Forum: UNHRC

Issue: Evaluating potential human rights infringements by technological development.

Officer: Thomas Marteau

Table of Contents

Introduction

The technological advancement of the 21st century has revolutionized our lives; we can now communicate with AI, receive health advice, and even move around through AI. However, we must learn to balance emerging technologies such as AI and their gloomier impact on society's human rights. We must do so better and faster than during other technological revolutions. As we find ourselves at a crossroads, we must strive to develop, innovate and strengthen technology. However, human rights cannot be forgotten in their applications as their developers or users may have alternative motives.

From the creation of ARPANET to the development of Generative AI, technological development has at times failed to safeguard human rights. Governments and Multinational Corporations have financed and used unethical privacy and data management practices. The US is an example of how far population surveillance and control through user data can extend, as seen with the Patriot Act in 2001, in 2013 by Edward Snowden, and later by Meta Platform Inc.'s user data management.

The US also shares the spotlight with its BRICS trade partners: India, China, and Russia. These nations have not hesitated to implement biometric technology for "identification purposes only." However, their true intentions are unknown but presumed terrible. Research has found that they frequently violate human rights through perfidious practices like network traffic control and digital surveillance.

As we take our first steps in a world with emerging technology, action is required to make human rights the core or guide of technological development. Identifying solutions is necessary to keep up with technological developments. This report will cover possible solutions and information on the subject so that informed decisions and resolutions are made.

Definition of Key Terms

Human Rights

All human beings have rights simply because they are human beings, and these rights are universal and thus innate to all humans regardless of sex, nationality, ethnicity, and religion, and include the right to life, food, education, health, and liberty. The Universal Declaration of Human Rights (UDHR), passed in the UN General Assembly in 1948, serves as an assertion that defines our rights as beings. Human rights are not ratified by all states as the UDHR is not a legally binding document.

Technological Development

Technological development is the process of technological advancement, improvement, invention, and innovation. It is the cornerstone of most of evolutionary history. Homo Sapiens may not have survived were it not for technological development, as it would be unable to develop its neurological capabilities that development helps fully.

Artificial Intelligence

Artificial intelligence (AI) is a binary computer's ability to perform tasks associated with intelligent beings such as humans. Artificially intelligent computers have developed humane characteristics such as the ability to reason, learn, make decisions, problem-solve, and think critically. In an era of technological development, AI's potential threatens human rights due to its unpredictable capabilities and ability to be self-sufficient.

Digital Privacy

Digital privacy can be defined as the ability or the right of a person to keep their private information and data safe and undisclosed. Important data like names, addresses, banking details, and other sundry details should be secured to maintain privacy. Digital privacy is key to protecting humans from hackers who may, for example, sell their information to corporations.

Background Information

Historical context of technology and human rights

Since the Industrial Revolution onward, technological innovations and developments have increasingly clashed with protecting human rights. Over time, awareness and concerns about these rights have also dramatically increased. These worries have led to evaluating technological developments in terms of human rights within supranational institutions/structures like the UN and the EU.

The tremendous innovative leaps of the early 20th century, such amass communication through radio or television, could be used to suppress freedom of speech and information. It has led to deep polarization in politics and the spread of disinformation, however, without them there would clearly lack a medium of communication. In the late 1970s and early 1980s, developments such as the Global Positioning System (GPS) and the Personal Computer (PC) allowed governments to surveil their citizens digitally while pinpointing their location simultaneously. Still, they are now used by more than two-thirds of the world's population. The advancements of the late 20th and early 21st century—the invention of the internet and social media—have posed substantial privacy and security challenges that cannot be overlooked. Nevertheless, they have become so ingrained in society that we must work around the risks.

AI is growing exponentially as it revolutionizes healthcare, transportation, finance, and others. Efforts must be made to ensure the safe use of emerging technology, as its capabilities are potentially limitless. It is crucial to approach the risks of such developments with fundamental human rights in mind.

Undeniably, the Universal Declaration of Human Rights (UDHR) codified in 1948 has deterred some human rights violations—countless acts, treaties, and covenants have arisen from this text. Nevertheless, the technology of the 1940s is outdated compared to today's. That is why it is of the essence to create new and/or improved covenants that address the innovations of today and tomorrow.

The past decade: digital surveillance, data collection, and AI

In the last ten years, the world has seen a rise in digital surveillance and user data collection occurring through methods that infringe human privacy rights. A pronounced correlation and possible causation exists between technological development and human rights violations. Although some measures have been taken, technology actively outpaces legislation.

