Forum: The Economic and Social Council

Issue: The Right to Privacy in the Digital Era

Student Officer: Mr. Martin Kononov

Position: President

Introduction

As the prices of personal digital technologies continue come down year-over-year, these devices begin to increasingly present themselves in our daily lives. The question of privacy—or lack thereof—begins to take shape and become a major concern for such developments. The number of Internet users has increased four-fold in the 15 years since 2000, from 738 million to over 3.2 billion.[1] Internet usage have gone up from 7% to 43% of the world's population. Although Article 17 of the International Covenant on Civil and Political Rights (ICCPR), signed in 1976, ensures everyone's protection from random or unlawful intrusions into their "privacy, family, home or correspondence,"[2] the continued evolution of digital technologies has prompted the "United Nations Human Rights Committee to assist in this process."[3] This new wave of adoption brings with it massive responsibility on the side of governments to take action to protect privacy of individuals utilizing these services.

Technological advancements have not only made it easier to use modern information and communications technologies (ICTs), but have also increased the ability for entities, such as companies, governments, or even individuals, to partake in many data collection processes.[4] Nevertheless, these may constitute violations of human rights, and the right to privacy.[5] As this continues, more and more such data is collected, potentially for future sharing or processing.[6] Many times, this all happens without explicit and informed consent of individuals and usually take aid at often vulnerable communities, notably women and children.[7] The way that governments deal with these developments, and more particularly

---

[1] Jacob Davidson, "Here's How Many Internet Users There Are," *Time Magazine*, last modified May 26, 2015, http://time.com/money/3896219/internet-users-worldwide/.
[2] "The Human Right to Privacy in the Digital Age," *American Civil Liberties Union,* last modified 2015, https://www.aclu.org/other/human-right-privacy-digital-age.
[3] Ibid.
[4] Deborah Brown, "New UN resolution on the right to privacy in the digital age: crucial and timely," *Internet Policy Review*, last modified November 22, 2016, https://policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436.
[5] Ibid.
[6] Ibid.
[7] Ibid.

the private sector which is generally responsible for it, will shape the evolution of many future technologies.

In general, the rapid growth and expansion of technologies which ease communication and data-sharing has improved democratization by giving voices to those who previously did not have, but has also allowed for more infiltration of digital information through covert operations.[8] Protecting human rights, as they pertain to digital privacy does not only have an impact on society, but also on economic prosperity of industries which heavily rely on the use of these technologies.

Definition of Key Terms

Anti-discrimination Laws

Laws which govern the fair and equal treatment of all individuals.[9]

Authentication

The process which an entity shows that something is valid or confirmed.[10]

Authorization

When referring to digital privacy, authorization refers to the process by which the end user allows for the use of certain information.[11]

Biometrics

Usually recorded measurements of unique physical or behavioral characteristics of individuals.[12]

Common Law

Principles referring to laws which are not written, but accepted as expectations under social customs.[13]

Confidentiality

---

[8] "The Right to Privacy in the Digital Age," *The United Nations Human Rights Office of the High Commissioner*, last modified 2017, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.
[9] IAPP, "Glossary of Privacy Terms," *International Association of Privacy Professionals*, last modified 2012, https://iapp.org/media/pdf/resource_center/IAPP_Privacy_Certification_Glossary_v2.0.0.2.pdf.
[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Ibid.

Obligations by entities to protect certain information, and by such prevent from misuse and disclosure, of individuals, corporations, or even governments.[14]

Consent

A legal requirement regarding the agreement or disagreement of the use of their personal information by other entities with full prior disclosure of all information pertaining to digital privacy.[15]

Encryption

A process by which information is placed under high digital security measures, usually requiring special knowledge, such as a code, to read.[16]

Information Privacy

One of the four types of privacy concerning individuals, along with bodily privacy, communications privacy, and territorial privacy. Information privacy refers to the personal choice by entities to how their information will be shared to others.[17]

