PRIVACY IMPLICATIONS OF AI-BASED SURVEILLANCE TECHNOLOGIES: A REVISED PANOPTICON

Anushree Raman, Reva University

ABSTRACT

This article examines the complex interplay between customary behaviour and developments in technology within today's surveillance systems, centring on privacy concerns associated with AI-driven surveillance mechanisms. The research makes sense how big data analyses and AI algorithms have transformed the methodologies concentrating on the panopticon model developed by Michel Foucault which describes disciplinary power. Privacy concerns are on the rise due to advancements in technology and the decreasing costs for businesses to use smart monitoring systems. It's important for stakeholders to carefully consider the potential for misuse when it comes to Surveillance Analytics (SA) innovations. To help balance privacy implications and related issues stemming from the adoption of SA, a two-by-two Monitoring, Security, Privacy and Ethical Decision (SPED) Process Guide suggests reviewing key terms and ethical frameworks. The guide recommends using three ethical frameworks – Consequence, Duty, and Virtue – in one or more cases. In the SPED matrix, an organization's level of SA sophistication is shown on the vertical axis, while its current privacy level is evaluated on the horizontal axis. The matrix assesses the existing level of privacy and the rights granted for the surveillance targets, as well as the sophistication of the organization's SA. The suggested decision process guide can be used by senior managers and technicians to determine whether adopting SA is the right move.

Introduction

One of the big concerns with AI technologies is privacy. However, when it comes to philosophical or legal discussions, the meaning of "privacy" is pretty tricky. There's no clear agreement on what it really means. Some philosophers have called it a "concept in disarray"[1], while others have compared it to navigating an "unknown swamp"[2] in a more poetic way. Some even argue that there's no universal definition of privacy[3] . Because of this, privacy concerns are often vague and not well-defined, which makes it hard to address them and figure out how AI technologies might or might not put people's interests at risk. This article aims to highlight important differences and explain how they connect to worries about the risks linked to AIrelated technologies.

It's a common misunderstanding that privacy only involves controlling information about yourself, like stopping others from getting or using that info without permission. Some experts have questioned this idea[4]. While we won't delve deep into it here, we believe it's wrong to think that a lack of control means a lack of privacy. Understanding this involves shedding light on often overlooked aspects of privacy, such as the role of entities that understand meanings[5]

Theoretical Background

The concept of a transpersonal judicial system traces back to the ideas of English philosopher, sociologist, and lawyer Jeremy Bentham.[6] His influential work "Panopticon, or Supervisory House," written between 1786 and 1787 and expanded upon in 1791, is a must-read for anyone interested in this concept.[7] This paper delves into the impact of Bentham's "panopticism" theory on prison architecture, global penitentiary systems, and the proliferation of dystopian narratives centred on constant surveillance. The concept was further explored by Michel Foucault. Although Foucault's idea is important, this article mainly looks at where Bentham might have

[1] Solove, Daniel J., Understanding Privacy. Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008, GWU Legal Studies Research Paper No. 420, GWU Law School Public Law Research Paper No. 420, Available at SSRN: https://ssrn.com/abstract=1127888
[2] Julie C Inness., Privacy, Intimacy, and Isolation., Oxford University Press, 1992
[3] https://www.researchgate.net/publication/280292851_Privacy
[4] Macnish, K. (2017). The Ethics of Surveillance: An Introduction (1st ed.). Routledge. https://doi.org/10.4324/9781315162867
[5] https://www.researchgate.net/publication/359948856_AI_Technologies_Privacy_and_Security
[6] The Contradictions of Jeremy Bentham's Panopticon Penitentiary, Journal of Bentham Studies 2007
[7] https://www.researchgate.net/publication/363902010_JEREMY_BENTHAM'S_PANOPTICON_AND_ITS_POSSIBLE_ORIGINS

gotten his inspiration.[8] It suggests that Bentham could have been influenced by the English legal system, particularly the practices from the 16th and 17th centuries. During that time, English courts used methods similar to "watching," which is a key aspect of the "panopticism" theory. This emphasis on surveillance was apparent during the witch trials in the English Kingdom and is documented in various legal records. Though not distinctly referenced in "Panopticon" Bentham's explicit lexicon and conceptualization suggest a robust reliance on legal precedents. English ones that is. This claim springs from the contents of the text. Subsequently, the evidence seems to highlight Bentham's inspirations though they are not overtly expressed. Bentham's major influence seems to be the legal system.[9] That is the English system particularly. Specifically, the system that was prevalent in the early Modern era.

