Ensuring the protection of privacy in regards to new and upcoming technologies

Committee: HRC

Student Officer: The Chairmanship

Forum: Human Rights Council (HRC)

Issue: Ensuring the protection of privacy in regards to new and upcoming technologies

Name: Laura Alavi Namine, Ban Habib, Adithya Vijay

Position: Chair, Co-Chairs

Introduction

Protecting privacy is one of the most pressing and critical challenges of our time. Today's technological advancements have led to a world where personal data can be collected, used and shared in ways that we previously thought were unimaginable. Many people's lives are starting to depend on mobile phones, laptops and more. There is a lot of technology on the market that is intended to protect our privacy, but these technologies can also be misused to violate our privacy. In recent years, technology has played an increasingly important role in our daily lives. We use technology to communicate, get information, shop and make payments. These technologies have made it easier to communicate with each other, but have also compromised the privacy of the individuals.

With the advent of new technologies such as the Internet of Things (IoT), cloud computing and artificial intelligence (AI), the protection of privacy has become even more important. These technologies can collect a huge amount of personal data, such as location data and health information, which can be used by companies and governments to improve the quality of service. But this data can also be used to control and manipulate us.

Therefore, it is crucial that we properly protect people's privacy with respect to these new technologies. It is important that the privacy of our society can be safeguarded while at the same time, we can reap the benefits of the new technologies. If we get this right, we can take advantage of the benefits that technology offers us, while at the same time protecting people's privacy. It is important to remember that privacy is a fundamental right, and that protecting privacy is everyone's responsibility. If we work together to protect the privacy of our society, we can ensure that we can reap all the benefits of the new technologies, while at the same time protecting everyone's privacy.

Definition of Key Terms

Algorithm

An algorithm is a procedure used to solve a problem or perform a calculation. Algorithms function as a list of instructions that perform specific actions in hardware and software-based routines. They are used to solve problems or execute a computer program.

Artificial intelligence

Artificial intelligence (AI) is a branch of computer science that focuses on the development of computer systems and software that are capable of performing tasks that would normally require human intelligence, such as visual perception, speech recognition, language translation, decision-making, and problem solving. AI systems are able to learn and adapt to new situations, allowing them to improve their performance over time.

Digital identity

A digital identity is a body of information about an individual, organisation or device that exists only online. It arises from the use of personal information on the web and from the shadow data created by the individual's actions online. It can be a Pseudonymous profile linked to the device's IP address, or a randomly-generated unique ID. Examples of data points that can help form a digital identity include username and password, purchasing behaviour or history, date of birth, social security number, online search activities, and medical history. Digital identities come with privacy and security risks, including identity theft. Several authentication and authorization systems have been explored, but there is still no standardised and verified system to identify digital identities.

OECD

The Organisation for Economic Co-operation and Development (OECD) is an international organization that works to make lives better. They do this by using policies. Their goal is to put together policies that provide equality, opportunity and for better lives. The OECD works with government, citizens and politicians to put together the policies. They do this so that everyone agrees and there is no objection.

The OECD privacy guidelines are a set of internationally recognized standards for protecting personal data and privacy. They were developed in 1981 to ensure the privacy of individuals when

their personal information is collected and processed. The guidelines provide a framework for countries to implement their own national laws, as well as for organisations to develop their own privacy policies. The guidelines outline seven key principles for protecting personal data: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, and individual participation. They also provide guidance on topics such as cross-border data flows, data transfers, and sanctions for non-compliance.

IoT

The Internet of Things (IoT) is a network of physical objects, such as devices, sensors, and other items embedded with electronics, software, and connectivity, enabling them to exchange data and interact with one another. The main purpose of IoT is to collect data from the physical objects and use it to provide insights, improve efficiency, and automate processes. It has the potential to revolutionise the way we live, work, and interact with the environment around us. IoT is used in many industries, from healthcare to manufacturing, and its applications are still growing. It is revolutionising how we interact with the physical world, and is sure to bring many more benefits in the years to come.

General Overview

Several pieces of information that you might have believed to be private are known to the entire globe. From birth to death, a citizen of a developed country leaves a digital footprint that grows exponentially with online banking, e-commerce, and mobile commerce. Google, Tiktok, Meta, Visa, MasterCard, American Express, every bank you've ever used, your travel agent, every airline whose frequent flyer program you've ever joined, telephone and electric companies, all kinds of professional organizations, local governments, boards of education, utilities, and more are among the organizations that have detailed personal records about their customers.