Outsourcing

The contracting of third-parties for certain business processes. An example for outsourcing is the collection of privacy information by advertising agencies through website such, but not limited to, Facebook and Twitter.[18]

Background

A main part of economic growth in many More Economically Developed Countries (MEDCs) for the past 25 years was and is backed by the growth of digital consumer technology companies, the majority of which are in the private sector, while growth in Less Economically Developed Countries (LEDCs) has been created through the implementation of these same technologies. The growth of Internet availability, alone, on the entire African continent from 2000 to 2017 was a staggering 8,503%[19]. Now, more than ever, this industry is crucial to future economic prosperity. However, as information communications technologies (ICTs) have expanded into the hands of many individuals and industries,

---

[14] Ibid.
[15] Ibid.
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] "African Internet Usage, 2017 Population Stats and Facebook Subscribers," *Miniwatts Marketing Group*, last modified November 12, 2017, http://www.internetworldstats.com/stats1.htm.

the exploitation of flaws for abusing basic privacy considerations has been an incredible concern for individuals, corporations, or even entire countries and governments.

Privacy of Individuals and Corporations

The biggest, and most obvious, concern regarding privacy in the digital age is the privacy of information of individuals and corporations. Consumers, or private citizens, are generally concerned with the privacy of their personal information and identity and how it's shared throughout the Internet; while corporations mostly want to prevent the release of classified information which may harm or compromise their business and the ability to make profit. Furthermore, although many technologies are allowing people to enjoy greater freedom and mobility, they also make it even easier to track whereabouts, financial information, and identities, as a result, violating personal privacy laws and common law.

Data Breaches

The exponential influx of digital data available has also seen the rapid increase in breaches of security measures used to protect them. Figure 1 of Appendix B depicts a general trend regarding the growing number of data breaches over time. As people's tendency to continue to use technology for increasingly many aspects of their lives becomes more prevalent, security breaches would start to become a more commercialized industry both from the point-of-view of hackers trying to steal and distribute information and security firms which try to mitigate or reduce the impacts.

Security

Security concerns usually encourage governments to set up national surveillance systems, encroaching on privacy of ordinary citizens. The phrase 'if you've got nothing to hide, you have nothing to worry about,'[20] has become a very common defense for many such operations. Although this may be applied to a few cases, such an argument is statistically shown to be mostly flawed due wide-ranging issues concerning privacy problems and the usual risks associated with mass data collect schemes, most of which extend far beyond simply surveillance and disclosure.[21]

Transparency

The lack of transparency is another key facet of the issue regarding personal digital privacy. Although there is no definite international consensus on the meaning of transparency, it is generally considered to be the ability for the general public to have access to information about the regulations,

[20] Yves LeRoux, "Privacy concerns in the digital world," *Computer Weekly*, last modified October 2013, http://www.computerweekly.com/opinion/Privacy-concerns-in-the-digital-world.
[21] Ibid.

decisions, and actions of governments and organizations.[22] In the context of digital privacy, there are generally two takes on transparency: personal transparency and the transparency of organizations which possess personal informational of others.[23] Personal transparency is the creation of a digital presence through the social mediums, which help generate more trust and effectiveness.[24] However, transparency of organizations may be more important. Information held by large bodies may pose a conflict between transparency and privacy due to the ability to access personal information, and thus potentially violate personal privacy.[25] It is crucial to consider how transparency plays a role is affecting multiple aspects of privacy.

