International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI and Privacy: Ethical Concerns in Data Collection and Surveillance

Rishab Debnath[1], Vaishnav Veeraraghavan P[2], Nikita Hapse[3]

[1,2,3]D Y Patil International University Pune, Maharashtra

Abstract

Artificial Intelligence (AI) has evolved the process of data collection and surveillance, which could lead to a breach in privacy. But as this technology gains a foothold in both private and public sectors, the lines around best practices for using personal information are getting blurry. This paper examines the ethics of AI for data collection and surveillance, namely considering questions like informed consent, transparency but observes there are few debates about how such systems might be abused in state or corporate surveillance. This study aims to address this tension between technological innovation and individual privacy rights by conducting a broad analysis of literature in technology, as well by analysing current frameworks from the legal perspective. The results of this study suggest that privacy tends to take a backseat when compared with security requirements, and hence AI builders and policy makers should work together in developing strong effective privacy measures. The conversation also delves into the larger implications of AI surveillance for individual freedom and communal trust, suggesting measures to accommodate ethical deployments in future.

Keywords: Artificial Intelligence, Ethics, Privacy, Data Collection, Surveillance, AI Governance

INTRODUCTION

If anything, privacy is one of the most intractable wor- ries with the extraordinarily fast-paced expansion Artificial Intelligence (AI) solutions. With the rapid adoption of AI systems in various aspects of everyday life, ranging from online services that have more and more capability to cater specifically to our personal preferences, through to city scale surveillance networks these privacy considerations are being stretched. Clarifying what privacy will mean in the age of AI has proven more elusive, though. Privacy is classically described as a concept in disarray (Solove 2008, p.) and after some years of philosophical legal reflection the picture we get from literature shows precisely such fragmentation. The lack of consensus makes it challenging to define a unified perspective in discussing implications on privacy, and the corresponding ethical protections that should be adopted.

At the core of this debate is the notion of ”control” over personal information—traditionally seen as essential to privacy. The ability to prevent unauthorized access or use of one’s data is often presented as a fundamental right. However, privacy concerns extend beyond simple control, encompassing deeper issues related to individual autonomy and identity. As AI systems collect, analyze, and leverage vast amounts of personal data, they can influence decisions that affect people’s lives, such as credit eligibility, job opportunities, and even personal freedoms. This raises critical questions about how much control individuals truly have over their data and how AI-driven decisions can lead to unintended harms. This paper examines the ethical implications of AI in data collection and surveillance, focusing on

how privacy is impacted by the widespread use of these technologies. By exploring the intersection of privacy, consent, and control, this study seeks to uncover the broader ethical challenges posed by AI surveillance and its potential consequences on human rights. Through this exploration, we aim to provide insights into how AI technologies can be regulated to protect privacy and uphold ethical standards in a rapidly evolving digital world.

LITERATURE REVIEW: PRIVACY AND ITS ETHICAL IMPLICATIONS IN THE AGE OF AI

There has been much discussion among academics on the concept of privacy, with different meanings and interpretations depending on the context. Differentiating privacy from other related issues like security or autonomy is one of the main obstacles when talking about privacy. This section examines the body of research on privacy, paying special attention to ”informational privacy”—the control people have over the gathering and use of their personal data—and how it relates to surveillance systems and artificial intelligence.

A. *Definitions of Privacy and Informational Privacy*

The phrase ”privacy” frequently describes a person’s right to shield their personal data from unwanted access. But privacy has several facets, and how it is interpreted differs depending on the situation. For instance, Solove (2008) highlights the difficulty of defining privacy in a way that is widely accepted by characterising it as a ”concept in disarray” [6]. Although this concept has also been contested, Parent (1983) contends that privacy should be interpreted as the individual’s right to control personal information [5]. Doyle (2009) presents the idea of a ”perfect voyeur,” describing situations in which privacy may be jeopardised even in cases when no malicious use of the information is made [1].

When discussing privacy in the context of artificial in- telligence, ”informational privacy,” or the safeguarding of
personal data, is frequently used. This idea was developed in part by Feldman (1994), Velleman (2001), and Shoemaker (2010), who emphasised the significance of protecting per- sonal information in a world where surveillance technologies facilitate the collection and analysis of enormous volumes of data by corporations and governments [9]. Information privacy security is more important than ever because AI technologies are making it easier to obtain information.

B. *Privacy as Control over Information*

One widely held belief in the literature is that people’s control over their personal data is related to privacy. The main goal of privacy interests, according to Menges (forthcoming), is to keep anyone from obtaining personal information without permission [9]. The idea of ”persona-building,” which was first proposed by Johnson (1989) and Marmor (2015), supports the idea of privacy as control by implying that people choose which parts of themselves to disclose in order to establish and preserve particular views [5].

