Committee: Human Rights Commision

Topic: The question of the right to privacy in the digital age

(Right to privacy in the digital age : Call for inputs, Business and Human Rights Resource Centre)

Committee:	Human Rights Commission
Issue:	The question of the right to privacy in the digital age
Written by:	Kiana Pajouhesh
Position:	Chair

Introduction

With the increasing interest and access to technology, privacy is becoming one of the biggest concerns of people around the world. The advances are improving real-time communication and information-sharing everyday is helping global information access and debates. These technologies have also become the tool to amplify voices of human rights defenders and helping to expose abuse which means that they can offer the promise of improved enjoyment of human rights. However, with the increase of users around the world, many are becoming vulnerable to electronic surveillance and interception. Recent discoveries have shown how new technologies are being developed covertly, often to facilitate these practices, with chilling efficiency. These surveillances threaten individual rights - including to privacy and to freedom of expression and association – and inhibits the free functioning of a vibrant civil society. The right to privacy in the digital age is now of the most concerning issues that needs to be tackled. This statistic shows the number of social media users worldwide from 2010 to 2016 with projections until 2021. In 2019, it is estimated that there will be around 2.77 billion social media users around the globe, up from 2.46 billion in 2017. All the information shared by these users need to be protected and should users should have the right and capability of knowing how to control their information sharing and their rights in this era.

Definition of Key Terms

Privacy: is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively.

Information Privacy: Information privacy is the privacy of personal information and usually relates to personal data stored on computer systems.
The need to maintain information privacy is applicable to collected personal information, such as medical records, financial data, criminal records, political records, business related information or website data.

Security: The state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

Digital Age: Time frame in history that the use of digital technology became prevalent and of common use throughout the world. The digital age began in earnest with the widespread use of the Internet.

Surveillance: Network surveillance is the monitoring of computer activity in a network. It is usually done covertly by organizations, governments or individuals to monitor illegal activities. A network engineer/operator, network equipment manufacturer or service provider should have the means to do surveillance tasks related to networking. Network surveillance helps governments and organizations in understanding their user base and gathering intelligence. However, at times it is perceived as a threat to network users as an invasion of privacy.

Data Interception and theft : Data theft is the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. Data theft is increasingly a problem for individual computer users, as well as big corporate firms.

Information sharing: Information sharing describes the exchange of data between between various organisations, people and technologies.

General Overview

The internet :

The access to internet is increasing for any use around the globe. From social media, academic reasons to doing business and much more. The world is now connected and able to communicate through the internet and therefore it is becoming a necessity for everyone to have it. However, with all its advantages, there are some disadvantages that can threaten the right to privacy. Privacy in the virtual world has become a significant issue as it cannot be solved as easily as privacy in the non-virtual world. The right to privacy and to the protection of personal data is a fundamental right enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human rights and the European Union Charter on Fundamental Rights. It follows that respecting the rule of law necessarily implies that this right is afforded the highest possible level of protection.

Protection of the Law

Paragraph 2 of article 17 of the International Covenant on Civil and Political Rights explicitly states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This implies that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State's own constitutional regime and international human rights law.[1] "Accessibility" requires not only that the law is published, but that it is sufficiently precise to enable the affected person to regulate his or her conduct, with foresight of the consequences that a given action may entail. The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.

Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary or unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".[1] In other words, interference that is permissible under national law may nonetheless be "unlawful" if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights. The expression "arbitrary interference" can also extend to interference provided for under the law.

Surveillance and intelligent agencies:

Since the summer of 2013, several international media outlets have reported widely on surveillance activities from intelligence services, both in the United States and in the European Union based on documents primarily provided by Edward Snowden. The revelations have sparked an international debate on the consequences of such large-scale surveillance for citizens' privacy. The way intelligence services make use of data on our dayto-day communications as well as the content of those communications underlines the need to set limits to the scale of surveillance. The Snowden revelations have been a hard wake-up call for many. Never before the existence of so many different surveillance programmes run by intelligence services and able to collect data about virtually everyone, had been disclosed. Some cases have emerged before, but now for the first time extensive evidence about their pervasiveness has been brought into the debate. Surveillance, by its very nature, impacts on personal privacy. Sharing surveillance intelligence with other governments greatly exacerbates the interference with personal privacy. It might not just be your own government that holds sensitive information about you, but potentially many other governments all over the world.
For this reason, intelligence sharing should be subject to safeguards that are already well-established in international human rights law. Without proper safeguards, states can use intelligence sharing as a way of outsourcing surveillance to each other, bypassing any constraints and limits on their own intelligence gathering . Unregulated intelligence sharing can also contribute to or facilitate serious human rights abuses, such as unlawful arrest or detention, or torture and other cruel, inhuman or degrading treatment.

Major Parties Involved

Internet society:

The Internet Society was founded in 1992 by a number of people involved with the Internet Engineering Task Force (IETF). One of their principal rationales is to provide an organizational home for and financial support for the Internet standards process.The Internet Society calls upon the global community to work together to confine the ambit of data collection for national security purposes to those truly exceptional instances where the public interest objectively outweighs an individual's right to privacy. And also to agree a set of strong principles for ethical data handling. One of their initiatives are the disclosures concerning the nature and extent of government surveillance of Internet users' communications and data drew the world's attention to a new threat model: pervasive surveillance and interception of private communications. The IETF and W3C have responded with initiatives to develop standards that strengthen the Internet against this type of threat.