Key member states and NGOs

United States

While it is generally considered common practice and in the interest of national security, many governments around the world are involved in the interception of private communication among its citizens or residents. In 2013, Edward Snowden, a former US National Security Agency contractor leaked thousands of documents regarding the NSA's operations; drawing international attention, this re-ignited the relevance of the question: what, if any, private information should governments be allowed to collect.[26] The government of the United States has been known to be collecting records of basic forms of communication, such as phone calls and Internet communications, since at least 2001.[27] Furthermore, many whistleblowers have revealed that major telecommunication companies have been coping with the illegal surveillance activities.[28] Nevertheless, in 2006, the US government confirmed that such activities were truly taking place under the Patriot Act[29], a bill passed by President George Bush, following the September 2001 attacks, which provided legal framework for collect data in order to prevent major terror plots in the future.[30]

Privacy International

---

[22] Joseph A. Cannatacci et al, "Privacy, free expression, and transparency – Redefining their new boundaries in the digital age," *UNESCO*, last modified 2016, http://unesdoc.unesco.org/images/0024/002466/246610E.pdf.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] "Edward Snowden: Leaks that exposed US spy programme,"*BBC*, last modified January 17, 2014, http://www.bbc.com/news/world-us-canada-23123964.
[27] "NSA Spying," *Electronic Frontier Foundation*, https://www.eff.org/nsa-spying.
[28] Ibid.
[29] Ibid.
[30] "What is the USA PATRIOT Web," *Department of Justice*, https://www.justice.gov/archive/ll/highlights.htm.

Privacy International is a London based Non-Governmental Organization (NGO) which was founded in 1990.[31] The organization works with a few European Union (EU) and United Nations (UN) agencies with the goal of helping mitigate infringements on personal privacy through examining the actions of governments and surveillance technologies.[32] Campaigns director Harmit Kambo stated that "There's a whole industrial complex around surveillance in the private sector…As the issues continued to evolve and mutate, one thing remain – technology is providing more and more means to undermine our privacy. That's something we rail against. We think personal privacy has been a very under-recognised human right. Until Privacy International arrived, and has worked hard to put privacy on the agenda, it wasn't a human right that was given much consideration or credence."[33]

Open Rights Group

The Open Rights Group is another UK based NGO which focuses on the actions that governments, particularly that of the UK, regarding their collection and distribution of personal information.[34] The group embodies a legitimate campaign to help governments [better] understand [privacy issues facing individuals]"[35]. The organization is mainly funded by individuals who pay a subscription fee.[36]

Timeline of Events

Date	Description of event
2014	EU Court approves the right to be forgotten.[37]
2013	Edward Snowden reveals NSA surveillance operations.[38]
2000	Web bugs are introduced.[39]
1995	Spyware starts to become common and is transmitted through the Internet.[40]
1994	HTTPS introduced to help secure web traffic.[41]

[31] Tamlin Magee, "The UK NGOs fighting for digital rights, data, and privacy," *TechWorld*, last modified Feburary 3, 2016, https://www.techworld.com/security/uk-ngos-digital-rights-data-privacy-3634432/.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] Ibid.
[36] Ibid.
[37] Calvin Pappas, "A Brief History of Digital Privacy," *AVG Now*, last modified August 8, 2014, https://now.avg.com/history-digital-privacy/.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] Ibid.

1990	Identity theft starts to become common.[42]
1980	DNA fingerprinting starts to become common.[43]
1976	Public-key encryption created to prevent the stealing of personal and business information.[44]
1928	US Supreme Court rules that seizures of electronic communications systems is constitutional.[45]
1890	Fingerprints are first used to identify people; "The right to be let alone" introduced.[46]

UN Involvement, Relevant Resolutions, Treaties, and Events

- The right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014 **(A/HRC/27/37)**
- Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms – The right to privacy in the digital age, 16 November 2016 **(A/C.8/71/L.39/Rev.1)**
- The right to privacy in the digital age, 21 January 2014 **(A/RES/68/167)**
- International Conference of Data Protection and Privacy Commissioners – Resolution: Privacy in the digital age (Appendix A)
- Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms – The right to privacy in the digital age, 22 March 2017 **(A/HRC/34/L.7/Rev.1)**

[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.

Possible Solutions

Due to the nature of digital devices, the implementation of privacy standards concerning them have far reaching implications.