Artificial intelligence (AI) systems have the ability to gather data in ways that are opaque and challenging for people to comprehend, let alone manage. AI technologies collect personal data without express consent, whether through data mining, facial recognition, or online behaviour tracking [6]. Since people might not be aware of how their data is being used or shared, this loss of control over personal data has significant ramifications for individual autonomy and dignity. According to Soifer and Elliott (2014), AI technologies have the potential to worsen this issue by extending the scope and size of data collecting beyond conventional bounds [7].

C. ***Security Interests and Privacy Violations***

The difference between privacy loss and privacy violation is another important topic in privacy literature. Unintentional exposure of personal information (such as when someone is accidentally spotted in public) results in privacy loss, whereas intentional attempts to get private information without consent are referred to as privacy violations (Parent, 1983) [5]. In AI applications, where extensive data collection frequently makes it difficult to distinguish between unintentional exposure and deliberate monitoring, this distinction is crucial [4].

Additionally, the literature makes a distinction between se- curity and privacy considerations. According to Doyle (2009), ”security interests” refer to safeguarding people against poten- tial harm, including financial theft or stalking, that could arise from unauthorised access to their personal data [6]. This is different from ”privacy per se,” which describes the intrinsic value people have on limiting the amount of information that others know about them, even when that information does not directly cause harm. Marmor (2015) elaborates on this by contending that people’s ”security interests” in protect- ing information are not limited to preventing harm because illegal surveillance itself can erode personal liberty and self- determination [9].

D. ***Epistemic Privilege and Persona-Building***

”Epistemic privilege,” the notion that people typically know more about themselves than others, is a key element of privacy theory [7]. This enables people to selectively disclose personal information about themselves in order to create their public personas [9]. Because it gives people control over how others see them, this epistemic privilege forms the basis for privacy in conventional contexts [5].

But as AI develops, this privilege is being challenged more and more. Real-time data collection and analysis by AI systems is possible, frequently without the subject’s awareness or consent. According to Feldman (1994), AI surveillance undermines people’s autonomy by endangering their capacity to curate their own image and manage how others see them [9]. As a result, ”persona-building,” a crucial component of individual autonomy and identity development, is undermined [3].

E. ***The Feedback Loop and Autonomy***

Another critical concept in privacy theory is the ”feedback loop,” wherein individuals adjust their self-presentation based on the reactions of others [8]. This iterative process allows people to refine their self-understanding and develop their autonomy [5]. AI complicates this feedback loop by collecting and analyzing information on a scale that individuals cannot perceive or control. Mokrosinska (2018) notes that when AI surveillance becomes pervasive, individuals may lose the ability to gauge how others perceive them, thereby stunting their personal development and autonomy [10].

F. ***Impact of AI on Privacy and Ethical Concerns***

The expanding use of AI in data collecting and monitoring raises a number of ethical issues, which are highlighted in the literature on AI and privacy [2]. According to Menges (forthcoming) and Shoemaker (2010), the extensive use of AI technology for surveillance runs the risk of establishing a ”panoptic society” in which people are continuously watched [3]. Because people may change their behaviour out of fear of being watched, this surveillance puts both privacy and human autonomy at risk [5].

Furthermore, research indicates that marginalised communi- ties are disproportionately impacted by AI surveillance, which raises questions of social justice and discrimination [10]. According to Marmor (2015), AI-driven surveillance systems have the potential to worsen already-existing disparities by giving particular groups more attention than others, increasing the likelihood that vulnerable

populations' privacy would be violated [9].

METHODOLOGY

A. *Data Collection*

On March 9th, 2024, we conducted a systematic search in the SCOPUS database to collect relevant literature pertaining to artificial intelligence and surveillance. The search param- eters were set to include the terms "artificial intelligence" AND "surveillance," specifically within the abstract, title, and keywords of the documents. We limited our study to publications in the disciplines of social sciences and humani- ties, intentionally omitting review articles. Furthermore, only articles, conference papers, books, and book chapters written in English were included in our analysis, with no additional restrictions imposed.

This initial search yielded a total of 293 documents. After screening the titles and abstracts, we excluded 14 papers deemed irrelevant to our study. Consequently, we performed a detailed topic modeling analysis on the remaining 279 publications.

B. *Analytical Techniques*

To identify the most influential scholarly topics related to our research question, we employed keyword co-occurrence analysis, a bibliometric technique widely recognized for its ability to ascertain the structure of research and its academic relevance. Following this, we conducted a comprehensive content analysis of the relevant publications to complement our bibliometric findings.