Marketers can now obtain data without the direct knowledge of consumers thanks to the internet. Organizations can collect new forms of information, like click-and-viewing behaviors, that can be used to target and profile specific consumers by employing tracking software and cookies. Marketers can monetize their websites by selling advertising thanks to the collection of this data. Despite the fact that these technologies raise the same privacy issues as conventional database marketing, customer data is now maintained on a system that may be open to all Internet users. The likelihood that this data will be accessed and used for purposes other than what it was intended for is rising.

Human rights, sometimes known as natural rights, and legal rights are the two main categories into which rights can be divided. Laws frequently seem to revolve primarily around the rights that people possess, particularly in the United States. There are certain constitutional rights, such as the freedom of speech, the right to practice one's religion as one chooses, the right to keep and bear arms, the freedom from being compelled to testify against oneself, the right to equal protection under the law, and the right to legal representation.

The right to privacy is one of many rights that are implied rather than specifically stated in the text of the Constitution. The right to privacy has become an enforceable constitutional right as a result of ongoing judicial interpretation. The ambiguous constitutional status has codified the idea that privacy is not a unified or singular concept but rather a term that entails at least three different dimensions or discrete legal torts: *intrusion* (i.e., physically invading a person's solitude or seclusion), *disclosure* (i.e., publicly disclosing embarrassing private facts), and *false light* (i.e., false public disclosure).

Your web browser comes with security features that can help safeguard your private data. Spend some time becoming familiar with your browser's privacy and security options and keep it updated. Some tools allow you to limit the amount of private information you post online, while others let you delete the records of the websites you've searched or visited from your computer. Install security and antivirus programs, and keep them updated.

The demand for safety is at the core of our need for online privacy. It makes sense to protect your digital life in the same way that you do your real house and possessions. Whichever technology you employ (or don't employ), privacy offers you control over your identity and everything that makes it up. Yet, because things are not as tangible or obvious to everyone, most people do not place a high value on online privacy. Online privacy is also difficult to achieve because of the complicated technological, legal, commercial, and social combination. That does, however, make it necessary.

Because it provides you control over your identity and personal data, internet privacy is crucial. If you don't have that control, anyone with the means and the will can use your identity to further their interests, such as selling you a more expensive trip or robbing you of your savings. Your closest friends, family, co-workers and even employers are affected by what you publish on social

media, what you discuss in online comments, and how well you safeguard your data. Because of this, anything you do to protect your personal privacy benefits other people as well.

With the help of social media and other technological developments, it is now remarkably simple to share every part of our lives and strengthen our social connections. The result of that, which frequently goes unreported because so many people do it, is oversharing.

Oversharing divulges more personal information about you than you ever intended to. They can get a complete map of your possessions and directions to them by posting videos of your house online. Photos of your boarding passes show where you are going and for how long you will be gone. You develop a clearer image of your life, routines, significant connections, and possessions with each post.

Example: Google

Giant firms such as Meta, Line, Kakao or Google collect every piece of information they can. Each website visit, each click, each remark is recorded. These companies know much more about us than we do. By deploying a plurality of tools, they are able to track every move, transaction or word users say and do.

The most recent sales pitch given by Google, which made its name by collecting the world's information, claims that it will attempt to accomplish more with less information collected. The tech giant unveiled a number of privacy improvements on May 11 at its I/O 2022 developer conference, claiming that they will give users more control over how their data is used by Google applications and made public through search. The My AdCenter interface, which is a center where users can choose from a variety of themes they are interested in or choose to see fewer advertising on a certain issue, is one new improvement made public during the conference.

At the presentation on safety and security, it was acknowledged that users' privacy expectations are evolving and that the business must take note of these changes and make necessary adjustments. Also, Google is claiming to be working to increase customer safety across all of its products by introducing additional security protections right out of the box, in line with the company's motto "secure by default, private by design."