In 2013, Edward Snowden exposed the US government and their extensive secret surveillance programs on citizens around the world, to which the international community reacted negatively, condemning it as violating privacy rights.

Five years later, in 2018, the European Union (EU) pushed for data protection regulations, including the General Data Protection Regulation (GDPR), which was only ratified by the EU, leaving most citizens of the world still vulnerable to their respective government's unethical actions.

Despite the backlash, biometric data gathering and surveillance systems implemented post-COVID-19 pandemic have proven efficient in monitoring public health. However, many have pointed out that such tools could be used to violate human rights.

On the other hand, there are multinational corporations (MNCs), the “Big Tech” industry in the US faces scrutiny for weak privacy policies that allow them to monetize user data. These have become evident in recent cases where platforms and companies such as Meta Platforms Inc. have been involved in a controversy regarding advertisement targeting and content censorship—creating gray areas of human rights violations.

In recent years, gathering biometric data for identification and authentication has proven to pose new threats to human rights. However, nothing has been published to

expose abuses; remaining alert and planning for possible misuse of this technology is essential.

New technology is developed weekly; AI, surveillance, and data collection are constantly revolutionizing the tech industry. With strong regulation and government intervention, can extract the best of this technology while keeping away the damage to society's rights.

Lastly, in the upcoming US administration under Donald Trump, hateful speech may blur into freedom of expression. The president-elect plans to deregulate privacy guidelines that telecommunication companies must follow—social media included. Contradictingly, there is a great chance he will suppress the news media. This could threaten the human right to privacy, freedom of opinion, and freedom of expression. However, this is yet to happen, thus emphasizing the importance of intergovernmental organizations (IGOs) in protecting human rights worldwide.

Countries and Organizations Involved

People's Republic of China (PRC)

In recent years, The People's Republic of China (PRC) has headlined newspapers due to allegedly infringing human rights through technology, within and outside their borders. The PRC's treatment of the Uyghur ethnic and religious minority in the province of Xinjiang is a case study that highlights the government's use of advanced technology to hold on to political power. The Muslim Uyghur population has been subject to invasive surveillance through mobile applications and biometric data acquisition, which the use of AI systems has heavily facilitated. The Chinese Communist Party has used these surveillance methods to target and arrest members of this minority who are thought to be "untrustworthy" due to their religion and misalignment with the governing body. It is estimated that 13,000,000 Uyghurs [1] have been detained, indoctrinated, restricted and/or oppressed through processes that involve advanced technology. This infringes their right to privacy, religion, culture, and more. The PRC's lack of a free press has hidden various facets of these infringements from the public. To date, China has not been held accountable for its apparent genocide of the Uyghurs by any impactful means. As technology develops each day, ethnic minorities are prone to unjust treatment, not only in the PRC.

The Russian Federation (Russia)

Russia has been accused of using technology to violate human rights, focusing on surveillance, censorship, and repression of political opposition. The Kremlin has implemented facial recognition systems in public infrastructures in order to identify and detain citizens reported of participating in protests or inveighed against the government. This network has been successful in Moscow's Public Transport; it has led to the detention of many perpetrators. Moreover, President Vladimir Putin's "Sovereign Internet Act" has

[1] https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mas

permitted the implementation of technologies such as Deep Pocket Inspection Systems (DPIS) and Centralized Traffic Control Systems (CTCS). These allow the government to control internet traffic within its borders, which has restricted access to thousands of websites and platforms—such as Instagram, WhatsApp, and Twitter—labeled as "Western Propaganda." Many argue that Russia's use of such technologies violates its citizens' rights to expression, privacy, and movement.

United States of America (USA)

The September 11 attacks on the Twin Towers and the World Trade Center changed the course of modern history; some argue that they ignited the Global War on Terror in the Middle East and a domestic one in the US. The signing of the Patriot Act by President George W. Bush (a month after said attacks) permitted the government's use of surveillance techniques that have slowly eroded the human rights to privacy in the US. Surveillance systems have been used to target minorities—Muslims, immigrants, and activists—to facilitate detention.

Moreover, no legislative action against "Big Tech" Firms has been undertaken. Since the creation of social media platforms, their lack of moderation has permitted harmful, false, and violent content—as seen by Meta's involvement in Myanmar's Rohingya crisis.

