Model United Nations of Hamburg 2014

Forum:	Special Commission
Student Officer:	Rouven Riegel
Issue:	The issue of data protection regarding privacy rights

'The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose.'

Yael Onn, et al., Privacy in the Digital Environment, Haifa Center of Law & Technology, (2005) pp. 1-12

Description of the problem

Privacy is a value that is incorporated in our every day lives. We commonly trust our storage devices to be safe and to guard our most sensible information. Today, this is not the case. Cyber criminalism and data thefts are also part of our every day lives. AOL has the first major breach in 2004, healthcare providers dominate leaks around 2009, and gaming companies had the major data losses in 2012. It does not matter who one is, as long as one is using social media, owning a smartphone or a computer, sensible data is collected and therefore able to be stolen.

It becomes increasingly difficult to control what one reveals of himself in the internet. Various search engines collect data, data mining is used by many instances and social media becomes very hard to control.

This topic does not only refer to the internet, but also includes medical, financial, locational, political and educational information of an individual.

This information, which is collected by healthcare and educational institutions, contains sensitive data, which can be used, when stolen, for criminal activities such as identity theft. Information about the situation of health of a person could be, if not treated sensibly, lead to problems with finding an employment for example and would therefore restrict the personal freedom of a person to a large extend. These examples should be kept in mind when discussing the importance of privacy.

The fact, that all this information is present in the internet, makes the task of data

protection increasingly difficult as the internet grows and advances every second. Intelligence agencies acquire data in order to prevent terrorism and keep criminalist activities at bay. With the internet a whole new ground was established, providing space for cyber warfare and criminal activities. Politicians and governments all over the world did not pay attention to growing threat of the internet as a no-mans-land, as Angela Merkel stated: 'Das Internet ist für uns alle Neuland' (the Internet is new to every single one of us). This puts governments and citizens in a delicate position, the internet is international, not restricted by borders as our world is and legislations are difficult to make. The Internet is a space not regulated by law, which is also supported by the users being anonymous. How is one then supposed to establish international laws? Should the internet be restricted? To what extend is privacy in the interest of national and international safety justifiable? These are questions to be discussed in the Special Commission.

United Kingdom of Great Britain and Northern Ireland

The *Data Protection Act* of 1998 (DPA) is an Act of Parliament of the United Kingdom of Great Britain Northern Ireland which defines UK law on the processing of data in identifiable living people. Although the Act itself does not mention privacy, it was enacted to bring British law into line with the EU data protection directive of 1995 which required Member States to protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data. In practice it provides a way for individuals to control information about themselves.

United States of America

The Defence Department is the largest user of data-mining technology, followed by the Education Department, which uses private information to track the life of student direct loans and to monitor loan repayments.

The most widely reported data-mining project — the Pentagon's *Total Information Awareness* (TIA) program — was shut down by Congress because of widespread privacy fears. The project sought to use credit-card, medical and travel records to search for terrorists and was dubbed by privacy advocates as a "supersnoop" system to spy on US citizens

The US government argues, that 'acquiring' personal data of its citizens and other people, is done in order to guarantee the safety of the nation. According to the USA, data mining

and surveillance software is not threatening the privacy of an individual, as long as no illegal data is uncovered. If there is illegal data, or a threat posed by the individual on public safety, the individual looses the right for privacy. This argument is called the 'nothing to hide' argument. The US government regards data-mining and surveillance as necessary to guarantee the safety of its citizens, the Defence Department is the largest user of data-mining programs.

China

The chinese government introduced a Consumer Rights Protection law, which demands the consent of the consumer for the usage and the collection of his personal data. This law will step in effect on March 15th, 2014.

European Union

The collection of data is, in the European Union, only permitted under certain legislations. Organisations, individuals and companies have to guarantee the effort of protecting their own personal information. The EU regulations concerning data protection have been implemented to ensure international trade as well as a common gradient of safety guaranteed by equal laws in the EU. Since 29 March 2011, the EU is negotiating with the US government about an international framework agreement (Data Protection Umbrella Agreement) in order to protect personal data circulating between EU member states and the USA. This also includes the cooperation between the EU and the US concerning the prevention, detection, investigation and prosecution of criminal offences, including terrorism.

The *Data Protection Directive* (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law. On 25 January 2012, the European Commission unveiled a draft European General Data Protection Regulation that will supersede the Data Protection Directive.

Definitions:

Personal data: personal data is any information related to identified or identifiable on the basis of such information individual (personal data subject), including his last name, given name, patronymic, date, month, year and place of birth, address, family, social, property

status, education, profession, income, other information

Sensitive personal data: sensitive personal data means personal data relating to:

- Race or ethnic origin
- Political opinions
- Religious beliefs
- Health condition
- Sexual life

Data-mining: Sifting through very large amounts of data for useful information. Data mining uses artificial intelligence techniques, neural networks, and advanced statistical tools (such as cluster analysis) to reveal trends, patterns, and relationships, which might otherwise have remained undetected. In contrast to an expert system (which draws inferences from the given data on the basis of a given set of rules) data mining attempts to discover hidden rules underlying the data. Also called data surfing.

A right for privacy is explicitly stated under Article 12 of the Universal Declaration of Human Rights (1948): "*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.*"
Privacy is therefore a fundamental right and freedom, and shall be reserved.

Interesting to find out:

- **Is my country fully supporting the declaration of Human rights?**
- **Is my country part in any treaty or taking part in international lawsuits?**
- **Is in my country internet censorship permitted?**
- **Are there any laws concerning internet or internet censorship?**
- **In how far does my county support the idea of democracy? If it is very harsh their might emerge problems when it comes to a strong observation of internet activities)**

Sources:

http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf

http://www.privacycommission.be/sites/privacycommission/files/documents/guidelines_computerized_personal_data_files.pdf

http://ec.europa.eu/justice/data-protection/index_de.htm

http://www.washingtontimes.com/news/2004/may/28/20040528-122605-9267r/?page=all

http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

http://www.lexology.com/library/detail.aspx?g=04c77add-d3da-4f62-b79b-5fb3da5a7943

https://www.privacyinternational.org/reports/european-union/i-privacy-and-data-protection-in-the-eu

http://www.oas.org/dil/data_protection_privacy_habeas_data.htm