

**LAW653 – AI, LAW AND ETHICS**

Assignment 2:

Q4: AI Surveillance: Balancing Safety and Ethics

Submitted by:

Melvin Ong You Le

G1

**Introduction**

In an era defined by rapid technological advancements, Artificial Intelligence (AI) surveillance emerges a hallmark innovation, shaping societal paradigms. This powerful tool, like a double-edged sword, offers promises of unprecedented security while raising questions of privacy concerns. As these digital eyes proliferate across various cities, they not only bolster public safety and national security but also entangle a web of ethical, legal and societal boundaries that necessitates scrutiny. While the potential of AI to deter crime is undeniable, the prospect of individual privacy erosion and the rise of a surveillance state cannot be ignored. Moreover, the balance between collective security and individual freedom becomes increasingly uncertain. This essay delves into the landscape of AI surveillance, exploring its benefits and drawbacks. Considering real world applications, ethical theories, and legal perspectives, we aim to understand its benefits and challenges and propose viable strategies to manage the risks, striving to strike a balance between security and liberty in this modern society.

**Background on AI Surveillance**

Before delving into the intricacies of AI surveillance, it’s important to first understand its fundamental aspects and global uses. At its core, AI surveillance encapsulates the deployment of automated processes and algorithms to analyze, recognize and interpret data, which is mostly collected through video cameras, sensors, and digital platforms (Sadowski, 2019). Leveraging technologies like facial recognition, behavior analysis and anomaly detection, AI surveillance transcends traditional security mechanisms, autonomously detecting potential threats and in the process, creates a pervasive monitoring system (Feldstein, 2019).

On the global stage, both government and private companies have adopted AI surveillance, applying it in areas ranging from crime deterrence and crowd control to health monitoring, a utility that was notably evident during the COVID-19 response (Barroca, n.d.). Countries like China and US stand out, not only using AI surveillance for security purposes but also for broader social governance and policy enforcement (Sophos News, 2019).

In this landscape, AI surveillance becomes a potent tool, simultaneously praised for its ability to enhance safety, and critiqued for its ability to intrude upon civil liberties. As this essay progresses, a deeper dive into these applications reveals the varying nature of AI surveillance, paving the way for a detailed and careful examination of its ethical, social, and legal aspects in the sections that follow.

**Benefits of AI Surveillance**

To fully understand the vast scope of AI surveillance, it’s essential to recognize the advantages it offers, especially concerning public safety, national security, and operational efficiency.

1. Public Safety and Crime Prevention

AI surveillance has materialized as an important tool in reducing criminal activity and enhancing public safety, with various cities witnessing a decrease in crime rates after its implementation. For instance, New York city observed a significant decline in criminal incidents following the adoption of the Domain Awareness System, a robust AI-powered surveillance network that facilitates real time crime data analysis and predictive policing (Levine et al., 2017). Similarly in Annapolis, Maryland, the employment of AI surveillance in the form of facial recognition has aided police in assisting a person who was attempting suicide (Parker, 2020). Also in UK, the use of facial recognition by convenience store operator Co-op has diverted 3,000 incidents of thefts in the span of 18 months (Burgess, 2020).

1. Enhanced National Security

On a national level, AI surveillance stands out as a critical asset in bolstering national security, particularly in contexts of counter terrorism and border control. US, through its Automated Targeting System, employs AI surveillance to scrutinize travelers and cargo at borders, identifying potential threats and preventing illicit activities (The Straits Times, 2023). Furthermore, AI surveillance can also be used to predict terrorist operations based on communication data, financial transaction information and travel patters which is used to develop models that predict the location and timing of terrorist attacks (Islamic Military Counter Terrorism Coalition, 2020).

1. Operational Efficiency

AI surveillance is not just a tool of safety, but it also enhances operational efficiency, particularly evident in settings like airports and public venues. For example, Tokyo’s Haneda Airport leverages AI surveillance to streamline passenger flow and optimize resource allocation, thereby improving operational efficiency and passenger experience (Ellichipuram, 2021). Furthermore, during large scale public events such as the Super Bowl in the US, AI surveillance is employed to monitor crowd dynamics, ensuring optimal allocation of security resource, and facilitating efficient emergency responses when necessary (Freiburger, 2020). Thus, beyond mere security, AI surveillance can be pivotal in optimizing operations and resource management in various public settings.

**Drawbacks of AI Surveillance**

While AI surveillance brings notable benefits, it also introduces significant downsides that complicate the discussion. Specifically, the clear issues of privacy invasion and potential misuses of the technology cannot be ignored and required thorough examination.