In summary, it is indisputable that the US' technological advancements have significantly changed the world. However, legislation such as the Patriot Act threatens the right to privacy. The same can be said about the lack of measures taken to prevent "Big Tech" from violating the rights of citizens in and outside of the United States.

Human Rights Watch (HRW)

Human Rights Watch (HRW) is one of the world's largest non-governmental organizations (NGOs), it stands for human rights around the globe and identifies infringements of rights. As technology advances, HRW has been a key factor in ensuring human rights abuses do not go unnoticed. They have focused on surveillance, Artificial Intelligence (AI), censorship, and digital privacy—on whatever technology seems to threaten our universal rights. HRW actively promotes the passing and ratifying of laws on national levels that protect rights from significant technological advancement.

Timeline of events

1969	The launch of ARPANET, known as the beginning of our digital era, received early wariness regarding privacy violations through surveillance. Developed by the US Department of Defense, it is one of the building blocks of the internet of this day and age. Although its purpose was to transfer data between government institutions, it diverged into a tool for potentially unlawful data collection and surveillance.
1983	The inauguration of the Motorola DynaTAC 8000X as the first commercial mobile phone set the stage for concerns about location tracking privacy. However, being revolutionary greatly overshadowed dissent.
1991	The creation of the World Wide Web transformed data sharing; it allowed people around the globe to connect digitally, which many consider the most significant technological achievement of the 20th century. Some observe that it has brought the necessity for the protection of personal information as well as many other privacy concerns. Moreover, its creation has facilitated the development of the "Darkweb," which can offer services that violate Human Rights.
1999	With the development of browsers like Google, the search engine boom of the late 90s and early 2000s was a turning point for information access. However, it allowed businesses to collect data on tastes and preferences in quantities never done before. With it came monetizing user information, which allowed firms to influence consumers through personalized advertisements.
2001	The 9/11 attacks led to the codification of the Patriot Act, which aimed to detect terrorism plots against the USA, thus a counterterrorism measure. However, it gave the US Government legal permission to monitor digital communication systems. This raised obvious privacy concerns as the act did not limit surveillance to known terrorists but to anyone who might be—essentially, all US citizens could be monitored.
2007	The creation of the iPhone concerned many who advocated against user data, location, and communication collection. Again, it gave companies more control over consumers.

2013	Edward Snowden exposed the National Security Agency (NSA) and its widespread surveillance systems, revealing the US' domestic and international monitoring of digital communications, igniting accusations of human rights breaches.
2014	China creates its "Social Credit System," using AI and biometric data to monitor and rank the behavior of its citizens. It allowed the PRC to control Chinese citizens. It exemplified the dangers of technological advancement on individual rights, as citizens were now constantly under watch. Although voluntary, it deceived many who didn't see past its benefits, taking away the human right to freedom of movement and privacy.
2009 2016 **2018**	India implements the Biometric Identification system "Aadhaar." It has faced harsh social and legal criticism, with some arguing that the government may misuse the data for alternative motives. Debate sparked as it was deemed to violate the human right to privacy.
2020 2021 **2024**	The European Union (EU) proposed the Artificial Intelligence Act, which pushed for the regulation of AI due to the growing risks of its violation of human rights. It established guidelines for the safe use and development of AI in the EU by implementing stricter laws as the necessity for transparency in AI systems became apparent.
2025	The world is currently entering a new era of technological innovation, and the development of AI is growing by the day, specifically in the forms of Large Language Models (LLM) and Generative AI. On our current trajectory, it is likely to be an increasingly central part of our daily lives in the future. Its use can improve the lives of many; however, we must not disregard its dangers, as it can generate fake information and content. These concerns have been answered with new, stronger regulations for the use of AI, many believing that it will otherwise further violate human rights.

Relevant UN Treaties and Resolutions

Universal Declaration of Human Rights (UDHR) (1948)

The Universal Declaration of Human Rights (UDHR) is a document that defends humans' inalienable rights, declaring they should never be taken away. The United Nations General Assembly proclaimed this declaration on December 10, 1948: its purpose was to establish fundamental *universal* rights for all citizens in hopes that they protect all. The document cannot be ratified as it is not a treaty. Nevertheless, its creation has led to the implementation of binding covenants like the ICCPR, ICESCR, CERD, CEDAW, and the UNCRC

UN Human Rights Committee Resolution 42/15 (2019)

This resolution emphasizes the importance of privacy as technology develops, defending that individuals should not face unlawful interference in their privacy. Moreover, it urges states and businesses to consider human rights when developing new technology, addressing surveillance by calling for the importance of its use being ethical, legal, and responsible. It stresses protecting rights from data collection and processing systems. Therefore, it supports technological development as long as it respects the UDHR.