One solution to improving general privacy is to introduce strict regulations on the exact type of data that large technological corporations would be mandated to follow. However, since many such companies rely heavily on consumer's personal data through its sale to advertising agencies, a crack-down on the type of data and its uses would be hard to execute. Nevertheless, such programs could potentially grant subsidies to minimize the loss of revenues, seeing that the majority of these corporations are headquartered in MEDCs.

Another solution to this growing issue is to provided clearer and more simplified disclosures to users when using a service which would be undermining their privacy. While being maximally informed of the privacy risks, Carnegie Mellon University conducted research to find out whether that would be practical. It is estimated that it would take the average individual living in an MEDC over 76 work days to read all the privacy policies they absent-mindedly agree to, on a daily basis.[47] Helping consumers better understand the privacy risks involved would help them make better decisions, while potentially staying more economically productive.

Yet another solution that governments should potentially focus on is the sale and use of personal information. Although it is common that many governments collect personal data on their citizens for the purposes of national security and development, there may be only limited ways to encourage countries to reduce or end this practice altogether. Nevertheless, the focus can shift, rather, to large corporations and their use and distribution of private information. Enforcing stricter regulations and audits on the ways that large corporations may use the personal information of their customers and outsource it to advertisement agencies. This may initially have a negative side-effect on the profitability and economic output of these corporations, but the long-term departure from an information-selling business model of companies would help attract more customers, and thus increases revenue streams.

Finally, in the effort to improve personal privacy of the younger generation, international consensus on the legal age at which children would be able to use public social-media websites. The usage of Twitter by teenagers who have access to the internet, alone, has increased to 24% in 2016 from 16% in 2011.[48] A similar trend has been reported in crime rates related to teenager abuse online. It

---

[47] Alexis C. Madrigal, "Right the Privacy Policies You Encounter in a Year Would Take 76 Work Days," *The Atlantic*, last modified March 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[48] Mary Madden et al, "Teens, Social Media, and Privacy," *Pew Research Center*, last modified May 21, 2013, http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

is evident that a larger, younger online presence leads to a greater risk of harm. Therefore, nations should reconsider at what age it would be legally appropriate to broadcast private information online.

Bibliography

"African Internet Usage, 2017 Population Stats and Facebook Subscribers." *Miniwatts Marketing Group*. Last modified November 12, 2017. http://www.internetworldstats.com/stats1.htm.

Brown, Deborah. "New UN resolution on the right to privacy in the digital age: crucial and timely." *Internet Policy Review*. Last modified November 22, 2016. https://policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436.

Cannatacci, Joseph A. et al. "Privacy, free expression, and transparency – Redefining their new boundaries in the digital age." *UNESCO*. Last modified 2016. http://unesdoc.unesco.org/images/0024/002466/246610E.pdf.

Davidson, Jacob. "Here's How Many Internet Users There Are." *Time Magazine*. Last modified May 26, 2015. http://time.com/money/3896219/internet-users-worldwide/.

"Edward Snowden: Leaks that exposed US spy programme."*BBC*. Last modified January 17, 2014. http://www.bbc.com/news/world-us-canada-23123964.

IAPP. "Glossary of Privacy Terms." *International Association of Privacy Professionals*. Last modified 2012. https://iapp.org/media/pdf/resource_center/IAPP_Privacy_Certification_Glossary_v2.0.0.2.pdf.

LeRoux, Yves. "Privacy concerns in the digital world." *Computer Weekly*, last modified October 2013, http://www.computerweekly.com/opinion/Privacy-concerns-in-the-digital-world.

Madden, Mary et al. "Teens, Social Media, and Privacy." *Pew Research Center*, last modified May 21, 2013, http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

Madrigal, Alexis C.. "Right the Privacy Policies You Encounter in a Year Would Take 76 Work Days." *The Atlantic*. Last modified March 1, 2012. https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

Magee, Tamlin. "The UK NGOs fighting for digital rights, data, and privacy." *TechWorld*. Last modified Feburary 3, 2016. https://www.techworld.com/security/uk-ngos-digital-rights-data-privacy-3634432/.

