online contact and many other things. However, as the quote goes; "With great power comes great responsibility", this has led to issues as well. Improvement in technology and internet access has allowed for the misuse of this technology for things such as mass identity theft, personal data being leaked, cyber terrorism, hacks into government facilities causing instability, election interference and many other things.

The main issue that this report will be discussing is the debate over the right of privacy on the internet, how much it is being infringed and how it could be improved. With this becoming more and more relevant to everyday life, the question about whether people on the internet even have privacy, has been raised, and who is responsible for this. People themselves obviously have to be careful, but it has started to become clear that different companies and governments have been responsible for this and it has become a debate on a political


level, with different countries having different views/policies on the issue.
https://www.irishtimes.com/opinion/state-s-approach-to-data-privacy-is-a-national-scandal-1.3246055

# Definition of Key Terms

**Personal data:** Information that relates to an identified or identifiable individual.

**Data protection:** Legal control over access to and use of data stored in computers.

# General Overview

Over the past decade or so, there has been rising concern over user's privacy on the internet, and how much of what they do or how much of their data is actually recorded or leaked. The two main sides to this issue have been;

- Websites, social media companies, advertising companies etc.

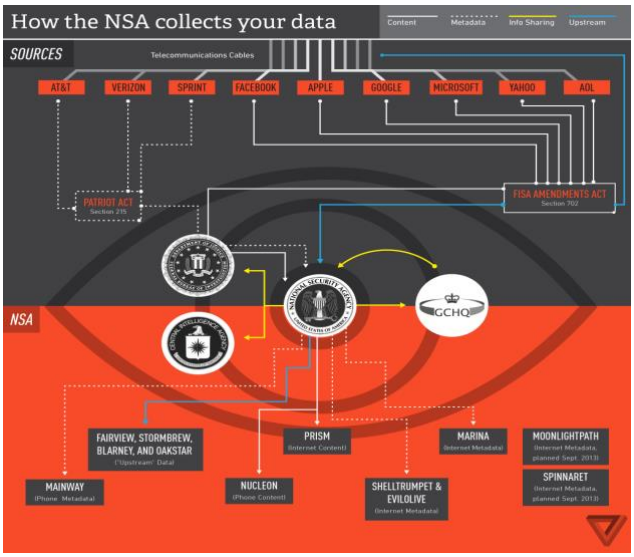
- Government surveillance on the internet.

To start with, as many may know due to large media exposure, there have been many sandals involving companies such as Facebook, WhatsApp, Yahoo etc. where mass user information that was stored by the companies was leaked and privacy of users was infringed. For example, the 2018 'Facebook - Cambridge Analytica' scandal where the profiles and private information of over 87 million Facebook users was leaked to the UK based political consulting firm Cambridge Analytica. This triggered large outrage toward both Facebook and CA, ending with the firm going defunct and Facebook facing large backlash with the CEO, Mark Zuckerberg, actually testifying on the issue in front of US congress.

There have been many other scandals such as this one. For example, Yahoo having 1 billion user accounts hacked in 2013/14 and also 500 million user accounts being leaked to US government intelligence in 2016.

This also brings up the subject of Government access to private information. After the September 11 attacks, the US Government agency, NSA, started mass surveillance on citizens in the name of counter terrorism. This was not known to the general population until Wikileaks exposed it, and the US government was forced to declassify the issue. While law allowed for this to happen, it has become a large civil and political debate over if governments should have access to this kind of information or not, and if the name of counter terrorism is a proper justification.

https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet




This has been a large debate in the UK as well for example, with the 2016 Investigatory Powers Act. This expanded the surveillance powers of UK intelligence agencies on citizens to better fight crime. This has also since sparked large public debate over if this should be allowed or not.

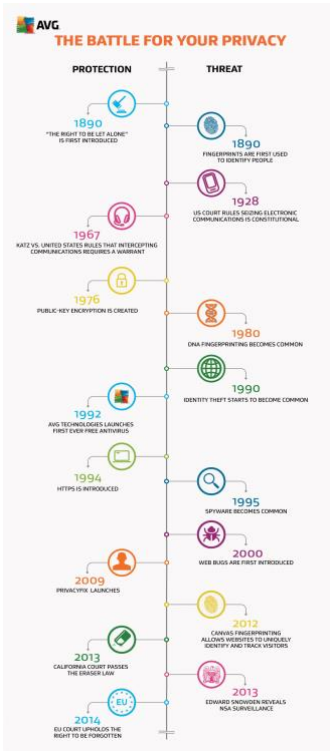
While a lot of the reasoning for all of this is counter terrorism, many people believe that their privacy is being infringed too much in the name of this, and that it is unnecessary and simply infringes personal liberty. There is a prominent argument stating that the government should not be getting involved in the private lives of people, and there is risk of this data getting into the wrong hands.