Foucault and other social scientists along with architectural historians have illuminated the significance of Bentham's Panopticon in an engrossing manner.[10] They envision it as a model for new supervisory power that extended beyond just prisons. Also this model took in varied nineteenth-century institutions. Factories, schools hospitals and barracks were among these establishments. Foucault underscored the extensive use of the Panopticon's architectural design in the construction of prisons. This was especially true in the 1830s. Moreover, he asserted that its persistent popularity for close to two centuries testifies to its inventive potency.[11]

Foucault argued that the Panopticon in its essence, spans broader societal spectrums than mere physical structures. He highlighted that the panoptic paradigm hinges on continuous observation. It could be applied any time when it is essential to enforce rules. Control of behaviour among a group of people is also possible.

This flexible nature of the scheme underscores its profound effect. It has shaped social and institutional arrangements over time. Bentham's conceptualization is still pertinent today. Revisionist historians such as Foucault "and others connect the prison system with the emergence of the entire apparatus of social power that developed as a reaction to the

[8] Light and Power: The Panopticon as a Political Form and its Variations, 2020 Svyatoslav Kaspe
[9] https://www.researchgate.net/publication/330908954_Bentham_A_Guide_for_the_Perplexed
[10] M. Foucault, Surveiller et Punir: Naissance de la Prison , Paris, 1975; trans. as A. Sheridan, Discipline and Punish: The Birth of the Prison , London, 1977
[11] Foucault,Discipline and Punish,p. 249

requirements of the emerging commercial capitalist society," according to Janet Semple, the author of the only the monograph on the Panopticon.[12]

Privacy concerns in AI based Surveillance

Striving for equilibrium between safeguarding privacy rights and the perks of exploiting advanced surveillance technologies suggests pursuing a mutually advantageous resolution amidst competing interests. This systematic procedure involves identifying the possible degree of privacy rights that may need to be surrendered to realize the supposed benefits of adopting specific surveillance analytics solutions. It accepts that people's right to privacy has boundaries. Some advancements in surveillance can lead to positive societal change. These should be considered.

Sableman (2014) confirmed a crucial point in the development of privacy policy.[13] It requires a balancing act. Personal privacy is violated in some form by virtually every facet of modern life. This highlights the immense challenge in managing privacy issues. The difficulty is more apparent in the backdrop of swiftly evolving technology scenarios.

In today's context notably in 2024, stakeholders are urged to prioritize achieving balance. They must do this before deploying tools like video surveillance. The emphasis placed on this balance underlines the import of observing implications. These implications are associated with surveillance techniques and individual privacy rights. They also relate to larger social good.[14]

Through mindful consideration stakeholders can use the potential benefits of surveillance technologies responsibly. Simultaneously, they are also part of a mission; promoting trust. They work to enhance accountability as well.[14]

In surveillance analytics "balance" doesn't necessarily equate to sacrificing privacy for the advantages of these innovations. Nor does it involve relinquishing our rights to privacy. The use of surveillance analytics does not fundamentally clash with privacy rights. It's cultural

[12] Semple,Bentham's Prison,p. 152.
[13] Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. Journal of Applied Psychology, 86(4), 797–804. https://doi.org/10.1037/0021-9010.86.4.797 [14] Andrejevic, M. (2019). Automating surveillance. Surveillance & Society, 17(1/2), 7–13. https://doi.org/10.24908/ss.v17i1/2.12930
[14] Campbell, C. (2019). "'The entire system is designed to suppress us.' What the Chinese surveillance state means for the rest of the world," Time. https://time.com/5735411/CHINA-SURVEILLANCE-PRIVACYISSUES

norms, trust levels and history of privacy violations that determine balance perception in surveillance subjects. [15] This insight comes from Luppicini & So's work in 2016.

