The Threat of Facial Recognition Technology

Anjali Mehta, University of Virginia, USA, anjali8203@gmail.com

Abstract

The rapid emergence of facial recognition technology (FRT) has caused significant concerns in terms of personal security and cybersecurity. As this technology continues to advance, it will pose serious challenges to individual liberties and human rights. For nation-states to keep up with the impacts of FRT, it is important for the United Nations to create a working group that can offer standards for FRT to ensure this technology is used ethically and responsibly per Sustainable Development Goals 5, 9, and 16.

Introduction

Facial recognition technology (FRT) is rapidly developing and gaining widespread use in recent years. Its ability to identify individuals has been used in various fields, from law enforcement and security to marketing and social media. While the technology has the potential to revolutionize these fields, there are also concerns about its impact on privacy and human rights.[1] It is crucial for the United Nations to focus on this issue and take action to address the risks posed by facial recognition technology.

One of the main concerns is the potential for the misuse of facial recognition technology by governments, corporations, or individuals due to the lack of regulations and standards.[2] The technology can be used to invade people's privacy by collecting and storing vast amounts of personal data without consent. This can lead to a range of negative consequences, including the creation of biased systems that unfairly target certain populations, the perpetuation of discrimination, and the violation of human rights. [3]

It is essential that the international community and members of the UN take action to address the issues caused by rapidly emerging facial recognition technology. This could include developing standards and regulations for the use of the technology, increasing public awareness about the risks and potential consequences of its use, and promoting transparency and accountability in the development and deployment of facial recognition systems, by allowing citizens a means to hold organizations responsible for abuse of power.

Issues Posed by Facial Recognition Technology

Facial recognition technology is used in a variety of settings, such as law enforcement, border control, advertising, access to finance, housing, and even in social media platforms.[2] While facial recognition technology has its advantages, such as enhanced security and convenience, it also poses a significant threat to privacy, human rights, civil liberties, and violates the UN's Sustainable Development Goals (SDGs), specifically goals 5, 9, and 16, detailed below.

Abuse by Government Bodies

One of the major concerns with FRT is its potential for abuse by governments and law enforcement agencies. Authorities can use facial recognition technology to identify and track individuals without their consent, which will lead to an increase in government surveillance, thereby eroding away personal privacy rights.[2] FRT also has the potential to be used as a tool for social control, particularly in authoritarian regimes. A significantly harmful example is when governments use FRT to monitor attendance at lawful protests, which raises serious concerns about the safety of those citizens.[7]

Risk of Gathering Biometric Data

Another concern is the potential for facial recognition technology to perpetuate existing biases and discrimination.[4] For example, the use of FRT by law enforcement has raised questions about how FRT is influenced by racial biases, as it has been observed that the technology is less accurate in identifying individuals with darker skin tones and women, which can lead to false identifications and wrongful arrests.[4] This issue leads to unjust targeting and profiling of marginalized groups.

The collection and use of biometric data is also a threat to individual privacy and security.[2] There exists a fundamental lack of consent and transparency when people are susceptible to facial recognition technology.

The use of facial recognition technology in public spaces, such as airports or shopping centers, can create a sense of constant surveillance and forced consent. The misuse of facial recognition data can also result in identity theft and other forms of cybercrime. [2]

Sustainable Development Goals

The threat of facial recognition technology is relevant to several of the UN Sustainable Development Goals (SDGs), particularly those related to human rights, equality, and innovation.

SDG 16

SDG 16 aims to promote peaceful and inclusive societies, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels.[6] The use of facial recognition technology can undermine these goals by enabling governments and other institutions to monitor individuals without their knowledge or consent, leading to a strain on individual freedoms. A major part of this is the lack of accountability on institutions that misuse FRT. There should be clear and transparent policies for how this technology is used in investigations and other law enforcement activities. Another way to improve accountability is by allowing citizens the right to challenge the misuse of this technology. [5]

SDG 5

SDG 5 aims to achieve gender equality and empower all women and girls.[6] However, facial recognition technology has been shown to have biases and inaccuracies, particularly when it comes to identifying people of color and women. This can perpetuate existing societal inequalities in areas such as employment, education, and law enforcement - which reinforces gender and racial biases. [4]

SDG 9

SDG 9 aims to build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation.[6] While facial recognition technology has the potential to improve security and reduce crime, it also poses significant threats to individual privacy and civil liberties. For example, FRT can be used to track an individual's movements, monitor their behavior, and collect sensitive information without consent. Therefore, it is important to ensure that innovation in this area is developed and implemented in a responsible manner that takes into account human rights considerations. This can be done by promoting transparency and working to ensure that individuals have control over their personal information.

