Navigating the Intersection of AI, Surveillance, and Privacy: A Global Perspective

Sarah Kasthuri Francis, University of Virginia School of Engineering and Applied Science, United States of America

Abstract

In 2019, at least 75 countries had employed Artificial Intelligence (AI) technologies for surveillance. This has sparked concern regarding the impact of these technologies on marginalized communities around the world. The reasoning behind why nations use these technologies and what measures are being taken globally to safeguard the rights and privacies of citizens has been analysed in this brief. The policy recommendation for the United Nations (UN) is for the UN High Commissioner for Human Rights to host a forum to support UN Sustainable Development Goal (SDG) 16.

Artificial Intelligence does not have a universally accepted definition but is understood to be the infusion of information into computer systems to create applications capable of learning from preexisting datasets to simulate and predict various scenarios (Filgueiras, 2023). AI is increasingly used in human-decision making processes. It uses both personal data and preexisting data sets to reach its conclusions. This means that AI systems perform only as accurately as the datasets they "learn" from. This causes problems for marginalized communities because they're not often included in the datasets these systems are being trained on (Fontes et al., 2022). These datasets can reflect the biases of its creators, leading to skewed AI performance and negatively affecting marginalized peoples. For example, if training data is biased, which is seen with facial recognition systems being predominantly trained on faces of white individuals, the conclusions drawn can be incorrect. This leads to increased misidentification of the faces of people of color (Denning, 2020). There are also privacy concerns surrounding how these systems are getting and distributing the private data they are using because the misuse or exploitation of private data poses significant risks to individual autonomy and freedom (Fontes et al., 2022).

Moving forward, looking at examples of AI surveillance techniques and their global prevalence, as of 2019, include (Feldstein 2019):

1) Smart Cities/ Safe Cities: Networks of sensors and cameras in urban centers focused on enhancing services and safety. 56 of the 75 countries using AI surveillance techniques use this.
2) Facial Recognition Systems (FRS): Camera-based identification that matches faces with stored images for various analytical purposes. 64 of the 75 countries using AI surveillance techniques use this.
3) Smart Policing: Analytical tools used in law enforcement to aid in investigations and predict potential crimes. 53 of the 75 countries using AI surveillance techniques use this.

The use of AI in surveillance raises ethical and privacy concerns surrounding the accuracy of its outputs because of the inherent biases the systems are trained on. These concerns have been validated by instances globally. In Australia, the Suspect Target Management Plan police initiative using smart policing was found to disproportionately target young Aboriginal and Torres Strait Islander people: "of the 73 children under the age of 16 identified as targets, 73% were indigenous, compared with national census data of 3.2%" (Cutts & Zalnieriute, 2022). In Rio de Janeiro, a smart city, cameras wrongly identified a woman as a criminal who was in the database of their local police. She was falsely arrested (Carvalho & Powell, 2022). These are two examples of many, reinforcing the fact that AI-driven technologies have a pattern of enhancing social divides and disparities, especially affecting historically marginalized groups (Hagerty & Rubinov, 2019). As such, in aim to promote SDG 16.b, "Promote and enforce non-discriminatory laws and policies for sustainable development," the reasoning behind why nations use these technologies and how they are regulated should be discussed amongst nations at a forum hosted by the UN High Commissioner for Human Rights (United Nations, 2016).

AI Surveillance: A Global Overview

Nations defend their use of AI surveillance with the stance of needing to protect national interests, which depending on the country, can include guarding against external threats as well as internal dissent. AI surveillance in democratic nations is frequently used to police borders, prevent crime, monitor public behaviour, and identify suspected terrorists. For example, on the U.S.-Mexico border, Israeli defense contractors have built, "dozens of towers in Arizona to spot people as far as 7.5 miles away," where this technology was initially perfected in Israel to build a "smart fence" to separate Jerusalem from the West Bank (Feldstein, 2019). Another example is France's Big Data of Public Tranquillity Project where in 2016, the goal

was to make the port city Marseille, "the first 'safe city' of France and Europe" by establishing a public surveillance network of nearly 1000 closed-circuit television (CCTV) cameras (Feldstein, 2019). From the perspective of governments, it can be seen why this technology is preferable: it reduces human operators which is cost effective, and it can cast a wider surveillance than traditional methods (Feldstein, 2019).

The likelihood of a government procuring AI surveillance is often correlated with its military spending. As of 2018, 40 of the top 50 military spending countries had AI surveillance technologies in place. These include countries of different government systems and economies, such as France, Germany, Japan, South Korea, Pakistan, Oman, Kazakhstan, Egypt, and many others, all with differing interests (Feldstein, 2019). This supports that the use of AI surveillance is not restricted to developed nations, and developing nations are also adopting these technologies, often supplied by Chinese companies (Hicks, 2022). It is the social and cultural makeup of an individual country that influences the impact these AI surveillance techniques will hold. However, amongst researchers, there is a collective understanding that AI will deepen social fractures in developing nations like in developed nations. In fact, it is a global phenomenon that lower- and middle-income countries might even be more susceptible to (Hagerty & Rubinov, 2019).

Legislative Landscapes for Data Privacy and AI

Globally, the legislative landscape for AI surveillance and privacy varies based on domestic and international interests.

In 2018, the European Union (EU) passed the General Data Protection Regulation (GDPR) which provides privacy and security protection of citizens' personal data. It mandates that personal data must be processed transparently and lawfully, requiring explicit consent for data processing from citizens and granting individuals the right to access, amend, and erase personal data. While the GDPR serves as a model for data privacy laws around the world, it does not prevent personal data collection as a practice overall, just regulates it (Almeida, 2022; Fontes et al., 2022; Human Research Protection Office, 2024). Then, in 2021, the EU established the AI Act. This was the world's first comprehensive AI law to regulate AI's development and use. Parliament's priority was to make EU AI systems "safe, transparent, traceable, non-discriminatory and environmentally friendly" (European Parliament, 2023; Fontes et al., 2022). The GDPR and AI Act demonstrate the EU's proactive commitment to protecting human rights, setting global benchmarks in AI and data ethics about compromised privacy.

