AI Surveillance: Examining its Current and Future Impacts on Individual Privacy

Alomiri Mohammed, Aquino-Ellul Pavlos, Edy Antoine, Mandy James, Sanjeevvijay Kirishoban

1. Abstract

This paper dives into how privacy laws are changing worldwide, thanks to new technological advancements that make spying on private data easier. Europe's General Data Protection Regulation (GDPR) effective from 2018 has been very serious about violators, and the protection of individual privacy while enforcing transparency [7].

Urgently upgrading rules and policies is essential in AI and privacy. The lack of transparency in AI decision-making poses concerns for privacy and fairness. This paper advocates for an ethical AI system aligned with evolving laws to balance AI's advantages with privacy respect [9].

2. Introduction

Privacy is very important in our data-driven world, especially with the fast development of AI technologies. AI's significant potential, combined with large amounts of data, comes with a high risk of how data might be misused or lead to heavy surveillance, which can be a significant risk to individual privacy. Global events like the COVID-19 pandemic have led to greater government surveillance for public safety, making us question the balance between our privacy and the use of AI to address the needs of public safety. This complex landscape gets even trickier with political shifts and businesses' involvement in how personal data is used. These factors show how important this topic is, touching on our basic human rights and how privacy is changing in a world that's under more surveillance and powered by more advanced technologies.

The main aim of this essay is to critically analyze the impact of AI and surveillance technologies on privacy, as well as develop a comprehensive understanding of the potential risks. This entailed examining global privacy regulations, assessing their ethical impact on data collection, and exploring the influence of AI on individual privacy. Objectives encompassed evaluating ethical aspects of surveillance, probing the evolution of surveillance practices, scrutinizing legal frameworks, and proposing strategies to balance AI innovation, surveillance, and privacy protection.

3. Research Methodology

Privacy being the focus of this essay, we decided to take a qualitative approach to our research. This meant that we focused on text resources, in order to understand existing concepts. It consisted of gathering information about case studies (examples that support these concerns), analyzing already placed laws regarding the regulation of AI in society concerning privacy, comparing these regulatory frameworks across regions and finally analyzing the ethical aspect of AI-powered systems that may invade our privacy.

4. Background

4.1. How does AI impact surveillance methods

The AIGS Index delineates three crucial AI surveillance tools: smart/safe city platforms, facial recognition systems, and smart policing. These tools manifest diversely, showcasing high technical sophistication and ongoing evolution. For instance, in addition to facial recognition, there are advancements in speech and gait recognition. Regardless of their specific applications, state authorities perceive numerous benefits in these systems: cost-effectiveness, decreased dependency on human labor, meticulous data analysis, and, on a larger scale, unparalleled capabilities for societal oversight.

These surveillance tools are not necessarily unlawful or unethical by design; for example, the same AI surveillance tools that could be used on the battlefield or for identifying criminals could also be utilized for wildlife preservation. [6]

4.2. Privacy during the COVID-19 and lack of transparency

The COVID-19 pandemic was a particularly interesting time during which a global move was made toward authoritarianism in the name of public safety. Data tracking via smartphones gave governments unprecedented tools to combat the pandemic. Some countries being more lenient regarding information gathered, minimized the leaked information, while China used advanced tracking during the pandemic without consideration for personal information [11] even as to passing a security law, allowing greater

surveillance [5,10]. Globally, the pandemic response is fast-tracking the growth of the surveillance state, especially in authoritarian regimes, where emergency measures are leveraged to expand surveillance capabilities [11].

Snowden's 2013 revelations unveiled extensive collaboration between governments and corporations to gather data on both citizens and non-citizens, involving email and more [3]. It prompted limited policy changes aimed at reinforcing the legal justifications for surveilling citizens. However, there remains a lack of substantial privacy protections for non-citizens under surveillance [4].

4.3. The Current State of International Privacy Laws

Privacy protections for non-citizens are an important factor to account for when taking into consideration the diversity in legal infrastructure between different nations around the world. EU prioritizes a 'human-centered approach' regarding AI and digital initiatives; the High-Level Expert Group on AI issued ethics guidelines for trustworthy AI that advocate for AI to be lawful and ethical as well as emphasizing the differentiation between individual identification versus tracing [1]. On the other hand, more authoritarian states put less importance on individual liberty and instead focus on establishing control under the namesake of mass security; China being one of them [6].

Different jurisdictions have different standards for privacy which is problematic particularly when considering non-citizens of a particular nation. In this sense, nations around the world seem to fall short of addressing the global trend toward digital authoritarianism.

4.4. Regional vs. International Laws

The focus on domestic surveillance laws overlooks the global nature of modern surveillance practices and cross-border surveillance is increasingly common. However, regulations governing such practices lag behind. [2]

Snowden's leaks underscore the urgent need for a global legal framework safeguarding human rights and privacy, particularly for non-citizens facing foreign surveillance. Emphasizing the necessity for comprehensive global privacy regulations before widespread AI implementation across diverse jurisdictions is crucial.

