Forum: SDG 9 Committee

Student Officers: Rohan Joshi, Tanuska Bora and Zain Allaboun

Be sure to consult the UNIS MUN LibGuide for additional resources.

Topic 1: The Question of Digital Footprint Erasure and Digital Anonymity

Introduction to the Topic

In our ever growing and rising world, people strive for privacy in the digital age. Each person desires to anonymously surf the internet and conceal their identity from the digital platform. Over the past few years, more people are going on the internet anonymously due to government's surveillance increasing, raising issues of privacy. However, it has become difficult to not leave a digital footprint on the internet. Many websites require the user's permission to cookies to access the web page. These cookies track the user's browsing history, IP address and their on site behaviour. This does not allow users to hide their digital footprint and instead makes it harder for users to erase their personal data including digital footprint. Even if we try to erase our data and footprints, governments and private organisations have unauthorised access to our data.

Online anonymity has also brought up challenges to our digital society. With an increase in the implication of digital finance and online transactions, it brings up several challenges along the way. For example, individuals make transactions on websites such as Ebay and Etsy (that are run by private individuals without the support of organisations), and the payment through online means such as an invoice and the need for important documentation sent through emails.

Currently, everyone lives in an interconnected world where it is hard to avoid the internet. However, alongside individuals; governments, organisations and corporations have access to the internet and the data the users input into websites. This can stem into abuse of people who surf the internet. It is important to respect the human rights of people who choose to conceal their identity online. In addition, anonymity is a core concept in protecting these rights and other foundational rights that deserve closure. In a world where a user's data can be processed, collected and stored so easily, concerns about privacy. According to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, "the Internet is one of the most powerful instruments of the 21st Century".

With growing individuals engaging in anonymous online activities, it introduces the chance to express their voice and engage in different types of interactions with others on the internet. However, the chance of remaining anonymous has shown to be unlikely as the storage of personal information on websites, IP addresses and tracking through wifi has been prominent by governments and individuals. This causes the violation of privacy and the violation of the freedom of speech.

Definition of Key Terms

Digital Footprint: A trail of data a person leaves behind while using the internet. This includes the websites you visit, emails you have sent and the information you submit online.

IP Address: An Internet Protocol address is a numerical identification for network interfacing and location addressing.

Cookies: A piece of data stored within a web browser that the website can retrieve at a later time.

VPN: VPN (or a Virtual Private Network) establishes a private network and disguises your online identity.

Online Anonymity: Online anonymity is the ability for a person to browse the internet while their identity is protected from a third party.

eID: Similar to Bring Your Own Identity (BYOI), an eID is a proof of identity for citizens. An eID can be used for its citizens to gain access to several sectors from both governmental and private organisations.

Katz vs. United States: The Katz vs. United States case made by the U.S parliament to redefine the search and seizure of citizens to support the protection of the fourth amendment in the U.S Constitution.

Key Stakeholders

The Office of the High Commissioner of Human Rights (OHCHR) : The OHCHR ensures that states, who want access to encrypted or anonymous data should do so through judicial processes. The OHCHR ensures individuals' dignity by securing their personal data and information.

Europol: Europol, more specifically the European Cybercrime Centre has established laws to fight cybercrime and authorise the internet to be a safe and open space. It supports its member nations in preventing and combating cybercrime and organised crimes.

The General Assembly: The General Assembly urges and recommends the privacy of the internet by protecting the rights of digital communication. The general public are entitled to take part in public affairs under anonymous identities without the interruption of the State.

European Commission: The European commission aims to open access to the internet in rural areas and develop the digital infrastructure. They aim to use the digital media to develop growth, job creation and enable topics such as Gender Equality, Sustainable Agriculture and more.

The Financial Action Task Force (FATF): The FATF is an organisation aimed to promote policies to tackle the issue of money laundering, terrorist financing and the financial support of weapons. The FATF recognised the issues of money laundering and other financial misuses.

UNODC: Recognizing that cybercrime is a form of major crime, the UNODC recognizes the adverse effects and aims to promote capacity to fight cybercrime through national structures and actions. The UNODC provides technical assistance, prevention via awareness and international cooperation.

Key Issues

Cyberbullying: As the transition to anonymous users on the internet rises, many people sought the opportunity to misuse their anonymity to participate in cyberbullying of others.

Fake Accounts: Anonymity can interfere with the creation of fake accounts and fake presence on the internet. Over the years, the customization of online avatars and online accounts has seen an increase over many different platforms including Facebook, Instagram.