The analysis involved the following key steps:

- **Keyword Co-occurrence Analysis:** Using VOSviewer software, we analyzed and visualized the networks formed by keywords to identify significant research themes. We represented the items based on their total link strength (TLS) score, which reflects the quantity and strength of connections among various topics. Ad- ditionally, we utilized the modularity algorithm to reveal strongly related keywords and understand the strength of these research networks.
- **Content Analysis:** We conducted a qualitative exami- nation of the 279 publications, categorizing them into thematic clusters derived from the bibliometric analysis. This process aimed to delve deeper into the context and implications of the findings related to AI and privacy.
- **Visualization:** The results of our analysis were displayed in two formats: one based on modularity to showcase the themes identified and another utilizing overlay visualiza- tion to illustrate the evolution of keywords over time.

C. *Model Development and Ethical Considerations*

Upon gathering and analyzing the relevant data, we pro- ceeded to consider the ethical implications in the development of AI models related to surveillance. Our approach follows best practices aimed at ensuring that AI models are safe, effective, interpretable, and equitable:

- **Safety and Efficacy:** We acknowledge the responsibility of developers to create AI models that are tailored to specific tasks and informed by input from domain ex- perts. This ensures models perform effectively in real- world contexts. Moreover, we emphasize the need for generalizability across diverse populations and clinical environments.
- **User Autonomy:** It is crucial that AI models promote shared decision-making between users and clinicians. Therefore, we advocate for transparency regarding the intended uses and accuracy of AI models to enable informed discussions between clinicians and patients.
- **Fairness:** We recognize the importance of procedural and substantive fairness in AI models. Our

methodol- ogy includes efforts to address biases that may emerge from the training data, ensuring equitable treatment of subgroups within populations. This involves examining the implications of sensitive attributes, such as race and gender, in model training and application.

D. *Tools Utilized*

The primary tool employed for data visualization and analysis was VOSviewer, a renowned software for analyzing and visualizing scientific literature, enabling us to trace the evolution and knowledge structure of our research topics.

RESULTS

A. *Sector-wise Adoption of AI in Data Collection and Surveil- lance*

Table 1 presents an overview of the adoption of AI technolo- gies across various sectors, highlighting the prevalent privacy concerns, regulatory levels, and transparency practices.

TABLE I SECTOR-WISE ADOPTION OF AI IN DATA COLLECTION AND SURVEILLANCE

Sector	AI Usage	Privacy Concerns	Transparency
Gov/Public	High	Informed Consent	Medium
Healthcare	Moderate	Data Sensitivity	High
Finance	High	Consumer Consent	High
Retail	High	Data Exploitation	Low
Tech	Very High	Algorithmic Opacity	Low

B. *AI Surveillance and Legal Frameworks*

As illustrated in the following table, there is a significant disparity in the development of legal frameworks surrounding AI-based data surveillance across different regions. Many existing laws are outdated, lacking the necessary specificity to address the complexities of advanced AI systems.

TABLE II AI SURVEILLANCE REGULATIONS AND PRIVACY PROTECTIONS

Region	AI Surveillance Regulations	Privacy Protec- tions	State Involve- ment
United States	Developing	Moderate	High
European Union	Strong	Strong	Low
China	Weak	Low	High
India	Weak	Low	Moderate

C. *Keyword Co-occurrence Analysis*

The co-occurrence analysis of keywords led to the identi- fication of seven main scholarly subjects related to AI and privacy concerns.

- **Public Health Surveillance:** This topic encompasses the privacy implications of contact tracing applications, particularly during the COVID-19 pandemic. The ethical concerns focus on informed consent and the potential misuse of health data.
- **Video Surveillance and Facial Recognition:** Predomi- nantly discussed in the transportation

industry, this area highlights the balance between security measures and individual privacy rights, raising concerns about state surveillance and data collection without consent.

- **Military Surveillance:** This subject addresses the de- ployment of AI in military applications, including drones and autonomous vehicles, emphasizing ethical consider- ations related to privacy and the use of force.
- **Surveillance Capitalism and Disease Surveillance:** The relationship between economic incentives and surveil- lance practices reveals how personal data is commodified, raising ethical questions about consent and data owner- ship.
- **Smart Cities:** The integration of AI in urban planning and management raises privacy issues related to data collection from various sensors and surveillance systems, necessitating a focus on transparency and public account- ability.
- **Computational Surveillance:** This topic examines the implications of data analytics and machine learning on surveillance practices, highlighting the need for robust ethical guidelines to safeguard individual rights.
- **Security Surveillance:** The ethical considerations of using AI for security purposes encompass debates on privacy rights versus public safety, requiring a nuanced approach to regulation and oversight.

D. *Overlapping Themes and Ethical Considerations*

It is noteworthy that many of the identified topics overlap in their discussions. For instance, public health surveillance and disease surveillance share contentious ethical issues but differ in focus; disease surveillance primarily addresses state and citizen surveillance concerns, while public health surveillance emphasizes privacy and consent issues.

