Committee: Legal Committee

Issue: The question of government access to personal data held by the private sector

Student Officer: Marilina Gerasimou

Position: Deputy president

INTRODUCTION

Businesses and individuals have the reasonable expectation that the information they create and store in digital form should be accorded the same privacy protections as the information they commit to paper. To fight crime and protect public safety, governments have a clear and compelling need to access digital data. Balancing that interest against their citizens' expectations of due process and the rule of law is essential to maintaining trust in technology. This makes it a critical priority to craft modern laws that provide law enforcement and national security agencies with appropriate mechanisms to access digital information pursuant to lawful process. These laws should protect citizens' fundamental privacy rights, and respect the sovereignty of other nations.

For any further information needed, please do not hesitate to contact me through my mail (marger049@gmail.com). Remember that my role is to guide you through the process of preparation and note that I will be willing to answer any questions on this topic.

Important note from the chairs' team

In order for the chairs to fully understand the dynamics of the committee, discovering any
misunderstanding prior to the debate and for the better preparation of the delegates you
are asked to proceed as indicated below;

1) Conduct your chairs via email and informing them about your mun experience so that they can know what exactly to expect of you.

2) Prepare and send your chairs by 11:59 of the 6th of November one position papers for
each of the topics you are going to discuss during the conference. You can conduct the expert chair, of each topic for further information concerning your country's policy if needed, and for general guidance when it comes to your position papers (word limit structure etc). You are going to receive general comments during the lobbying for your position papers as well as personal feedback and grades for your papers. The points you will receive will add up to your general score which is one of the factors that determine the best delegate award. If you for any reason fail to send your papers before the final deadline you will not be eligible for any award.

DEFINITION OF KEY TERMS

Term 1: Personal Data

Personal data is information that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

Term 2: Government access

Government demands for data held by the private sector, including an expansion in government requests for (i) direct access by the government to private-sector databases or networks, or (ii) government access, whether direct or mediated by the company that maintains the database or network, to large volumes of data.

In most, if not all countries, the law provides an inadequate foundation for systematic access, both from a human rights perspective and at a practical level. Systematic surveillance

programmes are often not transparent and based on secret governmental interpretations of the law, and there is often inconsistency between published law and government practice.

[1]BACKGROUND INFORMATION

In recent years, there has been an increase worldwide in government demands for data held by the private sector, driven by a variety of factors. This increase includes an expansion in government requests for what could be called 'systematic access': direct access by the government to private-sector databases or networks, or government access, whether direct or mediated by the company that maintains the database or network, to large volumes of data. Recent revelations about systematic access programs conducted by the United States, the United Kingdom and other countries have dramatically illustrated the issue and brought it to the forefront of international debates.

Systematic access raises hard questions for companies that face demands for government access to data they hold. They must decide whether the demand or request is lawful, though the law may be vague. Although it seems that systematic access is growing, there are also cases—in Germany, Canada, and the UK—where government proposals for expanded access have recently been rejected due to public and corporate concerns about privacy, cost, and the impact on innovation. Companies must also decide what information about their responses to these demands they may disclose to their customers and to the public—the 'transparency' issue that has received increased attention since June 2013.

In our digital society the phenomenon of gaining access to personal data is enhanced, since governmental sources manage to breach digital accounts held by private companies.

The Cambridge Analytica scandal has been the latest in a series of eruptions that have caught peoples' attention concerning the data breach.[2] Cambridge Analytica is a company that offers services to businesses and political parties. It is able to analyse huge amounts of consumer data and combine that with behavioural science to identify people who organisations can target with marketing material. It collects data from a wide range of

[1] Abstract from the article: Systematic government access to personal data: a comparative analysis, Ira S. Rubinstein, Gregory T. Nojeim, Ronald D. Lee, International Data Privacy Law, Volume 4, Issue 2, May 2014

[2] The Cambridge Analytica Files, Hilary Osborne, The Guardian, 18/03/2018, https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach

sources, including social media platforms such as Facebook, and its own polling. During the 2016 US presidential elections, the company worked on three candidates' campaigns for the presidency, including Trump's. On its website it describes analysing millions of data points to identify the most persuadable voters and the issues they cared about and then sending them messages to "move them to action". Voters in 17 states were polled every day, and online advertising and social media used to send them messages. The company claims that in this way it boosted donations and turn out and contributed to Trump's victory.As we now know, some of the data came from profiles to which the company was not supposed to have access, rather than being freely available to harvest.

Legal Framework

In most, if not all countries studied, existing legal structures provide an inadequate foundation for the conduct of systematic access, both from a human rights perspective and at a practical level. Transparency about systematic surveillance programmes is weak, so it is difficult to achieve an accurate or comprehensive understanding of systematic access. Nevertheless, the relevant laws are at best vague and ambiguous, and government interpretations of them are often hidden or even classified; that practices are often opaque (because it is sometimes in the interests of both governments and companies to proceed quietly, and the companies are often prohibited from public comment); and that oversight and reporting mechanisms are either absent or limited in scope when they exist, and generally do not reach voluntary data sharing. Transparency remained weak even after information about some systematic surveillance activity appeared in the press as a result of leaks of classified in- formation by former NSA contractor Edward Snowden in 2013. Access for regulatory, law enforcement, and national security purposes is often excluded from laws; alternatively, they are treated as accepted purposes for which access is authorised under separate laws that may or may not provide adequate safeguards against possible abuses.