Spam: Over the years, the expansion of spammers across social media platforms has grown exponentially. Some users take their anonymity online to an advantage and harass others online by portraying themselves as other users. In Instagram alone, 95 million accounts are spam. These trolls threaten other users by sending them demeaning messages in order to hook them and eventually send spam messages.

Public Manipulation: Anonymous users can also be used to manipulate public thinking. The most notable use of this is during the 2016 U.S presidential election. It was speculated that Russian invested thousands of dollars to create facebook advertisements to influence the presidential election. The aim was to support the outcome for Donald Trump and discredit Hillary Clinton.

Identity Theft: Identity theft, the act of using another person's identity, usually for personal benefit or financial gain. Identity theft can occur in many different ways such as financial identity theft (where an individual uses another person's identity to obtain credit or debit cards and other financial benefits), medical identity theft (where a person uses another person's identity to get free medical care and other health benefits), and child identity theft (where posers use children's names to obtain free student loans, housing and other benefits that children may have access to).

Cases of identity theft occur when people receive unsolicited emails that guarantee them the benefit of the victim. They obtain the person's financial information or even personal information for later purposes.

Internet Inclusion: While most of the advanced world seems to have access to the internet, an approximate of 35% of the rural population do not have access to the internet, compared to the 80% of the advanced world having access to basic internet services. The challenge of expanding broadband access to simple services is necessary as the reliance of others to complete simple transactions on the internet is lessened, reducing the chances of fraud and scams.

Timeline of Resolutions, Treaties, and Events

Date	Description of event
1850	The United States Census Bureau starts collecting information about U.S citizens through businesses by surveys they conduct. They also collect data from local governments and federal states.
1967	The Katz vs. United States rules that intercepting communications require a warrant. It supports the Fourth Amendment of the U.S constitution which

	protects citizens from unreasonable searches and seizures by the government.
1974	The United States released the Privacy Act which governs data collection and information about an individual in systems by federal agencies.
1983	Robert Kahn and Vinton Cerf founded the internet. First starting out as a communications model, which introduced the transmission of data across networks. This transmission protocol was called “Transfer Control Protocol (TCP)”.
1993	A famous publisher on The New York Times said that, “On the internet, nobody knows that you’re a dog”. At the time, the web was a new technology introduced to the world. Many users who logged on early were promised digital anonymity and pseudonyms while browsing the internet.
2016	During the presidential election against Donald Trump and Hillary Clinton, 13 Russians and 3 Russian companies indicated charges to boost the outcomes for candidate Donald Trump while discrediting Hillary Clinton to rig the presidential election.
2020	CCPA (California Consumer Privacy Act) is reenacted. America’s strictest law comes out of California. This act gives them more control over the personal information and what information businesses and the government. It regulates the information and data taken from the government

June 1, 2020 - May 32st 2021	Former president of Brazil: Bolsonaro continued to spread false information regarding the Covid 19 pandemic by promoting fake treatments.
June - December 2020	Bolsonaro and his government ministries monitored online activists, journalists and critics towards the Bolsonaro administration.
May 2022	Members of the European Parliament (MEP) and the Council discussed to strengthen the laws surrounding cybersecurity and obligations regarding online information sharing
November 2022	The European parliament updated the EU laws to bolster cybersecurity to essential services across Member States

Possible Challenges & Solutions

Making the most of privacy settings: It is important to take care of your privacy settings and make sure that the user uses their privacy settings to the maximum extent possible. By adjusting the settings, the user is able to control the information they are showing to the rest of the internet and websites they visit. By minimising the information they are showing, especially in social media platforms such as Instagram and Facebook, they are not as likely to be a target of cyberbullying.

Monitoring: Seeing as the issue of online manipulation grows and it serves an impact on major events such as the presidential election, it is important for the governments or organisational monitoring on comments made online or even advertisements shown on social media websites such as Facebook. It is important for organisations to monitor activity that might seem suspicious online, especially having confirmation from a reliable source to accept advertisements, not allowing unmonitored activity on their websites.

Clearing Cookies: Most websites tend to track a user by their cookies setting. When a person accepts the cookies on a website, they essentially leave hackers to track their activity on a website. This might

possess a threat especially when a person is making a transaction on a website (that has their bank details). By clearing cookies on a website, it makes it less likely for hackers to access personal data from a website that the person has visited. Furthermore, this provides almost no risk for hacking as hackers do not have access to data from the user.

Victim Support: Victims of digital attacks come in different variations. If an individual is a victim of hacking, they can seek help by reporting the scam on the Department of Justice's website. Furthermore, additional help from authorities can support victims to gain their information back. Rapid relief hotlines should be set up in order to support victims at immediate disposal.