1. Privacy Invasion

Even with its wide reaching protective capabilities, AI surveillance consistently invades personal privacy, becoming entangled in the private lives of those it observes. The omnipresence of surveillance cameras, equipped with AI capabilities like facial recognition, means that individuals will be tracked wherever they are and leaves no room for anonymity (Lively, 2021). The constant surveillance alters the very fabric of daily life, casting a shadow of doubt over our sense of individuality and freedom. Such widespread monitoring blurs the lines between public interest and private intrusion, causing many to question if we are silently trading our personal freedoms for the illusion of security. In the current world, the age-old maxim of “watching the watchmen” takes on a renewed significance, as society grapples with the consequences of its technological choices.

1. Potential Misuse

Furthermore, the technological prowess of AI surveillance doesn’t solely reside in benevolent hands and is susceptible to misuse, especially with authoritarian regimes. The case of Uyghur Muslims in Xinjiang, China provides a sobering example of how state-level AI surveillance can be used for mass surveillance and oppression (Feldstein, 2022). The surveillance cameras constantly monitors and collects data on the Uyghur population, combining technology with harsh method to control the minority group. Similarly in Russia, facial recognition technology has been deployed to quash dissent and to identify and subsequently detain protestors and opposition figures, thereby supressing democratic expressions and civil liberties (Masri, 2023). These instances show how AI surveillance can be weaponized to fortify authoritarian groups, suppress dissent, and perpetrate wide-scale human rights violations.

1. Psychological and Societal Implications

The omnipresence of AI surveillance not only affects our physical actions but also impacts the mental well-being and societal dynamics of the observed people. The consistent feeling of being watched can induce anxiety, stress and changes in behaviour (Trainor, 2021). Such ever-present monitoring creates a society where genuine expressions and interactions are curtailed for fear of misinterpretation by the unblinking electronic eyes. This continuous oversight can potentially suppress the richness of societal diversity, stifle creativity, and hinder the evolution of open societies.

Comparing theses drawbacks with the earlier mentioned benefits of AI surveillance requires a thorough look into the mix of ethical, legal, and social impacts. The following sections will explore this complex area more, looking at possible ways to balance the good and bad aspects, and exploring useful approaches that might find a stable middle ground between advancing technology and protecting human rights.

**Legal and Ethical Perspectives**

***Existing Legal Frameworks***

Across the globe, nations have initiated legislative actions to combat the rise of unregulated surveillance. The European Union’s General Data Protection Regulation (GDPR) stands out as benchmark. Implemented in 2018, GDPR focuses on the rights of individuals over their data, offering robust protection against unauthorized data processing and guaranteeing rights like ‘right to be forgotten’ measures (European Data Protection Supervisor, n.d.). While it sets a precedent, the constantly evolving nature of AI surveillance challenges the efficiency and comprehensiveness of even such advanced legal frameworks.

In Singapore, the Model Artificial Intelligence Governance Framework Second Edition, released by Singapore government in 2019 (Tan, 2022) emphasizes transparency and fairness in the decision making process for companies using AI. The California Consumer Privacy Act (CCPA), passed in the US, aims to give residents greater control over their data (Quinlan, 2023).

Beyond the mentioned countries, other nations have taken cues, crafting their own versions of data protection laws, aiming to ensure that AI surveillance respects individual rights while serving its purpose.

***Ethical Theories***

When we talk about the ethical portion of AI surveillance, its necessary to bring in ethical theories that can guide our understanding.

1. Utilitarianism: On AI surveillance, a utilitarian approach would evaluate the total societal benefits, such as reduced crime rates or improved public safety, against its drawbacks, such as privacy invasion or potential misuses. If the benefits surpass the negatives, then from a utilitarian viewpoint, the use of AI surveillance would be considered justified. However, the challenge lies in quantifying and weighing diverse benefits against potential harms, especially when these harms might impact marginalized communities disproportionately.
2. Rights-Based Ethics: This approach emphasizes the intrinsic rights and worth of individuals. From this viewpoint, any action that infringes upon individual rights, like privacy, is inherently wrong, irrespective of its potential societal benefits. Thus, no matter the advantages AI surveillance might offer for societal safety or efficiency, if it breaches personal freedoms, it would be seen as unethical.
3. Virtue Ethics: In the context of AI surveillance, this would involve examining the intentions and moral character of those deploying and operating these surveillance systems. The question we should ask ourselves is: Are these systems employed in a manner consistent with virtues such as fairness and respect?

In essence, the legal and ethical terrains of AI surveillance are intricate and deeply intertwined. While existing law attempts to safeguard individual rights, the ethical considerations extend far beyond mere legality, delving into the core values and principles that societies hold dear.

**Mitigating Harms and Managing Risks**

Considering the above sections, this section seeks to use the mentioned ethical theories as guiding principles to identify viable measures to mitigate these risks, while still harnessing the capabilities of AI surveillance.

