United Nations Commission on Science and Technology for Development

Background Guide

The Right to Privacy in a Digital Age

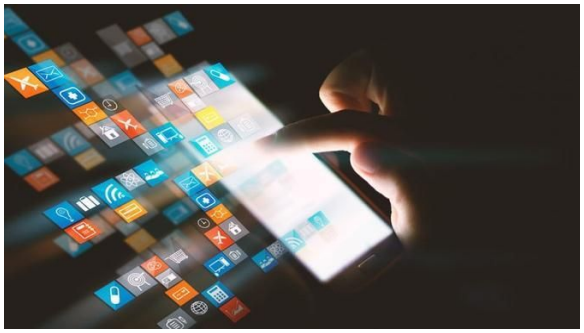
Lincoln Model United Nations

April 6 – 7, 2019

Table of Contents

Introduction to the Topic

Advances in technology have drastically improved real-time communication and information-sharing. These technological renovations have developed society in numerous ways. But, it has also become a matter of concern. Society has become defenseless and exposed to interception and electronic surveillance. New revelations are constantly emerging, creating new technologies to simplify and speed these methods of surveillance already in place effortlessly. These types of surveillance abuse individual rights, such as the right of freedom of expression, privacy and association, and obstructing the behaviors of a civil society.



History of the Committee

The General Assembly's 46/235 resolution created the United Nations Commission on Science and Technology. This commission consists of 43 members and falls under the 2003/37 resolution of the Economic and Social Council. This commission replaced the Intergovernmental Committee on Science and Technology for Development and its Advisory Committee (1979), and had its first meeting in April 1993 in New York City. Ever since July

1933, the officiator for the commission has been the United Nations Conference on Trade and Development Secretariat. The commission meets in at the Palais des Nations in Geneva, Switzerland, with the scientist Atta ur Rahman as the chairman.

This commission was mainly founded to offer the Economic and Social Council and the General Assembly with advice through policy recommendations and analysis on specific issues related to technology.

Current Situation

In December 2013, a resolution adopted by the UN conveyed their worry towards the negative impacts that monitoring and interception have on human rights. They declared that humans should have the same rights online and offline. They requested the states to revise their actions and habits towards this issue.

Today the resolution 68/167 conveys that “no one shall be subjected to arbitrary or unlawful interference with his or her privacy, nor unlawful attacks.” (OHCHR, UN) It also states that “everyone has the right to the protection of the law against such interference or attacks.” (OHCHR, UN) However, the right of privacy under international law is not thorough, and leaves a breach for attacks on privacy in the digital era, leaving every user vulnerable to certain attacks. As of today, the only actions taken under these attacks "must be subject to a careful and critical assessment of its necessity, legitimacy, and proportionality.” (OHCHR, UN)

Topics

1. **Right to Privacy Legislation**

   With an increasing use of technology in the digital era, and with that, a quicker rate at which entities can access information, countries and organizations around the world have updated their privacy laws. However, legislations struggle to keep up with constant advancements in technology, which allows for constant dodging of privacy laws and infiltration of information. Privacy laws are different around the world, and they all set different standards for minimum age for online presence, interpretations of user consent, government surveillance, penalties if

the law is broken, etc. Delegates must take into consideration the laws that have been passed in their own countries in order to properly represent the delegation and come to agreement in finding the solution.

1. **Government Surveillance**

Throughout the digital age, the internet and the information technologies have been a tool to government and security organizations such as the NSA and CIA to investigate suspects and criminals. It is a debatable issue whether governments around the world should have access to private calls of their residents and citizens, as well as access to their private information and correspondence. For instance, President George Bush passed the Patriot Act following the 9/11 attacks in 2001, which allowed the government to collect data to prevent future terrorist attacks. Furthermore, in 2013, computer professional Edward Snowden exposed the millions of email and SMS correspondence, as well as locations and cookies used and gathered by the National Security Organization, which earned international attention. Additionally, the public discovered the NSA used PRISM, a program for data collection, which was not only employed in the U.S, but in the Bahamas as well, without consent or knowledge from the government. This expanded originally national privacy issues in the US to an international problem.

1. **Censorship**

The lack of trust citizens have towards the government regarding privacy also reflects on the lacking of true freedom of expression. It is common for national governments to block a moderate amount of Internet sites. However, severe censorship is present in governments who block news casts, and even specific personal users for political, social, or religious motives. Originally begun in Tunisia, for instance, the Arab Spring in 2010 consisted of censoring multiple media sites in prevention of riots of

protests, since the government believed people were communicating online. Since then, the UK and Egypt, for instance, experienced censorship of Twitter in 2011, in response to protests and riots. More gravely, China's *Public Pledge on Self-Discipline for the Chinese Internet* not only allows the government to block social media sites such as Facebook and Twitter, but it gives officials the right to monitor individual user activity. They, in this way, limit their citizen's freedom of expression, since those spreading anti-regimen comments or ideologies, either privately or publicly, are punished through fines and can even face incarceration. "Amnesty International has stated that China "has the largest recorded number of imprisoned journalists and cyber-dissidents in the world"", stripping its citizens of digital privacy and knowledge of international events.

