Southern China International MUN

Official Background Guide

Human Rights Council: On measures to establish data privacy boundaries in the digital age

Agenda overseen by: William Kou

1. Description of the Issue

1.1 History of the Issue

In the rapidly developing landscape of the digital age, data privacy is becoming a critical issue for not only the people's privacies but also a country's security. Every click, every post, and every online transaction contributes to an individual's digital footprint, raising people's awareness of how to keep themselves and others safe in this sea of information. Additionally, the leakage of personal information affects not only people's daily lives but also their health and well-being, in which a minor misuse of personal information might lead to the exploitation of personal property. On the other hand, international governmental organizations depend on the internet to make certain moves regarding data transfer, in which a slight leakage of data might contribute to devastating impacts on the global situation. Data privacy has been an issue that lingered around for decades, and as new forms of data storage systems or methods are constantly being introduced into the modern world, monitoring data security becomes increasingly difficult.

Beginning in the 1970s, when data collection systems were gaining popularity and recognition, the risk of data leakage panicked investors and customers, making it a must-solve issue that could affect the entire future landscape of the Internet. To address this problematic situation, in 1973, the Department of Health, Education, and Welfare Advisory Committee developed a set of principles that tackle the problem of data privacy called **The Fair Information Practice Principles (FIPPs)**. According to the Federal Privacy Council, the FIPPs are "a collection of widely accepted principles that agencies use when evaluating information systems, processes programs, and activities that affect individual privacy" [4]. There are a total of nine principles that push and remind agencies to follow to ensure maximum security for their database. The standardization of data security systems at that time had a profound impact on the accessibility and accountability of web services and data collection programs.

In the 1980s, with the advent of personal computers and the transparency of data privacy protocols, businesses, and agencies started storing vast amounts of personal data. However, a drawback of FIPP was that it only mentored organizations on how to keep personal data secured. It did not consider the fact that information and data sometimes require transportation between places, causing this trade or movement of information to potentially put their privacies at risk. Thus, on 23 September 1980, a more detailed and elaborated guideline called the **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** emerged [9]. This set of standards was structured on the basis of FIPP and included measures that could combat privacy violations and even scaled data transportation up to a global scale, providing countries with the support for transborder data flows without being risked by leakages of information.

As people started working on securing their data by restricting external accessibility and limiting personal information usage, they forgot to build data resilience. Although the steps taken were on the right track, data at that time was still vulnerable, as there weren't any methods to encrypt the information after exposure. In the early 1970s, the **Data Encryption Standard (DES)** was created. It used algorithms for the encryption of digital data and was submitted to the National Bureau of Standards (NBS) to propose a candidate for the protection of sensitive, unclassified electronic government data. Although the algorithm itself was simple and insecure for modern applications, it spurred the creation of other new methods of encryption and influenced the advancement of cryptography. The **Advanced Encryption Standard (AES)** created in 2001 was a derivative of the DES system.

By the early 2000s, with the rise of **e-commerce and social media platforms**, companies of those platforms started to collect massive amounts of user data, which was not always transparent to the users themselves. This led to a rise in public concerns about how the data was being used or misused by those companies.

1.2 Recent Developments

As concerns over data privacy have intensified, the **COVID-19 pandemic** spurred a rise in data collection through status and position-tracking apps and devices. This period also implemented the usage of facial recognition and tracking devices to monitor and organize citizens more efficiently, which further raised the public's attention to the balance between privacy and public safety. Furthermore, certain financial companies and platforms incorporated the concept of facial recognition with the recent online payment system. It allowed citizens to pay without pulling out

their devices. Similar to the facial tracking device used in the pandemic, it led to a series of doubts over the merge between privacy and convenience.

In 2024, the growing interest and attention in the field of **Artificial Intelligence (AI)** pushed data privacy problems up to another level. As new forms of AI started to emerge, ensuring data security began to be difficult once again. AI is like a double-bladed sword, in which on one hand, it helps companies and individuals combat and identify potential threats that breach and exploit their privacy; on the other hand, it can be a tool cybercriminals use to create a more sophisticated and powerful attack that could steal information without being noticed or detected. Although law enforcement such as the **GDPR** limited companies to creating programs that might potentially put our privacies in danger, new technologies constantly outpace regular measures [5]. One day, regular methods of surveillance and protection will be useless against those technologies, and new methods will be required to restore stability and safety online.

Key Terms

Data Privacy – The protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information (Cloudflare).
Encryption – The process of converting information or data into a code, especially to prevent unauthorized access.
GDPR – General Data Protection Regulation. One of the strongest privacy and security laws in the world. It defines the individuals' fundamental rights in the digital age, the security of their data, the methods used for ensuring surveillance, and sanctions for those in breach of the rules [8].
Artificial Intelligence (AI) – The ability of a digital computer to perform certain tasks that mirror the tasks usually performed by intelligent beings. The development of artificial intelligence could potentially impact the data protection protocols developed prior to the creation of such algorithms [1].
AES – Advanced Encryption Standard. It was developed in 2001 and has been used, even till now, by the U.S. government to protect classified information. This system encrypts important data by chopping the data into unrecognizable pieces of 128 bits. When sending encrypted messages, the AES simply slices the plaintext into smaller blocks that are converted into ciphertext [6].
Confidentiality – The dictionary defines confidentiality as "the state of keeping or being kept secret or private." (Oxford 1) But in this case, it means protecting personal information. This information might include the user's lifestyle, health, and hobbies which they might want to be kept private.