***Technological Measures***

Differential Privacy: As one of the most innovative solutions to data privacy concerns, differential privacy ensures that the information extracted from databases doesn’t allow the identification of any specific individual within it. By adding a specific kind of ‘noise’ to the data, it becomes nearly impossible to trace back to an individual, ensuring their personal data remains private even in large data analytics (Stadler, 2020).

Data Encryption: Advanced encryption methods ensure that the data collected remains unreadable to unauthorized entities. Even if surveillance data were to be intercepted or accessed without permission, encryption would prevent the misuse of the information (Kapersky, 2023).

Automated Redaction: Implementing technologies that automatically redact or blur certain elements, such as faces or license plates, from surveillance footage can protect the identities of individuals and ensure their privacy (CaseGuard, 2023).

***Policy Regulation***

Robust Oversight: Policies should be put in place to ensure that only authorized individuals can access surveillance data. Regular audits and assessments can further deter any unauthorized use (Lewis and Crumpler, 2021).

Legislative Frameworks: Using GDPR as a starting point, nations can develop robust regulations that specifically address the nuances of AI surveillance, including clear guidelines on data storage, usage and rights of the individuals being surveilled.

Balancing Safety and Privacy: Its crucial to ensure that while surveillance tools are effective in ensuring public safety, they don’t infringe upon individual rights. Public consultation and expert panels can assist in achieving this balance, ensuring that all perspectives are considered in the policy-making process.

***Public Engagement and Awareness***

Education: A well informed public is an empowered one. Offering educational resources and workshops on AI surveillance can help the public understand its implications and the protections in place for their safety and privacy (Ang, 2022).

Feedback Mechanisms: Encourage the public to provide feedback on their experiences and concerns with AI surveillance. This feedback can be invaluable in adjusting policies and systems to better align with the needs and comfort levels of the people.

Advocacy and Public Discourse: Public discourse can significantly influence policy. As more individuals become aware of the intricacies of AI surveillance, their voices and concerns can help shape regulations. Advocacy groups and public forums can drive these conversations, ensuring that policies and implementations are both effective and ethically grounded (Tekisalp, 2019).

The technological measures, such as differential privacy and encryption, closely aligns with the principles of rights-based ethics. By ensuring individual data remains protected and non-traceable, we are safeguarding individual rights to privacy and autonomy.

Policy regulations and strong oversight echo the principles of utilitarianism. By implementing stringent guidelines on data access and striving for a balance between public safety and personal privacy, we aim to maximize overall societal well-being. Such measures ensure that the technology delivers the greatest good for the majority.

Finally, the emphasis on public engagement, feedback and discourse is deeply rooted in virtue ethics. By fostering an informed public, virtues of transparency, mutual respect and understanding are nurtured. Encouraging public discourse and education also ensures AI surveillance remains in harmony with societal value.

By integrating mitigating measures with ethical theories, we can ensure that the technology’s potential is realised without jeopardizing our ethical responsibilities.

**Conclusion**

The intersection of AI and surveillance presents both opportunities and challenges. As we’ve explored, AI surveillance, while offering advantages in public safety and businesses operational efficiency, raises ethical concerns that are impossible to ignore. The application of different ethical theories such as Utilitarianism, Rights Based Ethics and Virtue Ethics provides a well-rounded lens through which we can evaluate and mitigate these challenges.

Comprehensive policies and meaningful public engagements are essential for striking a balance between the advancement of technology and individual freedom. An informed society is not only a safeguard against potential misuses of technology but also an active participant in deciding how it should be used ethically.

As we move towards a future heavily influenced by AI, using surveillance ethically isn’t just a tech issue, but a matter of right and wrong. The road ahead is not simply about advancing in technology but ensuring that as we do, we uphold the values that define us a society. This discussion is a call for ongoing conversation and shared responsibility in AI surveillance. The responsibility lies with all of us to shape a future where technology amplifies, not compromises, our shared ethical principles.

Word Count: 2363

**References**

Ang, P. (2022) Public education, ground-up efforts key to fighting online threats: Edwin Tong, The Straits Times. Available at: https://www.straitstimes.com/singapore/public-education-ground-up-efforts-key-to-fighting-online-threats-edwin-tong (Accessed: 19 October 2023).

Barroca, J. (no date) Surveillance and predictive policing through AI, Deloitte. Available at: https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html (Accessed: 19 October 2023).

Burgess, M. (2020) Co-op is using facial recognition tech to scan and track shoppers, WIRED UK. Available at: https://www.wired.co.uk/article/coop-facial-recognition (Accessed: 19 October 2023).

