Forum: Human Rights Council (HRC)

Issue: The question of advancing legislation on digital privacy

Student Officer: Vishesh Shah

Position: Co-Chair

Introduction

In today's tech-driven world, where technology is advancing fast and digital platforms are ubiquitous, the need to protect our personal privacy is a big worry for everyone—individuals, governments, and international groups alike. As we navigate this evolving landscape, we're facing a pivotal decision point. It is critical that we are able to utilise the benefits of technology while simultaneously protecting our fundamental human rights, as outlined in the Universal Declaration of Human Rights.

The digital age has revolutionised our lives since it provides a wide range of benefits that have modified the way we live. It has made things a lot more convenient, making tasks that took days now into seconds. Nevertheless, it has also exposed us to fresh challenges and risks. The collection of our personal data by governments and businesses, often without our consent, has sparked crucial ethical and legal debates, making it tricky to determine how our information is being handled appropriately. Moreover, the growing need for security has driven enhancements in video surveillance technology, adding complexity to the equation. This has resulted in a broader range of organisations, beyond just law enforcement, using surveillance cameras, including households and small businesses. However, it’s difficult to draw a line between the vast collection and exploitation of personal data by governments and corporations, often without informed consent, and general surveillance use, and this has raised profound ethical and legal questions about the boundaries of individual privacy. The emergence of sophisticated surveillance technologies and the erosion of online anonymity further intensify these concerns.

Therefore as delegates, it is imperative that we grapple with the complexities of digital privacy by making resolutions that involve implementing legislation that not only respects the legal interests of governments and firms, but also legislation that safeguards the rights of citizens. While we find a way, let us remember the words of Eleanor Roosevelt, "Where, after all, do universal human rights begin? In small places, close to home – so close and so small that they cannot be seen on any maps of the world. Yet they are the world of the individual person; the neighbourhood he lives in; the school or college he attends; the factory, farm or office where he works. Such are the places where every man, woman and child seeks equal justice, equal opportunity, equal dignity without discrimination. Unless these rights have meaning there, they have little meaning anywhere. Without concerned citizen action to uphold them close to home, we shall look in vain for progress in the larger world."

Definition of Key Terms

Data Breach: Unauthorised access or disclosure of sensitive or confidential information, including personal or corporate data.

Surveillance: Systematic monitoring of people's activities or behaviour by individuals, governments, or organisations.

Anonymization: The process of removing personal information to prevent the identification of an individual, or a group of individuals.

Cybersecurity: The state of being protected against a perpetrator, who may try to carry out criminal activities against you on the internet; i.e. accessing, changing, or destroying sensitive information in order to extort money through ransomware or interrupt business processes. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

Encryption: The process of converting data into a coded format to prevent unauthorised access, especially during data transmission.

Ethical Frameworks: Establishing ethical frameworks involves defining principles and guidelines that govern the responsible development and deployment of AI technologies. These frameworks address issues such as fairness, transparency, accountability, and the ethical treatment of individuals impacted by AI systems.

Algorithmic Accountability: Legislations focus on holding organizations accountable for the algorithms they deploy. This includes transparency in algorithmic decision-making processes, the ability to explain AI decisions, and mechanisms for addressing biases and unintended consequences.

Key Issues

Cross-Border Data Flows

Regulating cross-border data flows remains a complex and unsolved issue in digital privacy legislation. In an increasingly interconnected world, personal data often traverses international boundaries. The challenge lies in ensuring consistent privacy standards and protections when data is transferred between countries. The recent Schrems II case in the European Union highlighted this issue. The European Court of Justice declared the EU-US Privacy Shield agreement unconstitutional, claiming that it did not provide European citizens with enough data protection when their data was transferred to the United States. This decision shows the need for regulations that are able to find a balance between global data transfers for legitimate purposes and safeguarding a person's individual privacy rights.

Biometric Data

Data is especially sensitive since it can be used for a variety of identification and identity reasons, especially biometric data such as facial recognition, fingerprint scans, and other sorts of unique human identifiers. As a result, clear international rules governing the acquisition and use

of biometric data are crucial. The Clearview AI case is a real-life example of this not happening properly, in which the company illegally took billions of facial photographs from social networking sites and sold access to these images to law enforcement officials. Similar incidents highlight the significance of comprehensive regulation in preserving an individual's privacy and preventing potential misuse.

Children's Privacy

Children's privacy is very important, particularly in online environments as they may not be able to fully comprehend privacy implications and the possible 'side effects' of their privacy being breached. In the past, legislation like the Children's Online Privacy Protection Act (COPPA) in the United States was used to protect children's data, but as digital platforms and smart devices have become increasingly popular, new challenges arise since COPPA isn't largely centered around the use of digital platforms and smart devices. A pertinent example is the TikTok case, where the platform faced allegations of mishandling children's data. This highlights the need for updated and globally applicable regulations that adapt to the evolving digital landscape and provide adequate protection for children's privacy.

