|  |  |
| --- | --- |
| sismun vi  2019 | The use of artificial inelegence and technology in surveilance |

**The Use of Artificial Intelligence and technology in Surveillance**

**Brief Description of the Committee**

The International Telecommunications Union (ITU) in an agency within the United Nations that is responsible for coordinating the operation of telecommunications and services throughout the world. This branch of the UN consists of three divisions; Radio Communication, Telecommunication Standardization and Telecommunication Development Department. The ITU prioritizes the publishing of regulations and standards pertaining to electronic communication and broadcasting. The decisions made in this committee today will go down as ITU regulation and could affect the world of telecommunication as we know it.

**Statement of the Problem:**

Multiple companies and governments have ventured into the development of technology for use in surveillance. Governments and corporations have both sought to collect information on individuals. Some argue that governments and corporations collect data to ensure national security and prevent crimes from being committed. Proponents of such surveillance would posit that surveillance is a violation of privacy and rights. The presence of the NSA’s PRISM system, China’s facial recognition system, India’s Central Monitoring System (CMS), and many other surveillance programs demonstrates the capability of governments to monitor the population and possibly breach the privacy of their citizens. Such surveillance has been put to scrutiny by many organizations and activists for privacy. Corporations have also developed their own technology that has surveillance built in, such as Google Glass. Google Glass was a pair of eyeglasses that featured a built in computer which let users access the internet and many other applications through voice commands. This device was later on discontinued (2015) in part due to the invasion of the public's privacy through the constant recording through the glasses. These recordings were capturing people's private information such as their credit card numbers without raising any suspicion.

**Historical Context:**

In today’s world, the internet is viewed as a general purpose technology that nearly everyone uses every day. The internet is what connects people around the world and allows for a sense of interconnectivity that was unprecedented beforehand. Prior to the introduction of the internet, ideas and news would spread via train, horseback, press, etc. Nowadays, the internet allows for the rapid transmission of ideas and news, keeping everyone up to date and providing an edge in the economy, education and government. With the induction of the internet as a tool of everyday use came the creation of other tools that were made possible by the internet. The internet was initially cultivated as ARPANET by the Department of Defense in 1969. ARPANET was created for scientific purpose in order to test and trial the new technology. It was never meant to link the world today; nor was it meant for the mass communication that it provided today. [[1]](#footnote-1)ARPANET was made in order for research institutions to connect to other institution’s computers to use the power of them to conduct calculations that were not possible otherwise. Through the development of ARPANET came packet switching, which opened the possibility of mass communication. ARPANET found its way into the military, government and eventually the public. [[2]](#footnote-2)

Governments have proceeded to use this vast array of information to collect said information on its citizens to prevent a national security threat. PRISM was developed by the US’ National Security Agency to listen in on phone calls, read texts and identify people. PRISM was developed to identify threats to the US.[[3]](#footnote-3) The NSA has also collaborated with various other nations to help them set up their own network of information collecting.

**Past UN Action:**

Two years after the Snowden revelations, the Human Rights Council resolution 28/16 was passed pertaining to the right to privacy in our digital age. Programs like PRISM and CSM were ruled as programs that could pose a risk to the privacy of citizens. Resolution 28/16 proposed the establishment of a Special Rapporteur on the right to privacy. It also reaffirmed that everyone is entitled to their right to privacy and that no arbitrary/unjust impositions upon their personal life and information be seized and stored. This resolution is very special because it addresses the broad spectrum of surveillance, and acknowledges the fact that technology such as artificial intelligence further enables the capability of a government to infringe upon their citizen’s privacy in the name of national security. The Special Rapporteur is tasked with gathering information on possible cases of infringement on privacy, obstacles to the right to privacy and identify possible violations of such right. The first Special Rapporteur on the right to privacy, Joseph Cannataci, has said that digital surveillance is “worse than Orwell” (reference to 1984’s Big Brother).[[4]](#footnote-4)

In 2007 Dr.Hamadoun I. Toure from ITU launched the Global Cybersecurity Agenda (GCA). This served as a framework aimed to come to agreement on set goals in the fight against cybercrime. The GCA has five different pillars to it: legal measures, technical and procedural measures, organizational strategies capacity building and international cooperation.

**Questions to Consider:**

* What is the balance between national security and the public’s right to privacy?
* Are governmental policies being kept up to date with the innovation of new technology?
* Should artificial intelligence be further introduced into surveillance?
* Have the decisions and agreements of past UN conventions pertaining to technological privacy been enforced properly?

**Helpful Links:**

[**https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/**](https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/)

[**https://www.hrw.org/news/2019/09/18/us-government-mass-surveillance-isnt-secret**](https://www.hrw.org/news/2019/09/18/us-government-mass-surveillance-isnt-secret)

[**https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data**](https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data)

[**https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx**](https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx)

[**https://www.theguardian.com/world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief**](https://www.theguardian.com/world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief)

**Roles:**

1. United States
2. China
3. France
4. UK
5. Belgium
6. Brazil
7. Russia
8. Iran
9. Syria
10. Saudi Arabia
11. Sweden
12. Czech Republic
13. Argentina
14. Japan
15. Estonia
16. Sweden
17. Senegal
18. Norway
19. Bahrain
20. Malaysia
21. Hong Kong
22. India
23. Germany
24. Philippines
25. Mexico
26. Congo
27. North Korea
28. South Africa

1. “What is ARPANET” Searchnetworking.com <https://searchnetworking.techtarget.com/definition/ARPANET> [↑](#footnote-ref-1)
2. “Brief History of the Internet” Internet Society <https://www.internetsociety.org/internet/history-internet/brief-history-internet/> [↑](#footnote-ref-2)
3. “Everything we know about PRISM to date” Washington Post <https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/> [↑](#footnote-ref-3)
4. “Digital Privacy ‘Worse Than Orwell,’ says new UN privacy chief” The Guardian <https://www.theguardian.com/world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief> [↑](#footnote-ref-4)