Existing Policies

Existing legislation can be used as a baseline when developing policy regulations regarding facial recognition technology. Two such examples are the BIPA (Biometric Information Privacy Act), and the European Union's General Data Protection Regulation (GDPR).

The BIPA requires organizations to obtain informed consent from individuals before collecting their biometric data, and to disclose how this data will be used, stored, and shared. It also provides individuals with the right to sue organizations for violations of their biometric privacy. This encourages organizations to take their obligations seriously and ensures that individuals have a legal remedy if their rights are violated, ensuring that the technology is used in an ethical manner and that individuals are protected from potential harms from biased systems.[8]

The GDPR also mandates that organizations obtain informed consent before gathering biometric data and that the data be necessary and proportionate to the intended purpose. These principles could be applied by the UN to ensure that individuals have control over their biometric data.[9]

Policy Recommendations

UN bodies including ITU, UNESCO, and the OHCHR need to establish clear governing guidelines regarding the use of facial technology; they should coordinate to create a task force to review FRT and the potential of harm to SDGs 5, 9, and 16. The task force could offer guidelines on the collection, storage, and sharing of biometric data, as well as guidelines on how FRT can be used in law enforcement and global security contexts. This ensures accountability and transparency in how the technology will be used.

FRT needs to be designed so that the current biases and inaccuracies, specifically towards women and people of color, are eliminated. This can be done by promoting diversity in the development of this technology and by

conducting more research on gender and racial biases.[10] It is crucial to make data sharing more clear and transparent to protect individuals and build trust between individuals and the government.[2]

Governments and private companies should engage in public education and awareness campaigns to inform the public about the risks and benefits of facial recognition technology. Organizations that utilize FRT should be required to specify exactly what data is being collected, how it is being used (including whether that data is being shared with third parties or not), disclose how long the data is being retained, when it is being deleted, and how they can opt out of the data sharing process. [5]

One way the UN could address these issues is by establishing an expert panel on FRT to provide guidance on how to regulate its use. This panel could also conduct research on the impacts of facial recognition technology on privacy, human rights, and civil liberties and make recommendations for best practices for its use.

Conclusions

Given the potential risks and threats posed by facial recognition technology, it is crucial for the United Nations to take action to address this issue. The UN should focus on developing ethical guidelines and standards for the use of facial recognition technology to ensure that its use is transparent, accountable, and does not violate human rights. The UN should also advocate for increased regulation of facial recognition technology, particularly in the context of law enforcement, national security, and protecting privacy laws.

Acknowledgments

Thank you to Dr. Rider Foley at the University of Virginia and Bill Kelly for their guidance on this memo.

References

1. Ahmed, Hafiz Sheikh Adnan. "Facial Recognition Technology and Privacy Concerns." *ISACA*, 21 Dec. 2022, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns

2. Lively, Taylor Kay. "Facial Recognition in the US: Privacy Concerns and Legal Developments." *ASIS Homepage*, 1 Dec. 2021, https://www.asisonline.org/security-management-magazin e/monthly-issues/security-technology/archive/2021/decem ber/facial-recognition-in-the-us-privacy-concerns-and-legal- developments/.

3. Read, Jennifer. "Facial Recognition Technology: What Are the Benefits and Risks?" *EMSNow*, 16 Aug. 2022, https://www.emsnow.com/facial-recognition-technology-what-are-the-benefits-and-risks/.

4. Gargaro, David. "The Pros and Cons of Facial Recognition Technology." *IT PRO*, IT Pro, 13 Dec. 2022, https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology.

5. "Facial Recognition and Identity Risk." *Facial Recognition and Identity Risk | Equifax UK*, Equifax, https://www.equifax.co.uk/resources/identity-protection/facial-recognition-and-identity-risk.html.

6. "The 17 Goals | Sustainable Development." *United Nations*, United Nations, sdgs.un.org/goals.

7. "Lawmakers Need to Curb Face Recognition Searches by Police: ACLU." *American Civil Liberties Union*, 27 Feb. 2023, www.aclu.org/news/privacy-technology/lawmakers-need-curb-face-recognition-searches.

8. "An Overview of Illinois Biometric Information Privacy Act (BIPA)."*Securiti*, 28 Feb. 2023, securiti.ai/illinois-biometric-information-privacy-act-bipa/.

9. Service, Government Digital. "Data Protection: The Data Protection Act." *GOV.UK*, GOV.UK, 16 Sept. 2015, www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK%27s%20implementation%20of,used%20fairly%2C%20lawfully%20and%20transparently.

10. Lunter, Jan. "Beating the Bias in Facial Recognition Technology." *Biometric Technology Today*, Elsevier Ltd., Oct. 2020, www.ncbi.nlm.nih.gov/pmc/articles/PMC7575263/.