"NSA Spying." *Electronic Frontier Foundation*. https://www.eff.org/nsa-spying.

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

"The Human Right to Privacy in the Digital Age," *American Civil Liberties Union,* last modified 2015, https://www.aclu.org/other/human-right-privacy-digital-age.

"The Right to Privacy in the Digital Age." *The United Nations Human Rights Office of the High Commissioner*. Last modified 2017. http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

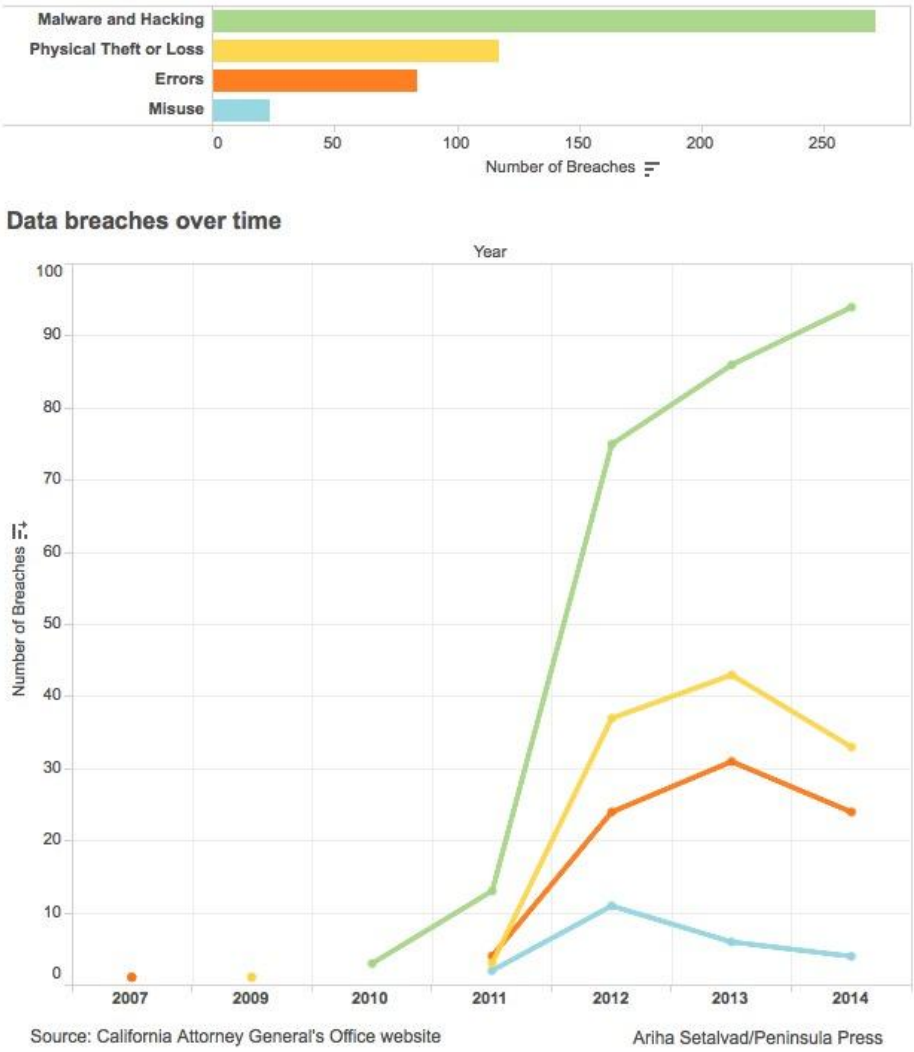
"What is the USA PATRIOT Web." *Department of Justice*. https://www.justice.gov/archive/ll/highlights.htm.

Appendices

A. https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Den_internationale_konference/Resolution-Privacy-in-the-digital-age.pdf

B.

Figure 1: The upward trend in data breaches over time reinforces the concern over personal digital privacy.



Source: http://peninsulapress.com/data-viz-data-breaches-by-type-and-over-time/.