Algorithmic Accountability

Addressing algorithmic accountability is a pressing but unresolved issue in digital privacy legislation. Automated decision-making processes, driven by complex algorithms, significantly impact individuals' lives in areas such as lending, hiring, and predictive policing. The challenge is to ensure transparency and fairness in these algorithms while harnessing their benefits. Real-life examples include biassed algorithmic decisions in lending, as seen in the Apple Card credit limits controversy, where women were reportedly offered lower credit limits than men. This underscores the importance of regulating algorithms to prevent discrimination and bias while maintaining their potential benefits.

Privacy by Design

Encouraging a "privacy by design" approach within organisations is essential, but establishing clear and enforceable standards for this practice is an unsolved challenge in digital privacy legislation. The concept revolves around integrating privacy considerations at the initial design

stage of products and services, rather than addressing privacy as an afterthought. Recent data breaches and privacy lapses, exemplified by the Facebook Cambridge Analytica scandal, underscore the need for comprehensive legislation compelling organisations to proactively embed privacy protections into their offerings. The challenge lies in defining specific requirements and enforcement mechanisms to ensure that privacy by design becomes a standard practice across industries.

Major Parties Involved and Their Views

United States:

One of the persistent issues in the United States is the lack of a comprehensive federal data privacy law. The USA relies on mainly state-specific regulations, resulting in inconsistent privacy protections. An example of this is the differing data breach notification requirements across states, leading to confusion and potential data breaches going unreported.

European Union (EU)

Cross-border data transfers within the EU remain a complex issue, particularly after the Schrems II decision. Balancing GDPR compliance with emerging technologies such as facial recognition poses challenges. A notable case involves Clearview AI's facial recognition technology, which we've already covered, has raised privacy concerns across Europe.

The People's Republic Of China

China faces a unique set of privacy challenges, including concerns about state surveillance and data practices of tech giants. One unresolved issue is striking a balance between innovation and privacy, particularly in defining the boundaries of government data access. An example is China's Social Credit System, which relies on extensive personal data for profiling citizens, sparking concerns about individual privacy and government control.

The Republic Of India

India is in the process of formulating comprehensive data privacy legislation. Key issues include balancing national security and individual privacy, particularly in the context of government surveillance. The Aadhaar system, which collects biometric data, has faced scrutiny over potential privacy violations.

Brazil

Brazil's General Data Protection Law (LGPD), similar to the GDPR, raises challenges in enforcement and implementation, especially for smaller businesses. Ensuring compliance with data protection standards and responding to data breaches are ongoing issues. Brazil also grapples with international data transfers and harmonising its data protection regulations with global standards.

Argentina

In Argentina, the implementation of the Personal Data Protection Act (PDPA) in 2000 aimed to protect citizens' privacy and provide access to their information in databases. However, an unresolved issue is related to surveillance, particularly involving the approval of ZTE, a Chinese manufacturer, to install security cameras. The US had expressed worry that such equipment could be used for spying. This case emphasizes the significance of striking a balance between national security and privacy rights.

Australia

Australia is navigating issues related to the balance between individual privacy and government surveillance. Proposed encryption laws have sparked concerns about potential privacy breaches. Clarifying data access boundaries and establishing strong oversight mechanisms are ongoing challenges. An example is the Australian government's push for access to encrypted messages for law enforcement purposes, raising debates about the impact on individual privacy.

Canada

In Canada, one unresolved issue involves regulating data protection in the era of advanced technologies. Balancing innovation with privacy protection is a challenge. A real-life example includes concerns over smart city projects like the Sidewalk Toronto initiative, where data collection and surveillance have raised privacy concerns.

Development of Issue/Timeline

Date: 1834	**Event:** Telegraph system hack	**Outcome:** One of the first ever cyberattack occurred in france. Two men were able to steal financial market information by hacking the French Telegraph system However it was not until the 1940s that cyber threats and privacy breaches really became a threat.
Date: 1914	**Event:** Establishment of the Federal Trade Commission Act (FTCA)	**Outcome:** The Federal Trade Commission Act (FTCA) was one of the first of its kind. This act severely outlawed unfair or deceptive commercial practices in correlation with Human rights abuses in accordance with digital privacy. The FTCA has always been one of the leading federal agencies that is most often involved with privacy regulations and enforcement.