Contact Authorities : Many individuals who are exposed to data breaches and identity theft can contact authorities immediately. This usually can occur in many different ways such as the theft of their bank information, credit or debit card information and the theft of their child's information. Many websites including Identity Theft.gov is a place to contact if someone's been a victim of identity theft.

Promoting Access and Application: Nonprofit and governmental organisations can aim their projects to expand access by opening public computer spaces for the open public to use. Furthermore, public schools and colleges can expand their network (Wi-fi) to support neighbouring areas. To imply application, in-person training should be utilised to teach adults and students how to use the basic platform overall.

Recommendations for Resolution Writing including Research

As the SDG 9 council will focus on the question of the erasure of digital footprint and digital anonymity, the chairs highly recommend the delegates to focus their research upon the problems that are introduced with digital anonymity. For example, digital anonymity introduces the problem of spam and fake accounts. According to Kicksta, there are a reported 95 million fake accounts currently registered on Instagram. This means that almost 1 in 10 accounts are fake. Delegates can focus on how anonymity can bring spam towards victims. From this, delegates can write resolutions in order to be in favour of digital anonymity to protect the rights of citizens (i.e the freedom of speech under the oppression of external influence).

However, with the advantage of not concealing your identity online, delegates could argue about the disadvantages of being anonymous online. As being anonymous could lead to online bullying, hacking

without being traced. Therefore, delegates can focus their research upon cases of anonymous hacking and how being digitally anonymous can cause harm to other individuals and society overall.

Additionally, delegates should widen their focus to people of different circumstances. For example, delegates could research on people who are victims of identity theft or other crimes under the influence of digital anonymity, or talk about the different perspectives that occur in this issue. Delegates should also focus their arguments for people who do not have access to the digital media. For example, many people in rural areas do not have access to the internet, and have to ask someone else to complete their bank work on personal information.

Bibliography

"Brazil: Freedom on the Net." *Freedom House*, freedomhouse.org/country/brazil/freedom-net/2021. Accessed 7 Jan. 2023.

Carr, Brad. "Digital Identity: Public and Private Sector Opportunities." *Future Identities*, thefutureidentity.com/digital-identity-public-and-private-sector-opportunities/. Accessed 21 Dec. 2022.

"Cybercrime." *United Nations Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/index.html. Accessed 7 Jan. 2023.

European Parliament. "Cybersecurity: Parliament Adopts New Law to Strengthen EU-Wide Resilience." *European Parliament*, 10 Nov. 2022, www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience. Accessed 7 Jan. 2023.

---. "Fighting Cybercrime: New EU Cybersecurity Laws Explained." *European Parliament*, 10 Nov. 2022, www.europarl.europa.eu/news/en/headlines/security/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained. Accessed 7 Jan. 2023.

"General Assembly Backs Right to Privacy in Digital Age." *The United Nations*, 19 Dec. 2013, news.un.org/en/story/2013/12/458232. Accessed 14 Dec. 2022.

Hussain, Ali. "What Is Identity Theft? Definition, Types, and Examples." Edited by Marguerita Cheng. *Investopedia*, 21 Sept. 2022, www.investopedia.com/terms/i/identitytheft.asp. Accessed 22 Dec. 2022.

Kaye, David. "Human Rights, Encryption and Anonymity in a Digital Age." *United Nations*, 1 July 2015, www.ohchr.org/en/stories/2015/06/human-rights-encryption-and-anonymity-digital-age. Accessed 14 Dec. 2022.

Moyakine, E. "Online Anonymity in the Modern Digital Age: Quest for a Legal Right." *Journal of Information Rights Policy and Practice*. *Research Gate*, http://doi.org/10.21039/irpandp.v1i1.21. Originally published in *Journal of Information Rights Policy and Practice*.

