The Ethical Dilemmas of AI Surveillance

A Critical Perspective

Ayush Srivastava	2021457
Aditya Dahiya	2021228
Shivam Chaudhary	2021489
Shyama Goel	2021492
Aalokik Singh	2021223

Introduction

Artificial Intelligence (AI) has changed the way surveillance works. It allows monitoring in bulk with very great speed and automation. With these strides into technology come fundamental ethical dilemmas: many of which intersect core philosophical concerns such as privacy, fairness, bias, autonomy, transparency, and sufficient human oversight.

There are real cases in which these intersecting concerns apply, like in case studies of Amazon Ring. Amazon Ring refers to an AI-powered system of doorbells providing real-time video monitoring, motion detection, and remote access via smartphones. As an added security device for home use, it forgives the user the opportunity to share recordings made with the Neighbours app, thereby strengthening local security within a network of neighbors and local law enforcement. Conversely, it is considered unethical because it records individuals without their consent, allowing for mass surveillance, hence often infringing on individual privacies and racial profiling.

In this project, we shall investigate the ethical implications behind the AI aspects of Amazon Ring. We will examine the operational modes of these systems and the concerns engendered for individuals and communities, including even the more extensive societal impacts of AI-driven surveillance. Through Amazon Ring and other related case studies, we aim at critically examining the responsibilities of developers, users, and policymakers to ensure an ethical design and deployment of such technologies.

Ethical Dilemmas surrounding AI surveillance

Privacy Invasion and Informed Consent

AI surveillance often collects data without explicit consent. This challenges the Kantian principle of respecting individuals as autonomous agents. Our case study of Amazon Ring stands as a clear example. These smart doorbells record people in public or semi-public spaces—even if those people have no relationship with the device owner. Non-users cannot give or withhold consent, and often have no idea they are being recorded (Frascella, 2020).

This concern is not limited to Ring. In facial recognition systems at airports, people are scanned by cameras without prior notice or choice, raising similar concerns about privacy and autonomy.

Bias and Discrimination in Algorithms

AI systems often reflect the biases present in their training data. This creates risks of discrimination, particularly against racial minorities. A well-known study by Buolamwini & Gebru (2018) showed that commercial facial recognition systems misidentify people of colour far more frequently than white individuals.

In the case of predictive policing, crime data historically over-represents marginalized communities. AI trained on this data may continue to flag these communities, leading to over-policing and reinforcing systemic bias (Choudhary et al., 2024).

Amazon Ring and the Neighbours app have also contributed to this issue, with reports often based on subjective, racially biased perceptions of "suspicious" behaviour (Frascella, 2020). These examples show that fairness must be prioritized over model accuracy in sensitive contexts.

Accountability and Transparency

Many AI systems lack explainability, making it difficult to understand or challenge their decisions. This violates principles of due process and individual rights. A key case is Amazon Ring's undisclosed partnerships with law enforcement. For a long time, users were unaware that Ring footage could be shared with police without warrants, creating a gap in accountability (Frascella, 2020). Binns (2018) stresses the importance of public reason—AI systems should provide justifications that individuals can understand and evaluate. Without this, accountability is weak and trust is lost.

Responsibility and the Problem of Many Hands

When harm occurs through AI systems, it is often unclear who should be held responsible. In Amazon Ring's ecosystem, responsibility is shared between Amazon, the user, and the police. This makes it difficult to attribute blame when something goes wrong (Coeckelbergh, 2019).

A broader example is autonomous weapons systems, where machine decisions occur faster than humans can intervene. If a strike goes wrong, should the blame fall on developers, military operators, or the algorithm itself? This "problem of many hands" highlights the need for traceability and clear responsibility chains in AI systems. Coeckelbergh (2019) argues for a relational view of responsibility—developers and companies must be answerable to the people their systems affect.

Mass Surveillance and Civil Liberties

AI surveillance may help prevent crime but can also suppress legitimate freedoms. The Neighbours app, linked to Amazon Ring, lets users report "suspicious" behaviour. These reports often reflect racial or social bias rather than objective risk (Frascella, 2020). The platform, intended for safety, sometimes becomes a tool for social profiling.