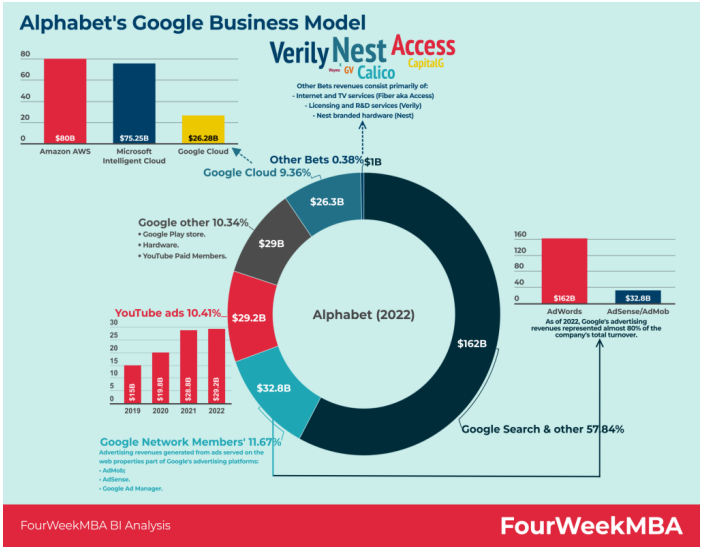

Figure 1: Google's business model, fourweekMBA

The company remains criticized by many who still doubt Google's transparency, mainly due to AdSense. AdSense is the company under Google that serves ads to all users of Google, they are also the company managing the revenue of customers such as money-making YouTubers. This company has been called out for being "opaque" and lacking transparency on the way they work and get their information in order to filter their ad service which is personalised for each user.

Google, and therefore AdSense too, are owned by Alphabet, a giant "collection of companies". Their largest companies are Google (YouTube, Google Maps, Google Pay, etc.) and Android. Google itself has not been transparent as to who has access to their user's information. AdSense services very likely get information from Google and its sub-companies, yet these remain only theories as it is very complicated to know what really goes on considering all information is confidential.

Fingerprints

Device fingerprinting, which identifies the operating system (OS) and browser that were used to initiate a connection, enables websites to identify your device. The justification for fingerprinting technology is frequently the desire to provide the greatest service to visitors. engagement with the page's material in a visually appealing manner. Although useful, this information simply allows the server owner to follow visitors' activities on the page and other websites.

The days of private internet are over, even when all personal privacy tools are turned on. Because there is a large amount of hardware and software that depends on confidential user data. And the only people who expect that are illiterate online users.

Figure 2: A fingerprint scan

Timeline of Key Events

Date	Event
1981	The Organisation for Economic Co-operation and Development (OECD) publishes its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," which provide a framework for protecting privacy in the digital age.
1995	The European Union adopts the Data Protection Directive, which sets out rules for how personal data should be collected, processed, and used in the EU.
1998	The United Nations adopts the Universal Declaration on Human Rights, which includes the right to privacy as a fundamental human right.
2004	The Asia-Pacific Economic Cooperation (APEC) adopts the APEC Privacy Framework, which provides guidelines for protecting privacy in the Asia-Pacific region.
2007	The Council of Europe adopts the Convention on Cybercrime, which criminalises certain cyber offences and includes provisions for protecting personal data.
2010	The Mexican government passes the Federal Law on Protection of Personal Data Held by Private Parties, which regulates how private companies collect and use personal data.
2012	The Brazilian government passes the Brazilian General Data Protection Law (LGPD), which sets out rules for how personal data should be collected, processed, and used in Brazil.
2014	The Japanese government passes the Act on Protection of Personal Information, which regulates how personal data should be collected and used in Japan.
2018	The European Union adopts the General Data Protection Regulation (GDPR), which strengthens and expands the Data Protection Directive's privacy

	protections.
2019	The Indian government passes the Personal Data Protection Bill, which sets out rules for how personal data should be collected, processed, and used in India.
2020	The California Consumer Privacy Act (CCPA) goes into effect, giving California residents the right to know what personal information businesses are collecting about them and the right to have that information deleted.
2021	The Chinese government passes the Personal Information Protection Law (PIPL), which sets out rules for how personal data should be collected, processed, and used in China.

Major Parties Involved

The Electronic Frontier Foundation

An organisation that was established in 1990 is a non-profit aimed at 'championing civil rights and liberties within the digital space' (Cliente and Identity Review). It promotes freedom of speech while also empowering illegal user surveillance and other privacy breaches that may (have) occur(ed). 'Notably, they are known to have led movements against facial recognition technologies that infringe on privacy rights.'

Fight for the Future

It is an activist organisation that aims to defend even the most basic of human rights in the new technological world. Specifically, they focus on 'racial, gender and wealth inequalities caused by certain tech policy issues.' They also offer guides on their website to improve self-security and privacy.