However, Moosavian in 2016 issued a caution about potential mishandling of private information. This warning originates from the metaphor of balance. He discusses that the pros of security analytics breakthroughs can be quantified.[16] Yet, they might not genuinely equate to the damage produced by privacy invasions. Invasions lead to reductions in privacy. This underscores how challenging it is to achieve true balance. The central issue here is about using surveillance technologies for security.

Rights to privacy

The concepts of privacy and rights associated with privacy are complex. They are open to various interpretations. These are often reliant on the country's legal system where surveillance takes place. "Freedom from unauthorized intrusion and the state or characteristic of being separate from company or observation" is a common definition of privacy (Merriam Webster 2020). Privacy according to the International Association of Privacy Professionals (IAPP, 2020) is "the freedom from interference or intrusion. It is also the right to be left alone". This right extends to a degree of control over the collection. Use of your private data is what we call "information privacy".[17]

According to some definitions, privacy is the capacity to manage personal information[18] (Bélanger et al., 2002; Stone et al., 1983). According to Clarke (1999), people frequently view privacy as a moral and legal right.[19] Individual privacy is a broad concept that includes the following dimensions: data, location and space, personal behaviour, communication, privacy of the person, privacy of thoughts and feelings[20] . In addition, privacy may mean keeping some actions and details private and avoiding publicity, particularly when it comes to private

[15]https://www.researchgate.net/publication/299604066_A_Technoethical_Review_of_Commercial_Drone_Use_in_the_Context_of_Governance_Ethics_and_Privacy
[16] Moosavian, R (2016) Jigsaws and Curiosities: The Unintended Consequences of Misuse of Private Information Injunctions. Communications Law, 21 (4). pp. 104-114. ISSN 1746-7616
[17] Driver, J. (2011). *Consequentialism*. ISBN 9780415772587. Routledge.
[18] Bélanger, France, and Robert E. Crossler. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." MIS Quarterly, vol. 35, no. 4, 2011, pp. 1017–41. JSTOR, https://doi.org/10.2307/41409971. Accessed 14 May 2024.
[19] https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology
[20]https://www.researchgate.net/publication/351384025_Balancing_privacy_rights_and_surveillance_analytics_a_decision_process_guide

matters.[21] All things considered, privacy includes a broad range of elements pertaining to personal autonomy, control over personal information, and immunity from unwanted observation or intrusion.

According to P. M. Schwartz (1994), privacy rights include the notion that information pertaining to an individual should be protected from public view.[23] Warren et al. (1890) conducted a thorough analysis of common law, the US Constitution, and laws related to the right to privacy in a seminal work.[22] The foundational article shaped subsequently discussions and debates on the subject by providing a framework to comprehend and understanding privacy rights within legal frameworks.

The Impact of AI on Surveillance and Monitoring

Artificial intelligence technology is used in AI surveillance to track and evaluate human behaviour for a variety of purposes, including marketing, law enforcement, and security. It filters through large data sets using sophisticated algorithms and machine learning techniques to find trends or abnormalities in human behaviour.[23]

Protecting Privacy in AI Surveillance

Even though AI surveillance has many potential advantages, like improved security and customized services, it also raises serious issues with civil liberties, ethics, and privacy. Because AI surveillance technology gathers and analyses personal data without explicit consent, it may infringe people's rights to privacy and autonomy. In a democratic society, protecting people's right to privacy is essential because it allows them to keep control over the information that about them, as well as to maintain their independence and autonomy. AI surveillance's extensive data collection and analysis has the potential to violate these fundamental rights.[26]

[21] Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. Journal of Social Issues, 33(3), 102–115. https://doi.org/10.1111/j.1540-4560.1977.tb01885.x [23] Schwartz, Paul M., Property, Privacy, and Personal Data. Available at SSRN: https://ssrn.com/abstract=721642

[22] Warren, Samuel; Brandeis, Louis (December 15, 1890). "The Right to Privacy". Harvard Law Review. IV (5): 193–220. Retrieved 4 June 2021 – via Internet Archive.