Block Positions

European Union: Europe implemented the GDPR which is an update to the 1995 Data Protection Directive. It provides Europeans with tools that allow them to control the data that is being collected about them. The law claims that anywhere around the world EU citizens must receive the option to view the information that is being collected about them. Penalties have also been initiated for violating this GDPR including 4% of the firm's revenue or a $23.5 million fine, this depends on which one is larger.

United States: All through America the digital privacy laws are not strict enough. The US congress has been discussing the "Social Media Privacy Protection and Consumer Rights Act of 2018". This proposal mimics in several

ways the GDPR, however it has not been voted into law. The act requires websites to provide users with all the data the firm has about them, and a detailed list of who had access to this data and how it was used. This act was proposed after Facebook's CEO Mark Zuckerberg's testimony to Capitol Hill.

The US as of now relies on each tech company to monitor themselves and consider regulations once data's are breached.

China: According to China data privacy belongs to the government. They believe it is the government's duty to stop users personal data from being used. China's approach to this issue might be considered one of the strictest approaches. Opposed to the GDPR, China's law states that personal data can't even be shared with third-parties without users consent.

Even though they try and maintain a highly secure digital privacy, China is willing to breach personal information when it comes to providing data for artificial intelligence algorithms, yet it has been moving towards the European model lately.

Russia: Russia has been more inclined towards breaching digital privacy due to their state surveillance. Ever since the 1990s their SORM monitoring system has been attacking servers and phones which allows the government to supervise everything Russians do online. Russian digital privacy laws allows individuals to protect their personal data, but leaves wiggle room for the government to oversee any information they consider necessary.

Possible Solutions

The General Assembly affirmed in December 2013 "that the rights held by people offline must also be protected online, calling upon all States to respect and protect the right to privacy in digital communication. The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law". Although all

nations must take their own cultural background and history into account when regulating right to privacy, an effective international legislation, with coherent repercussions for those who break the standards set by the committee, is essential to maintain order.

A research study conducted at Carnegie Mellon University found that it would take the average resident of an MEDC (More Economically Developed Country) over 76 work days to read all the privacy terms and conditions they agree to on a daily basis. “Helping consumers better understand the privacy risks involved would help them make better decisions, while potentially staying more economically productive”. Therefore, Internet users would benefit from simplified disclosure of privacy policies, and a consensus on minimum age for usage of social media.

Points Resolution Should Address

- Should humans have the same rights and legal standards online as they do offline?
- What changes should be made to laws in order to adequately prevent privacy violations in a technological environment?
- To what extent should governments have the right to breach privacy online?
- When does online monitoring become a privacy violation rather than a safety measure?
- How can the United Nations ensure privacy rights are protected?

Conclusion

In a globalized world, where approximately half of the world has access to the internet, information is easily spread, as well as privacy can be rapidly lost. The

right of privacy is one of the most pressing issues in the XXI, as technology advances more rapidly than ever, leaving national and international legislation behind. Even though technology in the digital age has allowed people to enjoy more effective communication, revolutionized careers, and given people easily obtainable information, it has made the tracking of financial information, identities, and locations equally as easy, ultimately resulting in the invasion of privacy. The lack of transparency of corporations, organizations, and governmental entities also poses an issue regarding privacy; when citizens do not have the knowledge of who can access their profiles, web searches, or media interactions, they cannot protect themselves and are unconsciously defenseless against powerful bodies that invade personal information. Therefore, it is crucial that this committee can find an innovative, timeless solution to this international issue, that affects the world equally.

Works Cited

Brumis, Alissa M. "The Right to Privacy in a Digital Age: Reinterpreting the Concept of Personal Privacy." *Inquiries Journal*, 2016, www.inquiriesjournal.com/amp/1450/the-right-to-privacy-in-a-digital-age-reinterpreting-the-concept-of-personal-privacy.

Hartzog, Woodrow. (2013). "Privacy and Terms of Use." In D.R. Stewart (Ed.), *Social Media and the Law.*

Nyst, Carky, and Tomaso Falchetta. "The Right to Privacy in the Digital Age." *Journal of Human Rights Practice*, Oxford Academic, 1 Feb. 2017, https://academic.oup.com/jhrp/article-abstract/9/1/104/2965689?redirectedFrom=fulltext.

"OHCHR | Right to Privacy in the Digital Age." *OHCHR | Convention on the Rights of the Child*, www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx.

"Commission on Science and Technology for Development, 16th Session | UNITED NATIONS ECONOMIC and SOCIAL COUNCIL." *United Nations*, United Nations, www.un.org/ecosoc/en/events/2013/commission-science-and-technology-development-16th-session.

"Home." *United Nations*, United Nations, www.un.org/en/index.html.

"The Right to Privacy in the Digital Age: Where Do Things Stand?" *Council on Foreign Relations*, Council on Foreign Relations, www.cfr.org/blog/right-privacy-digital-age-where-do-things-stand.