2. Emphasis of the Discourse

2.1 Right-Wing Approach

The right-wing approach to data privacy places a strong emphasis on personal accountability. Conservative politicians argue that excessive regulation could impede economic competitiveness and inhibit innovation, and thus they want little government involvement. Traditionalist governments prioritize protecting free business and enabling the private sector to provide data protection solutions that are driven by the market. By advocating for minimal government intervention, this approach seeks to create an environment where private sectors are encouraged to develop and implement their data protection measures and strategies.

This strategy has the advantage of encouraging innovation and guaranteeing strong national security through data sovereignty, but it also takes the risk of degrading privacy through widespread surveillance, lowering consumer safeguards, and possibly causing exploitation. Without robust governmental support and oversight, companies may prioritize profits over privacy, resulting in the exploitation of user data for financial gain. Furthermore, the lack of stringent regulations may leave individuals vulnerable to data misuse and exploitation, as not all companies may invest equally in comprehensive data protection measures.

2.2 Left-Wing Approach

The left-wing perspective emphasizes social justice and business responsibility while prioritizing data privacy as a basic human right. To protect individual rights and enforce moral business conduct, liberal politicians support strict government restrictions like the GDPR. Protecting vulnerable populations, empowering individuals, and fostering international collaboration on data privacy norms are the goals of progressive legislators. For instance, marginalized communities, children, or individuals with limited digital literacy often face higher risks of exploitation, making strict regulations critical for ensuring equity. Furthermore, this approach seeks to foster international collaboration to improve on current global data privacy standards. This helps to create a more harmonized regulatory framework that protects a diverse range of citizens to make sure that no one is left behind.

However, this strategy may hinder innovation, raise compliance costs for companies, and present difficulties when implemented globally, even though it guarantees better consumer rights and

advances social justice. For instance, small and medium-sized enterprises (SMEs) may struggle to meet the technical and legal demands that allow them to meet the standards of the strict regulations. This can potentially hinder innovation, as resources that could be used for research and development may instead be distributed to those enterprises to ensure equality and regulatory compliance.

2.3 Stance of Intergovernmental Organizations

An intergovernmental approach to data privacy boundaries is a crucial framework for creating involvement and collaboration between nations to establish universal data protection standards. In the span of just a few decades, the concept of data privacy has evolved from a relatively simple concern into a complex and multifaceted challenge. This transformation has been driven by rapid technological advancements, changing societal norms, and the increasing value of information in the digital age.

Themes, such as the principles of consent, data minimization, and transparency, reflecting a global consensus on the importance of protecting personal information in the digital age are all aspects of digital privacy that are emphasized. Through international structures like the European Union's General Data Protection Regulation or regional organizational methods, the prioritizing of data privacy in international relations, governments can work towards a unified stance that respects individual rights while promoting innovation and economic growth.

From early conceptualizations to the comprehensive legal frameworks of today, the evolution of data privacy illustrates the transforming ways of societal values and the need to protect personal information. As we navigate through the rapid digital age, an intergovernmental approach is not only a regulatory necessity but also a moral imperative in safeguarding citizens' rights in an increasingly interconnected world [3].

2.4 Stance of Developed Countries

Due to a combination of national interest and external influence, developed nations often play a leading role in establishing international standards for data privacy. By highlighting data privacy as a basic right and imposing strict rules on businesses, the European Union has established a global standard with its General Data Protection Regulation (GDPR). Although less regulated, the US places a higher priority on private sector innovation and concentrates on specific legislation like the California Consumer Privacy Act (CCPA), which frequently strikes a balance between

privacy and national security issues [2]. Other industrialized countries, like Canada and Japan, have implemented comprehensive frameworks like Japan's Act on the Protection of Personal Information (APPI) and promote international collaboration [7].

These nations frequently take different measures, driven by the need to safeguard cyber security and protect citizens' personal information. While the U.S. pushes toward self-regulation and tech-driven solutions, the EU places a greater emphasis on strict regulations and cross-border cooperation. These distinctions may lead to misalignment between developed nations, especially when it comes to the application of international data privacy rules. Furthermore, wealthy nations frequently put their interests ahead of those of developing countries, therefore supporting policies that could unintentionally hurt economies that lack the funding needed to set up strong privacy protections. This leads to conflicts because developed nations seek to achieve a balance between their economic and technological advantages and promote ethical governance.