[23] https://www.linkedin.com/pulse/ethics-ai-surveillance-balancing-security-privacy-aiethics-spair--sc2pe [26] https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-andchallenges/

Bias and Discrimination in AI Surveillance

The possibility of prejudice and discrimination is a fundamental worry in the field of AI surveillance. These systems' underlying algorithms run the risk of sustaining previous prejudices and discriminatory tendencies if they are trained on biased or incomplete datasets. One prominent example can be found in facial recognition systems, which have shown increased error rates when attempting to identify women or people with darker skin tones. This gap may result in the unfair targeting or characterization of particular demographic groups, which would exacerbate already-existing disparities in society. Therefore, in our increasingly digital world, it is crucial to address prejudice and bias in AI surveillance in order to guarantee equal consideration and adhere to fundamental principles of justice and fairness.[24]

Enhancing Surveillance with AI Technology

Recently, there has been a revolutionary change brought about by the incorporation of artificial intelligence (AI) technology, especially in integrated security systems. As a result of this progress, advanced clever structure and behavioural recognition capabilities have been developed. Furthermore, the development of AI-enhanced robots and drones has greatly expanded the reach and efficacy of security systems, making it possible to monitor campus activities more thoroughly and identify suspicious activity with greater accuracy than in the past. Convolutional neural networks (CNNs), which are used in video surveillance AI for analyzing and interpreting visual imagery, are a crucial part of this development. Through the use of algorithms for deep learning, the system continuously picks up new skills from an extensive library of video footage, improving its dependability and accuracy over time. In the end, this dynamic adaptation strengthens the entire safety infrastructure and capabilities by enabling more accurate and responsive surveillance measures.[25]

Emerging Technologies and Solutions for AI Privacy

- Privacy Enhancing Technologies (PETs) - In the era of artificial intelligence, privacy enhancing technologies, or PETs, are crucial for protecting data privacy. Federated

[24] https://www.forbes.com/sites/forbestechcouncil/2024/02/02/artificial-intelligence-the-new-eyes-ofsurveillance/
[25] https://www.asisonline.org/security-management-magazine/monthly-issues/securitytechnology/archive/2024/april/Addressing-Ethical-and-Privacy-Issues-with-Physical-Security-And-AI/

learning, differential privacy, and homomorphic encryption are some of these techniques.[26] By enabling model training without centralized data aggregation, allowing computations on encrypted data, and adding noise to query responses, they safeguard personal data during processing and analysis.[27] By integrating PETs into AI systems, privacy is protected and confidence in data-driven procedures is increased.[28]

- Homomorphic Encryption and Federated Learning - During the artificial intelligence training process, homomorphic encryption provides a safe way to execute calculations on encrypted data while maintaining its confidentiality. This offers a robust barrier against possible breaches of data by enabling AI models to be learned without requiring access to actual, unencrypted data.[29] Federated learning, on the other hand, shares only model updates rather than raw data, decentralizing the processing of information by training AI models promptly on users' devices. This strategy reduces the risks associated with concentrated data storage while also improving privacy.[30]

- Differential Privacy - Differential privacy allows for precise aggregate data analysis, but it also introduces random noise into data sets, making it challenging to identify individual entries. By ensuring that the results of AI remain essentially the same regardless of whether a particular person's data is included or not, this technique protects individual privacy.[31]

- Enhancing Data Security and Minimizing Bias - Putting in place good data hygiene procedures is essential to enhancing privacy in AI. This entails gathering just the kinds of data that are required, storing them safely, and getting rid of them as soon as they are no longer required. Fairness amongst various user groups can be promoted by reducing algorithmic bias through the use of inclusive and large-scale datasets.[32]

- Transparent AI Practices and Regular Audits - Building trust requires open AI practices and frequent audits. Users are reassured about the safety of their data by regular

[26] https://mostly.ai/blog/what-are-privacy-enhancing-technologies
[27] https://www.linkedin.com/pulse/ai-driven-privacy-enhancing-technologies-pets-clarifying-misconceptions
[28] https://research.aimultiple.com/privacy-enhancing-technologies/
[29] https://privacera.com/blog/6-ways-to-preserve-privacy-in-artificial-intelligence/
[30] https://www.walkme.com/blog/privacy-concerns-with-ai/
[31] https://www.itmagination.com/blog/ai-solutions-and-privacy-overcoming-common-challenges-committingto-responsible-ai
[32] https://www.trigyn.com/insights/ai-and-privacy-risks-challenges-and-solutions

evaluations of AI systems and models to verify compliance with confidentiality requirements and by the open disclosure of these practices.[33]

- Synthetic Data and Secure Multi-Party Computation - Privacy Enhancing Technologies (PETs) such as secure multi-party computation and synthetic data generation are becoming increasingly important. Without jeopardizing individual privacy, synthetic data makes it possible to create datasets that are statistically similar. [34]Secure multiparty computation is a useful tool in collaborative environments that prioritize data privacy, as it permits multiple parties to process encrypted data without disclosing the underlying data.

