Topic 2: Digital Identity and Surveillance: Empowering Citizens or Enabling Authoritarianism

Group of 20

I. Introduction

Living in the technological era, there is a digital identity for anyone who uses the internet. The advantages for a digital world are clear – expansive connectivity, faster communication and access to more information than ever. However, the risks also increase. Cybercrime and large criminal organisations use the online space as an easier way to plan and carry out digital and physical attacks.

Digital policing, therefore, has become an efficient way of detecting crime and preventing it. Spotting suspicious patterns and questionable interactions can be a good indicator of possible threats. However, that brings into question the possible infringement of personal freedoms, and creates spaces of self-censorship and paranoia, due to fears of being flagged. The conflict between digital safety and digital freedom is of growing importance.

II. Key Terms

Digital Identity: The online presence of an individual, including their own actions as well as actions done towards them. In this case more specifically, the pinpointing of real life individuals through their online activities.

Mass surveillance: The analysis and evaluation of data across the whole of an online or offline space. Often violating personal privacy, mass surveillance monitors and interferes when it deems necessary every interaction in that space.

Cybercrime: The group of crimes classified by the usage of an electronic device to carry out illegal activities, like identity fraud and the infringement of personal privacy.
Self-censorship: Linked to social paranoia, the limiting of one's self expression in fear of being targeted by authorities, for example, the governmen*t*.

III. Past International Actions

Since 2013, the United Nations has regularly adopted General Assembly resolutions reaffirming the right to privacy within the context of growing digital surveillance. For example, Resolution A/RES/73/179 (2018) encouraged states to review surveillance policies and ensure people are protected against unlawful data collection. More recent UN actions emphasize the importance of privacy within digital communications and also recognize the critical role of encryption, anonymity, and protection against risks associated with artificial intelligence and biometric technologies. The 2022 report from the Office of the High Commissioner for Human Rights (OHCHR) further highlighted the importance of encryption and the increased threats to privacy in the digital era.

Efforts to regulate digital identity systems have advanced. The Council of Europe published guidelines in 2022, urging that digital identity schemes comply with international human rights standards, with particular regard to privacy and data protection. Meanwhile, updates to the European Union's Digital Identity Framework adopted in 2024 have established technical and legal safeguards for cross-border digital identification and mandated that user privacy be at the center of design.

Convention on cybercrime - Budapest Convention
Signed by 50 countries, the Budapest Convention is the biggest international cooperation treaty addressing the rise of cybercrime. Its main aims are to share information on patterns prevalent in cybercrime scenes, aid each other in identifying and addressing threats, all the while procuring a lawful and ethical approach.

IV. Timeline of Key Events

1995	European Data Protection Directive (EDPD) signed, protecting individuals' personal data.
2004	Budapest Convention on Cybercrime adopted.
2018	EU General Data Protection Regulation (GDPR) implemented, introducing stricter rules on data collection and usage, including government surveillance.
2020	India launches NATGRID into use.
2022	OHCHR releases the report "The Right to Privacy in the Digital Age".

V. Current Situation

As technology grows bigger, more and more attention has been put on ensuring the safety and security of individuals when they use the internet. The Budapest Convention on Cybercrime is continually discussing and putting into order new legal frameworks to reduce misuse, and the United Nation's Human Rights council is focusing more and more in passing new laws to ensure personal freedoms are not violated.

However, with the growth of social media, governments and companies, such as Meta and Tiktok, using data they obtain without consent is also a rising phenomenon. It is necessary to set out strict and concise laws that draw the line at exactly what point is a fair compromise between privacy and safety.

Describing how these laws will be implemented clearly, including the role of transparency, data collection, and data processing will be essential to providing a blueprint of the future, and demonstrate the final goals that the blueprint aims to achieve.

VI. Major Parties Involved

China: China has an extensive database where online activity is often tracked and analysed to ensure no illegal or secret activities are being conducted. Identification documents, physical recognition, like Skynet, and fingerprints are examples of data collected by the government, while online interactions and transactions are tracked by large companies to police a stable online environment.

United States : The USA is a big advocate for freedom of speech. However it has steadily increased their digital surveillance in the past few years, with big American social media platforms like Meta and X being major data collecting sites. The Federal Bureau of Investigation (FBI) uses social media collected data often to detect and target threats to online and physical peace.

European Union: The European Union is quite protective of its citizens' digital rights. In the European Declaration on Digital Rights and Principles, the EU highlights the importance of freedom of expression and data protection. However, it also has a strict surveillance system regarding migration, like its digital framework, the EUROSUR.

India: India set up its surveillance database NATGRID in 2020. Because of the 2008 Mumbai Attacks, a strengthening of India's anti-terrorist systems was warranted and NATGRID was set up in order to detect and prevent such attacks in the future.

VII. Key topics to Debate

- How effective is digital surveillance in preventing crime and identifying potential threats compared to traditional policing methods?
- Does the use of advanced surveillance technology outweigh the risks of misidentification and increased public paranoia?
- Should national security and safety take precedence over individual digital privacy rights, or should privacy remain the stronger principle?
- How can countries ensure that surveillance does not lead to violations of democratic freedoms such as freedom of speech and expression?
- To what extent does digital surveillance encourage self-censorship among citizens, and is this an acceptable trade-off for safety?
- Should surveillance and content monitoring be primarily the responsibility of governments, or should private technology companies enforce regulations on their platforms?
- How can accountability be ensured when governments or companies misuse surveillance technologies?
- Is digital identity management and surveillance ultimately empowering citizens to live in safer societies, or does it enable authoritarian governance?

VIII. Bibliography

Council of Europe. (2025). The Budapest Convention on Cybercrime. Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention

European Commission. (2017). Commission proposes high level of privacy rules. European Union. https://ec.europa.eu/commission/presscorner/detail/en/ip_17_16

European Commission. (n.d.). European Digital Rights and Principles. European Union. https://digital-strategy.ec.europa.eu/en/policies/digital-principles

United Nations Human Rights Council. (n.d.). OHCHR and privacy in the digital age. United Nations. https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx

United Nations General Assembly. (2013). General Assembly backs right to privacy in digital age. United Nations. https://news.un.org/en/story/2013/12/458232

Privacy International (n.d.) Mass Surveillance. Privacy International. https://privacyinternational.org/learn/mass-surveillance