However, unlike other transnational issues that have been addressed through shared responsibility frameworks in international agreements, surveillance lacks similar cooperation between governments. Surveillance is rather intangible and often doesn't cause immediately recognizable harm, reducing the incentive for states to limit these activities. The perceived benefits for national security outweigh the costs, hindering cooperation to regulate surveillance practices at an international level. [10]

The UN Human Rights Council proposed the "International Principles on the Application of Human Rights to Communications Surveillance" in 2014, outlining principles such as surveillance needing a legitimate aim. However, even this seemingly obvious principle's lack of enforcement and incentives hinder widespread adoption.

Fortunately, pressures—political, rights-driven (from UN resolutions), and economic (from tech companies that fear being associated with a lack of privacy)—are challenging the norm of unfettered mass surveillance. The Snowden revelations accelerated these pressures but didn't lead to lasting changes in international law. Regardless, the Snowden leaks demonstrate the significance of how transparency can change public opinion and the laws that will subsequently be put in place.

5. Discussion

The momentum of the increasing use of AI in surveillance amplifies concerns regarding potential abuses and infringements upon privacy rights. As such, it becomes crucial to proactively establish robust laws and regulations governing AI-based surveillance to curtail misuse and protect individuals' fundamental right to privacy. Without these preemptive measures, there is a heightened risk of unchecked surveillance practices that could significantly compromise personal freedoms and civil liberties.

Clearly, then, the integration of AI into surveillance demands preemptive planning and stringent regulations to prevent potential misuse of data and violations of individuals' privacy rights. [10]

Certain suggestions can be made to not only improve the legal AI-privacy chaos but also to protect individual rights independently of the region. AI companies should adopt a human-rights-based approach to AI system design, promoting human dignity and providing compensation for any violation. This is important to apply on a global scale to provide uniformity regarding privacy laws, a 'golden standard', which will help to avoid regional misuse of AI surveillance technologies. For example, the GDPR's 'privacy-by-design' [8] and 'privacy-by-default' could be implemented by the US Department of Defence as well, safeguarding individuals by making user privacy the 'norm' of any AI system.

In the inevitable case that companies attempt to push these guidelines, a 'privacy impact assessment' system should be put in place to automatically check and produce a risk score for the privacy violation. Implementing AI systems with a focus on transparency ensures that users are informed about how their data is collected and processed, while accountability ensures that those who have control or influence over the system are responsible and liable for its output. If systems were designed with these in mind, user opinion of AI would likely see a positive shift, and the sys-

tems would be less likely to violate user privacy. If the right to individual privacy is put at the centre of how AI is regulated, and these standards are upheld through thoughtful and up-to-date policies, many of the discussed privacy risks may be mitigated going forward.

As for government entities, the most ideal (yet elusive) solution regarding AI and privacy-related laws would involve an international regulatory framework that is enforced by multiple global bodies of power including the UN. The laws should insight transparency regarding data collection and usage (the importance of which has been highlighted clearly by whistle-blowers such as Edward Snowden). Although this could prove to be a great stride forward for protecting the privacy of non-citizens, it would likely not be plausible to come to a consensus between the majority of governments around the world on regulating surveillance within their regions of power.

Regardless, fostering conversations about AI's usage in privacy to generate urgency in the matter of international private data collection and processing is a step in the right direction that will hopefully lead to a future international treaty being signed emphasizing the right to privacy from mass surveillance AI tools.

6. Conclusion

The integration of AI into surveillance poses significant challenges to privacy rights, necessitating urgent global regulations. The diverse legal landscape worldwide complicates matters, urging the establishment of standardized AI-privacy norms. Proposing a human-centric AI approach, including automated breach detection, aims to enhance transparency and protect against ethical bias. Active pursuit is crucial to shape international surveillance law, minimize government discretion, and ensure equal treatment of citizens and non-citizens. Crafting effective global standards is paramount for safeguarding human rights and privacy amid evolving technological capabilities [10].

References

[1] Ethics guidelines for trustworthy ai. 2

[2] Is freedom from cross-border surveillance a human right? 2

[3] Edward snowden: the whistleblower behind the nsa surveillance revelations, Jun 2013. 2

[4] Edward snowden: the whistleblower behind the nsa surveillance revelations, Jun 2013. 2

[5] Hong kong national security law: What is it and is it worrying?, Jun 2022. 2

[6] Cbranley. The west, china, and ai surveillance, Dec 2020. 1, 2

[7] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council. 1

[8] Karl Manheim and Lyric Kaplan. Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law and Technology*, 21:106, 2018. 2

[9] Rajan Rayhan and Shahana Rayhan. *AI and Human Rights: Balancing Innovation and Privacy in the Digital Age*. PhD thesis, 07 2023. 1

[10] Will Schrepferman. Supervising surveillance: International law and the surveillance state, Nov 2020. 2, 3

[11] Andy Wang. Authoritarianism in the time of covid, May 2020. 1, 2