- Addressing the Challenges of Advanced AI Technologies - With the development of AI technologies, it is critical to address privacy issues raised by complex systems such as large language models (LLMs) and generative AI.[35] Combating potential privacy risks requires integrating strong privacy-preserving strategies from the beginning and making sure that regulations and ethical standards are followed.

Future of AI Privacy: Trends and Predictions

Emergence of Explainable AI (XAI): XAI is anticipated to be a key component in promoting transparency, ensuring fairness, and demystifying AI decision-making procedures in a variety of applications, including digital platform content prioritization and loan approvals.[36]

Decentralized Data Management: A move toward decentralized data management has been predicted, giving people control over their personal information via tools like decentralized platforms and personal data vaults, improving privacy without sacrificing the usefulness of the data.

Developments in Privacy-Enhancing Computation (PEC): PEC methods like federated learning and secure multi-party computation will allow AI to operate on data without disclosing the raw

[33] https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world/
[34] https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information
[35] https://www.augusta.edu/online/blog/ai-privacy-guide
[36] https://secureprivacy.ai/blog/navigating-data-privacy-2024

data, enabling cooperative AI projects and lowering privacy concerns.[37]

Regulatory Developments: It is anticipated that regional data privacy laws will gradually become more uniform, impacting cross-border data privacy management and placing a strong emphasis on ethical AI practices and accountability.

Ethical AI Integration: With an emphasis on bias reduction, ethical data collection, and empowering user control over personal data, ethical principles are being progressively incorporated into AI development processes.[41]

AI for Improving Privacy: Artificial Intelligence technologies are used to improve privacy protections through advancements like fraud detection systems and AI-driven anonymization tools, in addition to being used as possible threats to privacy.[38]

Constant Development of Data Protection Law: In order to meet the challenges presented by artificial intelligence (AI), data protection law is always changing.[39] One such change is the requirement for thorough governance procedures in order to properly regulate AI systems.

Handling Algorithmic Decision-Making: In order to prevent discriminatory outcomes and guarantee fairness, future privacy laws are anticipated to concentrate on regulating algorithmic decision-making. This will strike an appropriate equilibrium between the individual privacy and AI innovation.

Opportunities and Difficulties in AI Regulation: Developing legislation that both fosters innovation and addresses the intricacies of AI is a challenge for legislators. In order to create legislative frameworks that strike a balance between safeguarding privacy and AI advancement, stakeholder dialogue is essential.[40]

Conclusion

A crucial area of concern in the midst of artificial intelligence's (AI) widespread spread across surveillance and common technologies is the intersection of privacy, ethics, and regulation.

[37] https://www.forbes.com/sites/forbestechcouncil/2024/01/29/five-data-privacy-trends-to-watch-in-2024/ [41] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m02/privacy-governance-and-ai-global-trendson-data.html
[38] https://infotrust.com/articles/emerging-data-privacy-trends-for-2024/
[39] https://hai.stanford.edu/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world
[40] https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf

The various ramifications that AI's integration into everyday life has, from the technical complexities of gathering and analysing data to the wider societal ramifications of increased surveillance, have been thoroughly explored in this article. It emphasizes the precarious balance that must exist between the advancement of technology and the protection of individual freedoms. The discussion has emphasized how important it is to have ethical discussions, open methods, and strong laws to help create an era where AI enhances privacy rather than violates it. As we move forward, it is critical that we direct additional research and efforts toward enhancing AI's privacy-preserving capabilities while also working to guarantee equity and reduce biases in AI algorithms. An ongoing conversation between technologists, legislators, and the general public should support these efforts by creating an atmosphere that is favourable to forming new innovations in order to effectively protect human dignity and privacy rights. In order to ensure that privacy and moral issues stay at the centre of this technological advancement, we must all work together to craft AI technologies that value the best possible outcomes for humanity.