UN Human Rights Committee Resolution 32/13 (2016)

This resolution stresses the importance of "promotion, importance, and enjoyment of human rights on the internet" [2], pointing out that the same rights protected off the internet should be protected online—specifically, the freedom of expression. While it also urges digital literacy and the facilitation of online information, it mainly emphasizes approaching the expansion of internet access with measures in mind protecting human rights. Lastly, it hopes to replace violence, hate speech, and discrimination online with "tolerance and dialogue." [3]

UN Human Rights Committee Resolution 48/4 (2021)

This resolution again reaffirms the human right to privacy in a world of technology, highlighting the possible dangers of advancements in AI, surveillance, and biometric data-gathering systems, which, if unregulated, may violate our inalienable rights. In addition, it encourages member states to approve international laws regarding the use of surveillance technology. Lastly, it advocates against data misuse by states and governments in ways that may violate human rights.

[2] https://documents.un.org/doc/undoc/gen/g16/156/90/pdf/g1615690.pdf
[3] https://documents.un.org/doc/undoc/gen/g16/156/90/pdf/g1615690.pdf

Previous Attempts to Solve the Issue

United Nations (UN)

The UN has played a significant role by providing a platform for dialogue on the detection and accountability of human rights violations by countries and individuals, and has, to some extent, succeeded.

The UDHR outlines human rights and is a foundation for all solutions. However, its purpose was not solely for technological development-related human rights violations.

Resolutions such as UNHRC 42/15, 48/4, and 32/13 are modern attempts to address the issue at hand, unlike the UDHR. In a developing world, these resolutions have been guidelines for member states to follow.

European Union (EU)

The EU has passed important legislation that further improves the standards of all EU member states. In 2018, the General Data Protection Regulation (GDPR) was proposed to the EU, which has been passed by all member states and served as a general guideline on protecting user data and ensuring digital privacy. It has dramatically diminished the chances of violations occurring in the EU. It has also opened a gateway for similar acts around the world.

The Artificial Intelligence Act was enforced in May 2024 and set the groundwork for the development of AI algorithms with human rights in consideration. It also categorized the applications of AI into various risk levels, banning those at the highest level. While basic, it has ensured a plethora of human rights violations in the EU from occuring.

Canada

There are similarities regarding government approach between Canada and Europe, as evidenced by Canada turning The Directive on Automated Decision Making into law in April 2020. The Canadian government briefed on the directive that the state's use of AI fully complies with the ethical, legal, and procedural requirements. In doing so, Canada has ensured that AI and technological advancements in general do not infringe on the human rights of Canadian citizens; it demonstrates that a balance between accountability and development is attainable.

Possible Solutions

Delegates should keep in mind while drafting resolutions that the suggested solution has not been proposed before, is attainable and realistic within the boundaries of the UNHRC, and, ideally, that it has a chance of being approved by the UN Security Council (UNHRC resolutions are non-legally binding documents, the UNSC must pass them for them to be international law). With this in mind, possible solutions may be the following:

Establishing an International Body within the United Nations that would serve as a committee to tackle the dangers of technological development. This subgroup could address more than human rights and interlink with other committees. Its creation could bridge the Commission on Science and Technology for Development (CSTD) and the Human Rights Committee (UNHRC), creating a powerful body that could identify and hold accountable those who use technological development as a tool to violate our universal rights.

Developing and teaching evolving technology—such as AI—to recognize Human Rights. If the tool used to violate rights is created not to be able to do so, perhaps it can change our current uncertain path. This moderation could come in the form of guidelines and the detection of potential issues in the technology through international testing.

Harsh accountability standards should be created by ratifying national or international legislation that protects human rights from technological development. These laws could mark clear guidelines for using new technologies, emphasizing transparency in its development, and, more importantly, addressing penalties in the case rights are violated.

Bibliography

Copeland, BJ. “Artificial intelligence (AI) | Definition, Examples, Types, Applications, Companies, & Facts.” *Britannica*, https://www.britannica.com/technology/artificial-intelligence. Accessed 19 December 2024.

“The Core International Human Rights Treaties.” *OHCHR*, https://www.ohchr.org/sites/default/files/documents/publications/coretreatiesen.pdf. Accessed 2 January 2025.