2.5 Stance of Developing Countries

Developing countries view the issue of data privacy as a dual challenge, in which they work on protecting citizens' rights while fostering economic and technological growth. Nations such as India, Brazil, and South Africa have all set hands on mitigating this problem. They tried to implement data privacy frameworks into their own countries' laws. For instance, India created the Digital Personal Data Protection Act (DPDPA), and Brazil implemented the General Data Protection Law (LGPD). These laws helped reinforce the concept of digital citizenship and also identify the right of individuals to protect their data.

The motives of these countries are the desire to ensure data dominance and to prevent the exploitation of national corporations. However, their differences in technological capacity and economic status delayed the development of intentions. A good example could be India, where the government put emphasis on data localization to maintain control over domestic data.

3. Possible Solutions

3.1 In Favor of Developed Countries

One of the greatest advantages developed by countries possess is their economic and technological capacity and can tolerate almost any form of solution as long as they are doable and ethical.

A possible solution might be promoting global data privacy standards, in which developed countries follow the existing frameworks such as the GDPR, and strengthen the protocols within them to ensure cross-border consistency in data protection. Furthermore, it can also encourage cooperation through international organizations to establish consensus on the guidelines as a whole.

Another possibility might be strengthening oversight of data transmission to ensure transparency. Creating standardized protocols and actions for data transfers between countries can alleviate possible leakages during the process and promote data security.

3.2 In Favor of Developing Countries

Although developing countries might not have the resources and power to implement such solutions, they can seek international collaboration to strengthen themselves.

One of the solutions could be that developing countries can balance data localization and economic growth. The stances of developing countries marked that they needed to find a way to balance their economy and technological advancements. Instead of enforcing strict data localization laws, they could implement data protection policies that come with flexibility, such as allowing data transfer for specific purposes. By doing so, it can minimize the capital spent on regulating such protocols while also providing flexibility to the citizens.

4. Keep in Mind the Following

While researching this topic, first understand and look through the profiles and the stance of your county. Put extra focus on the recent developments of the digital world and propose solutions that address such problems. Make sure that your county can afford to implement those solutions and check the feasibility of such solutions. Last but not least, consider some of the factors that might affect your solutions. Here are some guiding questions that you might want to think about while doing your research:

1. *What legal and regulatory frameworks can be implemented or strengthened to ensure data privacy while inspiring global cooperation?*
2. *How can the government of your country balance the need for data localization with economic affordability?*
3. *What role is your country playing or was playing in the long run?*

4. *How can public awareness be promoted to empower individuals to actively participate in protecting their data?*
5. *What measures can be taken to ensure corporations handle data responsibly while cooperating with international organizations?*
6. *What mechanisms can be established to address the problem of the transparency of data transmission?*

5. Evaluation

As the Internet evolves, new methods of data collection emerge, and the risk becomes greater at the same time. Concerns regarding data privacy and security intensify every day, and without proper methods to address such issues, aspects of life will be affected. As data become increasingly valuable and vital in the digital age, it interconnects with our everyday lives; from small things such as social media to bigger things like health insurance and financial status. Expand your knowledge and think critically about how to mitigate such concerns. Build your thinking upon prior knowledge and innovate beyond boundaries to create new possibilities. Good luck delegates!

6. Bibliography

1. Encyclopædia Britannica. 2024. “Artificial Intelligence.” *Encyclopædia Britannica*. December 19, 2024. www.britannica.com/technology/artificial-intelligence.
2. State of California - Department of Justice - Office of the Attorney General. 2024. “California Consumer Privacy Act (CCPA).” March 13, 2024. oag.ca.gov/privacy/ccpa.
3. Digital Privacy Guru. 2024. “The Evolution of Data Privacy: From Early Days to the Digital Age.” Accessed December 22, 2024. digitalprivacyguru.com/articles/the-evolution-of-data-privacy-from-early-days-to-the-digital-age.
4. FPC. 2024. “Fair Information Practice Principles (FIPPs).” Accessed December 22, 2024. www.fpc.gov/resources/fipps.
5. Consilium. 2024. “The General Data Protection Regulation.” Accessed December 22, 2024. [www.consilium.europa.eu/en/policies/data-protection/data-protection-

regulation](www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation).

6. University of Law. 2024. “The Importance of Data Privacy Law in the Digital Age.” *The University of Law*. October 11, 2024. www.law.ac.uk/resources/blog/the-importance-of-data-privacy-law-in-the-digital-age.
7. DLA Piper. 2024. “Law in Japan - DLA Piper Global Data Protection Laws of the World.” Accessed December 22, 2024. www.dlapiperdataprotection.com/index.html?t=law&c=JP.
8. GDPR Info. 2024. “Legal Text.” *General Data Protection Regulation (GDPR)*. April 22, 2024. gdpr-info.eu.
9. OECD. 2024. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Accessed December 22, 2024. www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.
10. Oxford English Dictionary. 2024. “Online Search, N. Meanings, Etymology and More.” Accessed December 22, 2024. www.oed.com/dictionary/online-search_n?tl=true.
11. United Nations. 2024. “The Right to Privacy in the Digital Age.” Accessed December 22, 2024. digitallibrary.un.org/record/3985679?v=pdf.