Systematic Access

Governments around the world have long sought access to personal information about individuals. The past half century witnessed the rise of what Professor Paul Schwartz has

described as the 'data processing model of administrative control',3 in which data are routinely collected and used for many purposes including to deliver social services, administer tax programmes and collect revenue, issue licences, support hundreds of regulatory regimes ranging from voter registration to employee identity verification, operate public facilities such as toll roads and national parks, and for law enforcement and national security.[4]

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

EU General Data Protection Regulation (or GDPR)

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the European Union, regardless of the company's location.

National Security Agency (NSA)

The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both signals intelligence (SIGINT) and information assurance (now referred to as cybersecurity) products and services, and enables computer network operations (CNO) in order to gain a decision advantage for the United Nations and their allies under all circumstances.

[3]Paul Schwartz, 'Data Processing and Government Administration: The Failure of the American Legal Response to the Computer', (1992) 43 Hastings Law Journal 1321, 1325 (emphasis in original). For more recent overviews, which confirm Prof. Schwartz's prescient description, see Ian Brown, 'Data Protection: The New Technical and Political Environment', (2010) 20/6 Computers & Law,; 'A Report on the Surveillance Society: For the Information Commissioner [UK], by the Surveillance Studies Network' (Sep. 2006).

[4]See generally Fred H Cate, 'Government Data Mining: The Need for a Legal Framework', (2008) 43 Harvard Civil Rights-Civil Liberties Law Review 436.

Privacy International

Privacy International is a charity that challenges governments and companies in order to protect the personal data of individuals or groups.

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.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.

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.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.

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
6 October 2015	The European Court of Justice rules the EU-US harbor agreement as invalid in Maximilian Schrems vs Data Protection commissioner case
April 2016	The GDPR was approved and adopted by the EU Parliament.
25th May 2018	GDPR came into force.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

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

"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 recognises 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 characterised 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 recognised by all Member States of the European Union. Hence, finalised 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 organisations' approach towards data privacy

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

EU Data Protection Laws

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.

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.

POSSIBLE SOLUTIONS

In order to find possible solutions, delegates should include clauses that cover all aspects of the issue, focusing on the abuse of privacy by governments.

Firstly, one of the most important measures that need to be taken is the creation of an internationally recognised treaty, which will be supported and signed by every nation across the world. Various Member-States have made guidelines on rules of conduct on the internet in order to ensure the safety of the personal data. 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 recognised 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 rights. 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, protect the digital personal data of the users and prevent the withdrawal of information even from governmental sources.

I would like to stress once more that you are welcome to contact me through my mail (marger049@gmail.com) for any questions that may occur to you concerning this topic during your research.

BIBLIOGRAPHY

1. Policy recommendation: Government access to data, https://news.microsoft.com/cloudforgood/_media/downloads/en/government-access-to-data-en.pdf
2. Information Commissioner' s Office, Guide to General Data Protection Regulation, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
3. Abstract from the article: Systematic government access to personal data: a comparative analysis,Ira S. Rubinstein, Gregory T. Nojeim, Ronald D. Lee,International Data Privacy Law, Volume 4, Issue 2, May 2014 (https://doi.org/10.1093/idpl/ipu004)
4. The Cambridge Analytica Files, Hilary Osborne, The Guardian, 18/03/2018, https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach
5. European Union, data protection and online privacy, https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm
6. EU General Data Protection Regulation, https://eugdpr.org/
7. National Security Agency & Central Security Service, Missions & Values, https://www.nsa.gov/about/mission-values/
8. The Privacy Project, https://theprivacyproject.org/?page_id=940
9. Privacy International, https://www.privacyinternational.org/about
10. "Data Protection", European Union, European Union,
11. https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm
12. "European Convention on Human Rights", European Court of Human Rights, European Union, https://www.echr.coe.int/Documents/Convention_ENG.pdf
13. "Universal Declaration of Human Rights", United Nations, United Nations,
14. http://www.un.org/en/universal-declaration-human-rights/
15. "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
16. "United Nations Official Document", United Nations, United Nations,

17. United Nations Official Document, Resolution adopted by the General Assembly on 18 December 2013 68/167. The right to privacy in the digital age, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167"

18. 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

19. Countries Should Protect Privacy in Digital Age - Human Rights Watch

20. "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

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

23. Paul Schwartz, 'Data Processing and Government Administration: The Failure of the American Legal Response to the Computer', (1992) 43 Hastings Law Journal 1321, 1325 (emphasis in original). For more recent overviews, which confirm Prof. Schwartz's prescient description, see Ian Brown, 'Data Protection: The New Technical and Political Environment', (2010) 20/6 Computers & Law,; 'A Report on the Surveillance Society: For the Information Commissioner [UK], by the Surveillance Studies Network' (Sep. 2006)

24. See generally Fred H Cate, 'Government Data Mining: The Need for a Legal Framework', (2008) 43 Harvard Civil Rights-Civil Liberties Law Review 436.