***"Does the UK really want the dubious honor of introducing powers deemed too intrusive by all other major democracies, joining the likes of China and Russia in collecting everyone's browsing habits?"*** - Anne Jellema, head of the 'World Wide Web Foundation

# Major Parties Involved

## The United States and the United Kingdom

As discussed earlier, there has been large public debate over the right of online privacy in the US, with the knowledge of mass government surveillance since the 2001 9/11 attacks, but yet no proper law/legislation regulating




Pappas, Calvin. "A Brief History of Digital Privacy." *AVG Now*, 8 Aug. 2014, now.avg.com/history-digital-privacy.

online privacy of US citizens. Many of the companies which have faced scandals, such as Facebook and Yahoo, are US based and some, such as Yahoo, have actually involved information exposure to the US government itself.

With the EU for example introducing the GDPR law, there has been growing pressure for the US to start introducing data protection law.

The United Kingdom has had similar political and social debate over the issue, especially since the 2016 Investigatory Powers Act, and also the Facebook scandal involving the UK based Cambridge Analytica. Now that Brexit is happening, tensions have been rising in the UK concerning wether the country will follow the GDPR or not, and what there is to come for online privacy rights for the UK.

# The European Union

For over a decade, there has been large debate over online privacy in the European Union, and there has been a fight for legislation and regulation to protect it. In April 2016, the European Parliament approved the

**2016 – January**
**April 8th** – Adopted by the Council of the European Union
**April 16th** – Adoption by the European Parliament
**May** – Regulation will enter into force 20 days after it is published in the EU Official Journal

**2015 – December 15th**, the Parliament and Council have come to an agreement, and the text will be final as of the Official signing to take place in early January of 2016.

General Data Protection Regulation, and came into force in May 2018.

This was a major success for the rights of EU citizens, allowing for much stronger personal protection on the internet, with rights such as; Right to Access, Right to be Forgotten, Breach Notification, Data Portability, Privacy by Design and Data Protection Officers (EU GDPR.org).

The aim of it is essentially to also give EU citizens more knowledge and control over the use of their personal data. This is the reason for new regulations on people having to give permission for different things

**2015 – June 15th**, the Council of the European Union approved its version in its first reading, known as the general approach, allowing the regulation to pass into the final stage of legislation known as the "Trilogue"

**2014 – March 12th**, the European Parliament approved its own version of the regulation in its first reading

**2012 – January 25th**, initial proposal for updated data protection regulation by the European Commission

such as photo use.

However, there has also been debate over if the EU is implementing regulation that is too strong and may be negatively affecting businesses. There has also been large debate over the way this legislation is adopted in the EU and if it is fair, with recent proposal of Article 13/11 copyright plan which would harm independent online creators greatly.

# Russia

One of the most known international issues is the extreme lack of online privacy in countries such as Russia. For example, the Russian government has been accessing personal information and communications of citizens for many years and has introduced law which gives the government even more control over this. Freedom of media and speech is not at a very good level in Russia, and people these days have to be very careful with their internet usage, given events such as when members of a WhatsApp group were arrested in Russia after criticising police over text. It has been known in Russia that in a lot of cases, that there is very little privacy for citizens with what they say or do, and now especially with access to the internet.

This is the case in other more authoritarian states such as China, where data privacy has been infringed due to freedom of speech and things such as that. With the growing awareness about this in the modern day, more and more people have started to protest against these issues and there is growing media awareness on it as well.

# Previous attempts to resolve the issue and possible solutions

As discussed earlier, with new regulations such as the GDPR, there has been a rise of awareness in online privacy rights, with citizens of other countries demanding for stronger protection laws and governments heading for plans for the future, after the EU became the first to introduce such strong regulation. People are also more aware now, and new methods of protecting your privacy on the internet are coming around, and people being more educated on the issue.

There are also growing movements to stop government surveillance and growing political debate over this becoming a more serious issue. Many countries have different stances on this and is a growing topic on the international and diplomatic stage.

In conclusion, countries such as the US could develop greatly from better protection law such as the EU's GDPR, but it is not that easy to simply stop the leaking of information. After scandals and government surveillance, the issue of hackers and recklessness still remains. There is always a way for hackers to find out information about people, as when you are not careful it is very easy to leak information and for this information to be found without a large corporation breaking law, but simply a skilled hacker using social engineering skills. There should be more awareness spread about being careful with what data you share on the internet, and how careful you are.

# Appendix/Appendices

# Bibliography

https://www.technadu.com/worst-internet-privacy-scandals/30236/

https://en.wikipedia.org/wiki/Mass_surveillance_in_the_United_States

https://www.mirror.co.uk/tech/13-ways-your-privacy-violated-9479084

https://www.legislation.gov.uk/ukpga/2016/25

https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html

https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

https://eugdpr.org

https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1

https://hackernoon.com/russias-internet-privacy-is-dead-dfdd58cb9abb

https://www.economist.com/china/2018/01/25/in-china-consumers-are-becoming-more-anxious-about-data-privacy