Privacy International

It 'aims to be an obstacle to powerful institutions that are trying to strip users of their digital freedom and autonomy'. On their website, they help users find information regarding recent events in the digital world, as well as provide help to maximise digital safety and privacy.

Foundation for Technology and Privacy

Outreach Formed by Privacy Vaults Online, this organisation is dedicated to raising awareness for youth privacy problems online, and aims to educate minors on ways to safely browse the internet. Privacy Rights Clearinghouse This is a nonprofit aimed at educating people on privacy rights. They teach the public on 'dealing with data breaches and identity theft all the way to spam emails'.

Privacy Rights Clearinghouse

This is a nonprofit aimed at educating people on privacy rights. They teach the public on 'dealing with data breaches and identity theft all the way to spam emails'.

Possible Solutions

Data privacy laws

By making data privacy rights, you as a country or organisation can ensure more detailed rules about how new and still upcoming technologies may handle your data. According to the OECD's privacy guidelines, new and future technologies should be designed and developed in a way that protects the privacy and security of individuals while preserving the possibility of further innovation.

The OECD guidelines are relatively general, and can therefore be used as a tool to create even more specific, important laws and regulations. This can be done both at the national level and in organisations such as the UN.

Encryption technologies.

Data encryption is the process of encrypting data so that only authorized individuals can access it. This is done by encrypting data. If a person without access does gain access, the data will be unreadable. This is beneficial for data protection because it prevents unauthorized access to it. Moreover, encryption technologies can be used to ensure that data collected from individuals is secure even if it is stored in a cloud or other remote location. This helps protect the data from being accessed by anyone other than those authorized to do so.

Websites such as Chatgpt and OpenAI can go through algorithms very quickly to provide correct answers to a person's questions. One can also take advantage of this by hacking the sites to then get too personal data faster. If this data is properly encrypted, it will be much harder to get behind data.

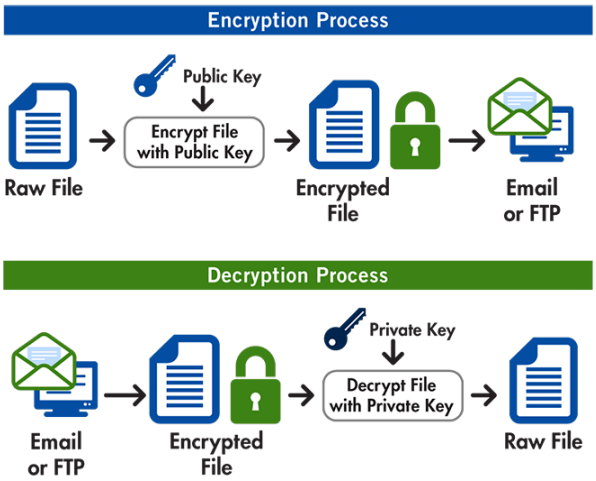

Figure 3: Encryption and decryption processes

Bibliography

O'Sullivan, Serena. « 8 Ways Google Constantly Invades Your Privacy — and How to Fix It ». Komando.Com, 26 may 2022, https://www.komando.com/security-privacy/ways-google-invades-your-privacy/804545/

"Privacy-OECD." OECD, www.oecd.org/digital/privacy

Simplilearn. "What Is Data Encryption: Types, Algorithms, Techniques and Methods." Simplilearn.com, 11 Nov. 2022, www.simplilearn.com/data-encryption-methods-article

Burns, Ed, et al. "What Is Artificial Intelligence (AI)?" Enterprise AI, 9 Feb. 2023, www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligenc

Faife, Corin. « Google Pitches for User Trust with Expanded Privacy Controls ». The Verge, 11 may 2022, https://www.theverge.com/2022/5/11/23066161/google-privacy-controls-protected-computing-io

Canada, Office of the Privacy Commissioner of. Protecting Your Privacy Online. 12 september 2016, https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/protecting-your-privacy-online/

Projet Cubicle, "Digital World and its Danger to Personal Privacy", Valencina, Pacelli, 2 August 2022 https://www.projectcubicle.com/digital-world-and-its-danger-to-personal-privacy/

“About the OECD.” Oecd, www.oecd.org/about

Contributor, TechTarget.“Digital Identity.” WhatIs.com, 30 Aug. 2017, www.techtarget.com/whatis/definition/digital-identity