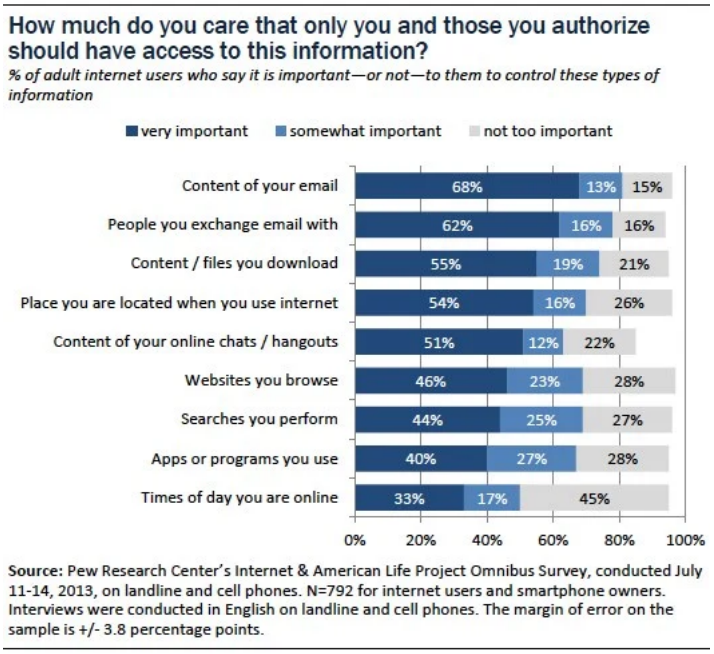
"Privacy in the Digital Age of Encryption and Anonymity Online." *Europol*, 30 Oct. 2016, www.europol.europa.eu/publications-events/events/privacy-in-digital-age-of-encryption-anonymity-online. Accessed 14 Dec. 2022.

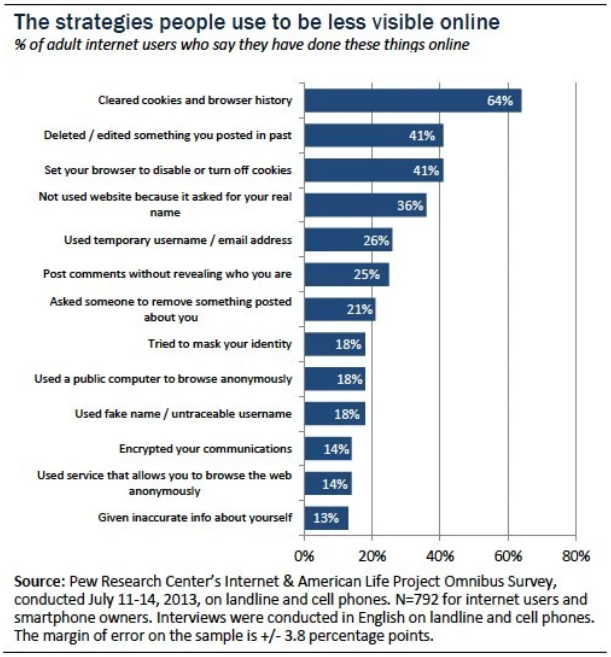
"The Problem with Anonymity on the Internet." *Risk Eye*, riskeye.com/the-problem-with-anonymity-on-the-internet/. Accessed 15 Dec. 2022.

United States, Congress, House, Federal Trade Commission. *Identity Theft*. *Federal Trade Commission*, www.identitytheft.gov/#/. Accessed 22 Dec. 2022.

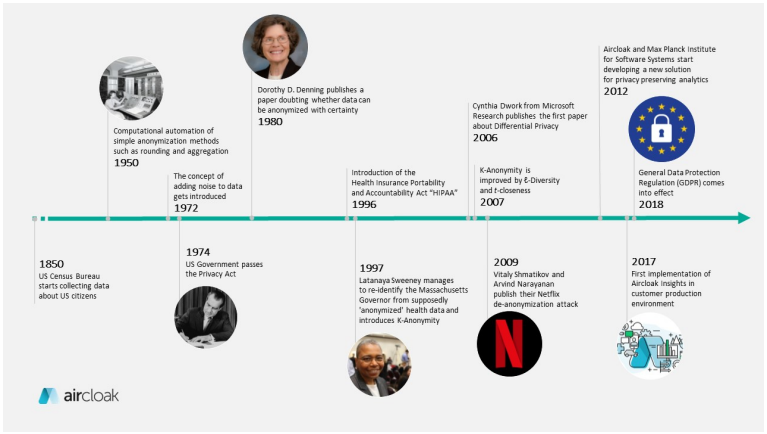
---, ---, House, Department of Justice. *Identity Theft*. *The United States Department of Justice*, 16 Nov. 2020, www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud. Accessed 21 Dec. 2022.

Additional Resources





According to a survey conducted by the Internet & American Life Project, Pew Research Center, a majority of its participants rely on the content of their email as the main source of privacy and importance. Furthermore, another survey conducted by the Pew Research Center shows that the strategies adopted by many people was to clear their cookies and browsing history.



The following timeline above provided by [Aircloak](), exhibits some important information regarding the evolution of anonymity. Furthermore, the website also provides some important information about the origin of data and data anonymization.