Council of Europe:

The Council of Europe has always been an active party involving the resolutions and debates at the United Nations about the right to privacy in the digital age. They have submitted different reports and requests to the United Nations outlining and explaining the importance of the human right to privacy and also the concerns that are brought with the advance in technology. Specially with efforts to keep terrorism at bay if the terrorist threat were substituted with a perceived threat of unfettered executive power intruding into citizens' private lives. It is of the utmost importance that the domestic legislation authorizing far-reaching surveillance techniques and prerogatives provides for adequate and sufficient safeguards in order to minimize the risks for the freedom of expression and the right to privacy which the "indiscriminate capturing of vast amounts of communications" enables. The standards related to targeted surveillance identified in the case-law of the Court have therefore to be adapted to apply to strategic surveillance.

Amnesty International:

Amnesty international has submitted an article to the the International Covenant on Civil and Political Rights that implies extraterritorial obligations to respect and ensure protected rights and that both the obligations to ensure and respect are to be exercised extraterritorially subject to the "power or effective control over the essence of the right," and therefore, in the context of surveillance of an individual's communications, this refers to effective control or power over those communications. This leads to the conclusion that extraterritorial surveillance engages the surveilling state's obligations to respect the rights to privacy guaranteed in the ICCPR.

Timeline of Key Events

Timeline of events in reverse chronological order leading up to present day.

Date	Description of Event
21 November 2016	The Committees of the Ministers of the Council of Europe adopted a declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies. The Declaration stresses that "legislation allowing road surveillance of the citizen can be found contrary to the right to respect of private life."

21 November 2016	New resolution on the right to privacy in the digital age, adopted on 21 November 2016 at the UN General Assembly.
30 June 2014	The United Nations High Commissioner for Human Rights submitted a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States.
24 February 2014	The High Commissioner delivered a keynote presentation at an expert seminar on “The right to privacy in the digital age”, which was co-sponsored by Austria, Brazil, Germany, Liechtenstein, Mexico, Norway and Switzerland, and facilitated by the Geneva Academy on International Humanitarian Law and Human Rights.
5 June 2013	Snowden leaked around 10,000 classified documents by using the Guardian on 5 June 2013. These were documents such as top-secret documents regarding NSA domestic Surveillance and practices and information on other government surveillance programmes.

Previous Attempts to Resolve the Issue

New resolution on the right to privacy in the digital age, adopted on 21 November 2016 at the UN General Assembly, comes at a time when the rapid pace of technological development is enhancing the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy. They want to provide the technology to the public that can exercise the human rights.

Possible Solutions

With the increase of technological knowledge, surveillance and interference is becoming easier and more worrying. Effectively addressing the challenges related to the right to privacy in the context of modern communications technology will require an ongoing, concerted multi-stakeholder engagement. This process should include a dialogue involving

all interested stakeholders, including Member States, civil society, scientific and technical communities, the business sector, academics and human rights experts. As communication technologies continue to evolve, leadership will be critical to ensuring that these technologies are used to deliver on their potential towards the improved enjoyment of the human rights enshrined in the international legal framework.

Bibliography

- “Committee of Ministers: Selection and Most Recent Adopted Texts.” *Council Of Europe*, www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/C10Tb8ZfKDoJ/content/declaration-of-the-committee-of-ministers-on-risks-to-fundamental-rights-stemming-from-digital-tracking-and-other-surveillance-technologies-adopted-by?inheritRedirect=false.

- “Data Theft Definition.” *Cybercrime.org.za*, cybercrime.org.za/data-theft/.

- High Stakes: UN Enters Late-Stage Negotiations for Recognition of Right to Privacy in Digital Age.” *Privacy International* , 6 Feb. 2018, privacyinternational.org/blog/1173/high-stakes-un-enters-late-stage-negotiations-recognition-right-privacy-digital-age.

- “In Quest of Privacy in the Digital Age.” *The New York Times*, 18 Oct. 2017, www.nytimes.com/2017/10/18/opinion/privacy-internet.html.

- “OHCHR | Right to Privacy in the Digital Age.” *OHCHR* | *Freedom of Religion: UN Expert Hails Albania, but Notes New Challenges and Unresolved Issues from the Past*, www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx.

- “OHCHR | Report on the Right to Privacy in the Digital Age.” *OHCHR* , www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

- “Right to Privacy in the Digital Age : Call for Inputs.” *Business & Human Rights Resource Centre*, 30 Mar. 2018, www.business-humanrights.org/en/right-to-privacy-in-the-digital-age-call-for-inputs

- The Right to Privacy in the Digital Age.” *About IFLA Membership Activities and Groups Supporters News and Events Publications Standards Annual Conference Global Vision The International Federation of Library Associations and Institutions* , www.ifla.org/files/assets/faife/ochr_privacy_ifla.pdf.