Date: 1940	**Event:** First Ethical Hacker	**Outcome:** Rene Carmille was the first ethical hacker, he was a punch card computer expert and a member of the resistance in France during the Nazi occupation. He disrupted the Nazis efforts in tracking down jews. This sparked many cyber security threats to take place as a new word of possibilities were revealed.
Date: 1948	**Event:** Establishment of the UN declaration of Human Rights	**Outcome:** On December 10th the United Nations Declaration of Human Rights. This set the basic standards for human rights as well as privacy rights for every single human in society.

Date: 1999	**Event:** The NASA Cyber Attack	**Outcome:** Another major cyber security event to take place in 1999, the NASA cyber attack involved the breach and subsequent shutdown of NASA's crucial computers for around 21 days. Around 1.7 million pieces of software were also downloaded during the attack, which cost the space company around $41,000 on repairs. What made this attack so famous wasn't the expense associated with the crime, but the criminal responsible for the action.

Date: 2014	**Event:** Yahoo Attack	**Outcome:** Yahoo became the victim of one of the largest data breaches in history. Approximately 500 million accounts were hacked by a state-sponsored actor. The theft was the biggest known cyber breach recorded at the time, and criminals were said to have stolen everything from names and email addresses to telephone numbers, passwords, and date of birth details.

Previous Attempts to Solve the Issue

Data Protection Regulations

Adoption of rigorous data protection regulations was a critical step towards ensuring digital privacy. The General Data Protection Regulation (GDPR) implemented by the European Union in 2018 is an example of such a regulation. Businesses must adhere to regulations outlined in GDPR, which require obtaining consent, for data collection implementing robust privacy policies and promptly reporting any data breaches. Access to personal data, the option to request deletion, and transparency in data processing empower individuals. GDPR's impact is illustrated through fines for violation, like Google's €50 million penalty.

International Agreements

International agreements have been drafted to make the transmission of personal data easier while maintaining data protection standards. The EU-US Privacy Shield sought to facilitate data flows between the EU and the US. However, the framework's invalidation due to privacy concerns has highlighted the need for revised international data transfer mechanisms.

Industry Self-Regulation

Tech companies and industry associations have undertaken self-regulatory initiatives, enhancing transparency and user control over data. Apple's App Store Privacy Labels, for instance, provide users with comprehensive information about how apps collect and use their data, encouraging responsible data handling.

Government Oversight

Regulatory bodies like the Federal Trade Commission (FTC) have a role in ensuring that privacy rules are enforced and privacy violations are thoroughly investigated in the United States. Notable cases, such as Facebook's resolution after the Cambridge Analytica scandal underscore the government's dedication to holding companies for breaches of data security.

Privacy-Enhancing Technologies (PETs)

Technologies like end-to-end encryption ensure data security and privacy. Messaging apps like WhatsApp employ this technology to protect user communications from unauthorized access. This approach has become integral to preserving user privacy in digital communication.

Public Awareness and Education

Initiatives like Data Privacy Day promote awareness and educate individuals on online privacy rights and responsible online behavior. Such campaigns empower users to take an active role in protecting their digital privacy. Recent data breaches and privacy incidents, like the Facebook Cambridge Analytica scandal, emphasize the need for organizations to proactively integrate privacy protections into their products and services, known as the "privacy by design" approach. Although this approach is vital, establishing clear and enforceable standards for it remains a challenge in digital privacy legislation. Integrating privacy considerations during the initial design phase of products and services, rather than treating privacy as an afterthought, is crucial for ensuring comprehensive privacy protections.

Possible Solutions

Enhanced Data Protection Legislation

Governments can enact comprehensive data protection laws to create a robust legal framework for safeguarding digital privacy. These laws should encompass various essential provisions. They must require organizations to provide clear and concise privacy policies that inform users about data collection and usage. User consent mechanisms should be mandated, ensuring organizations obtain explicit permission before collecting and processing personal data. Additionally, stringent data breach reporting requirements should be in place, compelling organizations to promptly notify both authorities and affected individuals in the event of a data breach. Equally crucial are strict penalties for non-compliance, serving as an effective deterrent against privacy violations.

Cross-Border Data Transfer Agreements

International cooperation is paramount in establishing clear and enforceable agreements for cross-border data transfers. These agreements should address several critical aspects, such as the necessity for consistent data protection standards across borders. Moreover, they should lay out mechanisms to ensure that data is adequately protected during international transfers, along with oversight and enforcement measures to monitor compliance with the agreements. Protocols for addressing disputes and resolving conflicts between countries are equally vital components of these agreements.