E. *Additional Findings*

In addition to the sector-specific concerns and legal frame- works, our analysis revealed that:

- The rapid advancement of AI technologies often outpaces the development of corresponding regulations, leading to potential exploitation of personal data and erosion of privacy rights.
- Stakeholders in various sectors must adopt transparent practices to foster trust and accountability in AI systems.
- There is a growing recognition of the need for interdisci- plinary collaboration among technologists, ethicists, and policymakers to create comprehensive frameworks that address the ethical implications of AI surveillance.

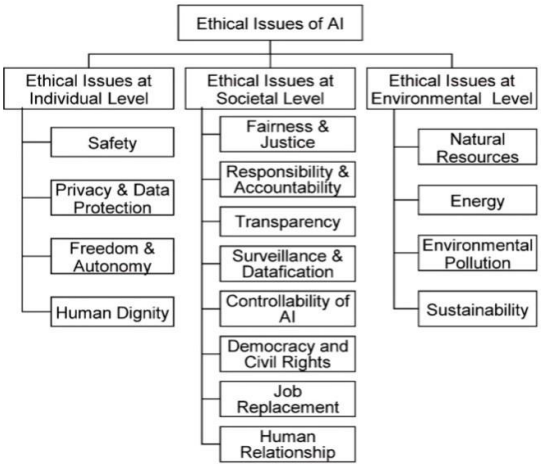

Fig. 1. Proposed categorization of AI ethical issues.

CONCLUSION

In conclusion, our study has demonstrated that while AI technologies offer significant advancements in data collection and surveillance, they also raise complex ethical concerns regarding privacy and security. AI systems have the capacity to access and process vast amounts of personal data, which amplifies risks associated with privacy violations and unau- thorized data usage. Although AI lacks the inherent ability to form perceptions or intentions, the data it processes can be exploited by human actors or other systems, posing substantial threats to individual privacy and security.

The findings indicate that there is a nuanced distinction between privacy and security risks in AI systems. While AI systems themselves may not directly threaten privacy by forming perceptions, they can indirectly contribute to privacy breaches when data is misused or accessed by third parties. This, in turn, may compromise individual autonomy and iden- tity, as control over personal information becomes increasingly difficult to maintain.

Moving forward, there is a pressing need for clearer regu- lations and frameworks that address both privacy and security concerns. Future research should explore more comprehensive methods of safeguarding personal data, and further investiga- tion is necessary to balance the benefits of AI surveillance with ethical responsibilities. Stakeholder involvement, including policymakers and the general public, will be critical in shaping responsible AI practices that protect privacy while enabling innovation.

ACKNOWLEDGMENT

We would like to express our gratitude to all those who have contributed to the completion of this research. We extend our sincere thanks to D Y Patil International University, Pune for providing us access to essential resources and data.

Special thanks to our colleagues and advisors for their valuable insights and constructive feedback throughout the research process. Finally, we acknowledge the support of our families and friends, whose encouragement and patience made this work possible.

REFERENCES

1. T. Gillespie, ”Platforms are not intermediaries,” Georgetown Law Tech- nology Review, vol. 2, no. 2, pp. 198-216, 2018.
2. R. Clarke, ”Privacy and AI: The challenges of privacy law and AI systems,” Journal of Information Technology and Politics, vol. 17, no. 3, pp. 234-256, 2020. doi: 10.1080/19331681.2020.1773651.
3. K. Crawford and R. Calo, ”There is a blind spot in AI research,” Nature, vol. 538, pp. 311-313, 2016. doi: 10.1038/538311a.
4. D. Leslie, ”Understanding AI ethics and safety,” Alan Turing Institute, 2019. [Online]. Available: https://www.turing.ac.uk/research/publications/understanding-ai-ethics- and-safety.
5. M. O’Neil, ”AI and the future of privacy: An exploration of the implications,” European Data Protection Law Review, vol. 5, no. 4, pp. 341-359, 2019.
6. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 1st ed. New York, NY, USA: PublicAffairs, 2019.
7. European Parliament, ”Artificial Intelligence: Challenges for EU Cit- izens and Privacy Rights,” European Parliamentary Research Service, PE 654.170, 2021.

8. N. Bostrom and E. Yudkowsky, ”The Ethics of Artificial Intelligence,” in Cambridge Handbook of Artificial Intelligence, W. Ramsey and K. Frankish, Eds. Cambridge, UK: Cambridge University Press, 2014, pp. 316-334.
9. P. Schiffner, J. Bennet, and C. Santos, ”Ethical implications of AI- powered surveillance systems,” Journal of Surveillance Studies, vol. 12, no. 1, pp. 45-63, 2020.
10. Rieke, M. Robinson, and A. Yu, ”Civil rights, privacy, and artificial intelligence: A matter of trust,” Upturn, 2018. [Online]. Available: https://www.upturn.org/reports/2020/civil-rights-privacy-ai/