CaseGuard (2023) Automatic ai face redaction, the powerful solution to Privacy Automatic Ai Face Redaction, CaseGuard. Available at: https://caseguard.com/articles/automatic-ai-face-redaction/#:~:text=Automatic%20AI%20face%20redaction%20is,long%20the%20video%20may%20be. (Accessed: 19 October 2023).

Ellichipuram, U. (2021) Tokyo Haneda Airport turns to Collins Aerospace for Biometrics Tech, Airport Technology. Available at: https://www.airport-technology.com/news/haneda-airport-collins-aerospace/ (Accessed: 19 October 2023).

European Data Protection Supervisor (no date) Rights of the individual, European Data Protection Supervisor. Available at: https://edps.europa.eu/data-protection/our-work/subjects/rights-individual\_en#:~:text=The%20GDPR%20has%20a%20chapter,decision%20based%20solely%20on%20automated (Accessed: 19 October 2023).

Feldstein, S. (2022) China’s high-tech surveillance drives oppression of Uyghurs, Bulletin of the Atomic Scientists. Available at: https://thebulletin.org/2022/10/chinas-high-tech-surveillance-drives-oppression-of-uyghurs/ (Accessed: 19 October 2023).

Feldstein, S. (no date) The global expansion of AI surveillance - carnegie endowment for ..., Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 (Accessed: 19 October 2023).

Freiburger, K. (2020) Biometric security technology at the Super Bowl is a big win for public safety: Biometric update, Biometric Update |. Available at: https://www.biometricupdate.com/202001/biometric-security-technology-at-the-super-bowl-is-a-big-win-for-public-safety (Accessed: 19 October 2023).

Islamic Military Counter Terrorism Coalition (2020) Artificial Intelligence and Counterterrorism, Limitations, Opportunities and Risks. Available at: https://imctc.org/en/eLibrary/INTReports/Documents/Report-Issu-09-EN.pdf (Accessed: 19 October 2023).

Kaspersky (2023) What is Data Encryption?, www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/encryption (Accessed: 19 October 2023).

Levine, E.S. et al. (2017) ‘The New York City Police Department’s Domain Awareness System’, Interfaces, 47(1), pp. 70–84. doi:10.1287/inte.2016.0860.

Lewis, J.A. and Crumpler, W. (no date) Facial Recognition Technology: Responsible use principles and the Legislative Landscape, CSIS. Available at: https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape (Accessed: 19 October 2023).

Lively, T.K. (2021) Facial recognition in the US: Privacy concerns and legal developments, ASIS Homepage. Available at: https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/ (Accessed: 19 October 2023).

Masri, L. (2023) How facial recognition is helping Putin Curb Dissent, Reuters. Available at: https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/ (Accessed: 19 October 2023).

Parker, J. (2023) Facial recognition success stories showcase positive use cases of the technology, Security Industry Association. Available at: https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/ (Accessed: 19 October 2023).

Quinlan, K. (2023). California legislature passes ‘delete act’ to protect consumer data, StateScoop. Available at: https://statescoop.com/california-legislature-passes-delete-act-to-protect-consumer-data/ (Accessed: 19 October 2023).

Sadowski, J. (2019) ‘When data is capital: Datafication, accumulation, and extraction’, Big Data &amp; Society, 6(1), p. 205395171882054. doi:10.1177/2053951718820549.

Sophos News (2019) Report: Use of AI surveillance is growing around the world. Available at: https://news.sophos.com/en-us/2019/09/20/report-use-of-ai-surveillance-is-growing-around-the-world/ (Accessed: 19 October 2023).

Stadler, W. (2020) Risks of privacy-enhancing technologies: Complexity and implications of differential privacy in the context of Cybercrime, IntechOpen. Available at: https://www.intechopen.com/chapters/72517 (Accessed: 19 October 2023).

Tan, S. (2022). Singapore releases framework on how AI can be ethically used, The Straits Times. Available at: https://www.straitstimes.com/singapore/singapore-releases-model-governance-framework-for-ai (Accessed: 19 October 2023).

The Straits Times (2023) US homeland security reveals new AI guard rails as it deploys technology across agency. Available at: https://www.straitstimes.com/world/united-states/us-homeland-security-department-reveals-new-ai-guardrails-as-it-deploys-technology-across-agency (Accessed: 19 October 2023).

Trainor, C. (2021) The psychology of camera observation: How the camera affects human behavior, Montana State University. Available at: https://scholarworks.montana.edu/xmlui/bitstream/handle/1/16306/trainor-the-psychology-2021.pdf?sequence=1 (Accessed: 19 October 2023).

Tekisalp, L. (2021) How should human rights advocacy balance the opportunities & risks of artificial intelligence?, Partnership on AI. Available at: https://partnershiponai.org/how-should-human-rights-advocacy-balance-the-opportunities-risks-of-artificial-intelligence/ (Accessed: 19 October 2023).