Industry Self-Regulation

Tech companies and industry associations can proactively enhance self-regulation efforts. This entails developing and enforcing industry-wide privacy standards and best practices. Moreover, organizations should conduct independent audits and certifications to verify their compliance with these standards. Transparent data collection and usage policies should be implemented, and users should be empowered with accessible privacy controls to manage their data effectively.

Government Oversight and Enforcement

Regulatory bodies must play a vigilant role in ensuring that data protection laws are upheld. This involves regular monitoring of organizations' compliance with privacy regulations and

conducting thorough investigations into privacy violations. Substantial fines and penalties for non-compliance are essential to create a strong deterrent against privacy breaches. Adequate resources should be allocated to agencies responsible for investigating and responding to data breaches swiftly.

Privacy-Enhancing Technologies (PETs)

Governments and organizations can encourage the adoption of Privacy-Enhancing Technologies (PETs) to bolster data privacy. This includes investing in research and development of PETs such as end-to-end encryption, data anonymization, and secure authentication methods. These technologies should be seamlessly incorporated into products and services to enhance user privacy. Additionally, supporting open-source PET initiatives that promote transparency and accessibility is crucial.

Public Education and Awareness

Collaborative efforts are needed to raise public awareness and educate individuals about digital privacy. Initiatives should promote responsible online behavior and safe data practices. They should also provide resources and tools for users to better understand their digital privacy rights. Teaching individuals how to protect their digital identities and personal information is essential in an age where online interactions are ubiquitous.

Privacy by Design

Organizations should adopt a "privacy by design" approach, integrating privacy considerations into the early stages of product and service development. This involves conducting privacy impact assessments to identify and mitigate potential risks. Ensuring that privacy features are integral to the design and not added as an afterthought is critical. Organizations should also set clear guidelines for data minimization and deletion to reduce the risk of privacy breaches.

International Collaboration

Countries can collaborate on international standards for digital privacy, focusing on common principles and guidelines for protecting digital privacy across borders. Harmonizing regulations and best practices to address global challenges effectively is essential. Sharing knowledge and

experiences can help strengthen global privacy protections, creating a safer digital environment for individuals worldwide.

Ethical Use of Biometric Data

Governments and organizations should establish clear ethical guidelines for biometric data, including restrictions on its collection and storage, especially facial recognition. Frameworks should ensure the responsible use of biometric data for legitimate purposes while implementing safeguards against its misuse and abuse.

Strengthening Children's Privacy Protections

Legislators can update and expand existing laws, such as COPPA, by considering age-appropriate privacy protections for children in the digital age. Enhanced parental consent mechanisms for children's online activities should be put in place. Monitoring and enforcement measures should ensure compliance with children's privacy regulations. Moreover, educational initiatives can teach children about online privacy and safety, equipping them with the knowledge to protect their digital identities.

Bibliography

"10 Inspiring Eleanor Roosevelt Quotes." *Unfoundation.org*, 6 Nov. 2015, unfoundation.org/blog/post/10-inspiring-eleanor-roosevelt-quotes/#:~:text=, https://unfoundation.org/blog/post/10-inspiring-eleanor-roosevelt-quotes/#:~:text="Where%2C%20after%20all%2C%20do,or%20office%20where%20he%20works

"Clearview AI Accepts Permanent Ban from Selling Data to Private Firms." *Euronews*, 10 May, 2022, www.euronews.com/next/2022/05/10/facial-recognition-company-clearview-ai-permanently-banned-from-selling-data-to-private-co#:~:text=Facial%20recognition%20com

pany%20Clearview%20AI%20permanently%20banned%20from%20selling%20data%20to%20private%20companies,

Feldstein, Steven, and David Wong. “New Technologies, New Problems – Troubling Surveillance Trends in America.” *Just Security*, 6 Aug. 2020, www.justsecurity.org/71837/new-technologies-new-problems-troubling-surveillance-trends-in-america/, https://www.justsecurity.org/71837/new-technologies-new-problems-troubling-surveillance-trends-in-america/

Gulf, Redington. *Evolution of Surveillance Camera - Blogs by Redington*. 28 Nov. 2021, mea.redingtongroup.com/blogs/evolution-of-surveillance-camera/. Accessed 10 Feb. 2024, https://mea.redingtongroup.com/blogs/evolution-of-surveillance-camera/

“Mass Surveillance | Privacy International.” *Privacyinternational.org*, privacyinternational.org/learn/mass-surveillance#:~:text=It%20creates%20an%20environment%20of%20suspicion%20and%20threat%2C%20which%20can, https://privacyinternational.org/learn/mass-surveillance#:~:text=It%20creates%20an%

20environment%20of%20suspicion%20and%20threat%2C%20which%20can,chilling%20effect%20of%20mass%20surveillance.