In the United States, privacy laws vary by state. For example, in 2020, California passed the California Privacy Rights Act which established the California Privacy Protection Agency and extended the rights of residents regarding the collection and use of their personal information by businesses. Some cities in California such as Berkely and San Francisco have also banned the use of FRT (Almeida, 2022). While California is making strides, it is important to note that there is no federal legislation in the U.S. similar to the EU'S GDPR or AI Act which means there is no uniform standard for AI and privacy ethics across the country.

In 2021, China passed the Data Security Law to protect national security by placing guidelines on "national core data" which includes data concerning Chinese citizen's welfare, national security, economic interests, and public interest. China also passed the Personal Data Information Protection Law which is modelled after the EU's GDPR. This was China's first data protection law concerning personal data. It states that it has jurisdiction over all Chinese citizen data regardless of where it was collected (Fontes et al., 2022; Perez, 2022).

In South America, research shows that policy design dynamics regarding national strategies for AI in Argentina, Brazil, Chile, Columbia, Mexico, and Uruguay share similar objectives. These countries are not operating together. Rather, they have similar positions on AI legislation which have been analysed. Some include: (Filgueiras, 2023):

1) Budget and funding for structures for the industry
2) Research, and development; placing emphasis on facilitating AI applications in league with universities and research centers
3) Issue regulations about AI deployment and big data policy. The goal being to create data protection laws, privacy laws, and algorithm and autonomous agent regulation laws
4) Implement workforce training for those interacting with AI systems

Overall, countries around the world are in different stages of creating and implementing legislation surrounding AI and data privacy.

Policy Recommendation

The diverse legislative approaches to AI and data highlights that nations can learn from each other, especially when it comes to addressing marginalized populations. With countries at varying stages of income and development experiencing these problems, a

platform for international dialogue and cooperation amongst these nations is crucial. The goal being to safeguard the rights and privacy of all peoples globally. In response, the policy recommendation is to convene a forum hosted by the UN High Commissioner for Human rights with key governments at the forefront of AI technology development like the United States, China, and members of the EU and other AI experts like Joy Buolamwini, the founder of the Algorithmic Justice League, and representatives from leading AI companies like Google and Microsoft. This will allow nations to examine and address the patchwork of legislative actions that currently exist. The goals of this forum include:

5) Stakeholders will discuss the direct harms of the intersection between AI-generated surveillance technologies with the decrease in data privacy.
6) Stakeholders will discuss how these harms are being avoided by different practices and legislation worldwide.
7) Stakeholders will discuss how to regulate AI systems to not widen social divides and infringe on human rights.

These goals coincide with UN SDG 16 to promote non-biased laws and policies for sustainable development. This recommendation has policy reform, technological accountability, and global cooperation working in unison to preserve human rights.

References

Almeida, D., Shmarko, K. & Lomas, E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI Ethics* 2, 377–387 (2022). https://doi-org.proxy1.library.virginia.edu/10.1007/s43681-021-00077-w

Carvalho, Fernanda Catao de, and Igor Baden Powell. "Brazilian Cities and Facial Recognition: A Threat to Privacy." *Fordham Urban Law Journal*, news.law.fordham.edu/fulj/2022/01/06/brazilian-cities-and-facial-recognition-a-threat-to-privacy/. Accessed 01 Mar. 2024.

Cutts, Tatiana and Zalnieriute, Monika, and. "How AI and new technologies reinforce systemic racism." *54th Session of the United Nations Human Rights Council, United Nations Office at Geneva, Geneva, 3rd oct* (2022).

Denning, Peter J., and Dorothy E. Denning. "Dilemmas of Artificial Intelligence." *Communications of the ACM*, vol. 63, no. 3, Mar. 2020, pp. 22-24 *EBSCOhost*, https://doi.org/10.1145/3379920

European Parliament. "EU AI Act: First Regulation on Artificial Intelligence: Topics: European Parliament." www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. (2023) Accessed 01 Mar. 2024.

Feldstein, Steven. *The global expansion of AI surveillance*. Vol. 17. Washington, DC: Carnegie Endowment for International Peace, 2019.

Filgueiras, F. (2023). Designing artificial intelligence policy: Comparing design spaces in Latin America. *Latin American Policy*, 14, 5–21. https://doi-org.proxy1.library.virginia.edu/10.1111/lamp.12282

Fontes, Catarina, et al. "AI-powered public surveillance systems: why we (might) need them and how we want them." *Technology in Society* 71 (2022): 102137.

United Nations "Goal 16 | Department of Economic and Social Affairs" sdgs.un.org/goals/goal16#targets_and_indicators. (2016) Accessed 01 Mar. 2024.

Hagerty, Alexa, and Igor Rubinov. "Global AI ethics: a review of the social impacts and ethical implications of artificial intelligence." *arXiv preprint arXiv:1907.07892* (2019).

Hicks, Jacqueline. "Export of Digital Surveillance Technologies from China to Developing Countries." (2022).

Perez, Christian. "Why China's New Data Security Law Is a Warning for the Future of Data Governance." *Foreign Policy*, Foreign Policy Magazine, 28 Jan. 2022, foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy/. Accessed 01 Mar. 2024.

Human Research Protection Office. "The European Union (EU) General Data Protection Regulation (GDPR)", www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr. (2024) Accessed 01 Mar. 2024.