“End Mass Surveillance Under the Patriot Act | American Civil Liberties Union.” *ACLU*, https://www.aclu.org/end-mass-surveillance-under-the-patriot-act. Accessed 3 January 2025.

“The future of technology: Lessons from China—and the US.” *Human Rights Watch*, https://www.hrw.org/news/2023/05/09/future-technology-lessons-china-and-us. Accessed 2 January 2025.

“How are today’s biggest tech trends affecting our human rights?” *World Economic Forum*, 11 December 2017, https://www.weforum.org/stories/2017/12/how-are-today-s-biggest-tech-trends-affecting-human-rights/. Accessed 23 December 2024.

“How Trump’s war on the media is expected to ramp up in his second term.” *The Conversation*, 20 November 2024,

https://theconversation.com/how-trumps-war-on-the-media-is-expected-to-ramp-up-in-his-second-term-243351. Accessed 3 January 2025.

"Human Rights and New Technology in Russia." *OVD-Info*, 17 May 2023, https://en.ovdinfo.org/human-rights-and-new-technology-russia#1. Accessed 2 January 2025.

"HUMAN RIGHTS RISKS IN TECH." *OHCHR*, https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/BTech-Institutional-Investor-Business-Models-Tool.pdf. Accessed 19 December 2024.

"The Impact of Digital Technology on Human Rights in Europe and Central Asia." *United Nations Development Programme*, 15 March 2023, https://www.undp.org/eurasia/publications/impact-digital-technology-human-rights-europe-and-central-asia. Accessed 23 December 2024.

Kanade, Vijay. "ARPANET Features and Importance | Spiceworks." *Spiceworks*, 5 July 2023, https://www.spiceworks.com/tech/networking/articles/what-is-arpanet/. Accessed 3 January 2025.

"Likely Trends in U.S. Tech and Media Regulation Under the New Trump Administration." *Covington*, 12 November 2024, https://www.insideglobaltech.com/2024/11/12/likely-trends-in-u-s-tech-and-media-regulation-under-the-new-trump-administration/. Accessed 3 January 2025.

"Mobile phone." *Wikipedia*, https://en.wikipedia.org/wiki/Mobile_phone#Restrictions. Accessed 3 January 2025.

"New report shows Facebook and Google's pervasive surveillance poses threat to human rights." *The Arab American News*, 26 November 2019, https://arabamericannews.com/2019/11/26/new-report-shows-facebook-and-google s-pervasive-surveillance-poses-threat-to-human-rights/. Accessed 3 January 2025.

"NSA surveillance exposed by Snowden ruled unlawful." *BBC*, 3 September 2020, https://www.bbc.com/news/technology-54013527. Accessed 3 January 2025.

Risse, Mathias, and Shoshana Zuboff. "Technology & Human Rights." *Harvard Kennedy School*, https://www.hks.harvard.edu/centers/carr/programs/technology-human-rights. Accessed 19 December 2024.

"RUSSIA 2023 HUMAN RIGHTS REPORT." *State Department*, 2023, https://www.state.gov/wp-content/uploads/2024/03/528267_RUSSIA-2023-HUMAN-RIGHTS-REPORT.pdf. Accessed 2 January 2025.

"A short history of the internet." *National Science and Media Museum*, 3 December 2020, https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-inte rnet#. Accessed 3 January 2025.

United Nations Human Rights Council. "A/HRC/RES/32/13." *UNDOCS*, 18 July 2016, https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F32%2F13&Lang uage=E&DeviceType=Desktop&LangRequested=False. Accessed 3 January 2025.

United Nations Human Rights Council. "A/HRC/RES/42/15." *UNDOCS*, 7 October 2019, https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F42%2F15&Lang uage=E&DeviceType=Desktop&LangRequested=False. Accessed 3 January 2025.

United Nations Human Rights Council. “A/HRC/RES/48/4.” *UNDOCS*, 13 October 2021, https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F48%2F4&Language=E&DeviceType=Desktop&LangRequested=False. Accessed 3 January 2025.

“US: Surveillance Practices Violate Rights.” *Human Rights Watch*, 12 March 2014, https://www.hrw.org/news/2014/03/12/us-surveillance-practices-violate-rights. Accessed 3 January 2025.

“What are human rights? | OHCHR.” *OHCHR*, https://www.ohchr.org/en/what-are-human-rights. Accessed 19 December 2024.

“What is GDPR, the EU’s new data protection law?” *GDPR*, 2018, https://gdpr.eu/what-is-gdpr/. Accessed 3 January 2025.