A broader example is China's Social Credit System, which uses surveillance and AI to rate citizens' behaviours. It discourages protest or dissent, raising fears of authoritarian control.

As Gunkel (2017) points out, treating technology as a neutral tool ignores how it shifts power dynamics. When surveillance becomes normal, it may limit free speech and peaceful assembly, even in democratic societies.

Legal Gaps and the Responsibility Gap

Laws have not kept pace with AI development. While regulations like GDPR or CCPA provide data rights, they do not cover all forms of surveillance. Real-Time Crime Centres in several U.S. cities now integrate Ring footage and predictive analytics without clear legal oversight (Frascella, 2020).

Coeckelbergh (2019) and Gunkel (2017) both highlight the "responsibility gap" that emerges when machines act autonomously, and no one is held accountable. Similarly, emotion recognition software in schools is used to track student attention without adequate ethical guidelines for informed consent.

Proportionality and Necessity

Surveillance should only be used when necessary and in proportion to the risk. This is a core idea in deontological ethics, which avoids violating rights unless truly justified. Real-Time Crime Centres, which monitor entire neighbourhoods with AI and camera networks, may exceed what is required for public safety (Frascella, 2020).

An academic example can be found in the design of portfolio comparison tools in research. Designers chose not to track individuals at a granular level to avoid surveillance-like behaviour, maintaining ethical restraint.

This shows that developers can make conscious decisions to limit data collection, even when more invasive tools are available.

Broader Impacts of AI

Cultural and Social Implications

Ai is not merely a breakthrough in technology, it has transformed itself manifold. It also influences how we live and interact in our culture and society. As AI tools and systems become more common in various areas, one significant impact of this is on privacy, especially in surveillance and data analysis, which changes our views on privacy. In the case of Amazon Ring, cameras attached at doorbells are turning one's personal spaces into porches and sidewalks being transformed into places of constant observation. This eventually changes the way we used to think about personal space and privacy, making constant surveillance feel normal. As a consequence of this, people lose some of the privacy they once had, and it's harder to stay anonymous in public like before (Zuboff, 2019). Surveillance raises serious ethical concerns as constant monitoring and alerts being shared on the neighbour's app can arouse a sense of fear, reinforcing racial bias, discrimination, transitioning people's trust from face-to-face interactions to a more advanced smart security system. AI and automation are reshaping the labour market. As smart systems like Amazon Ring handle tasks once done by night guards or patrol staff, some low-skill security jobs disappear, raising worries about unemployment. At the same time, the technology boosts efficiency and cuts costs, and it opens new career paths in AI development, data science, machine-learning engineering, device installation, and smart-home support. The challenge is helping workers move from roles that machines now perform to these newer, more technical positions through retraining and upskilling.

Policy Considerations

This widespread impact of AI on society and individuals shows the need for necessary and thoughtful policies to manage AI and intellectual property rights. In the current situation, there is considerable variation among the policies across different regions in the world, which creates an inconsistent mixing of regulations that is not useful for addressing the global nature of AI and understanding how data flows; for example, the U.S. has no federal data privacy law, but some states like California with its consumer privacy act have their privacy regulations, while the EU's

GDPR treats doorbell footage as highly confidential data. Also, the duration of copyright protection varies among different countries, video clips captured by Amazon Ring can be shared across countries with varying legal systems and laws, arising uncertainty to homeowners and bystanders as to how their data has been utilised and who controls the images. There is a need for consistent regulations to be followed by all countries that can guide and effectively manage the development and use of AI, especially in surveillance technologies like Amazon Ring, while protecting intellectual property and individual rights. Ethical committees at national and international levels can guide the deployment of AI systems, focusing on privacy and fairness. Meetings like the G20 summit and G7 highlight the need for such discussions to establish global standards for AI ethics and governance (Vinuesa et al., 2020) [11].

Solutions

Embedding Ethics in AI Design

Design Principles

Whenever developing and designing the intelligence systems the ethics should be integrated. It is not only the theoretical ideal but a practical need, especially in technologies like the Amazon ring. Since these systems are drastically different in use in most public and private domains, they collect and analyse huge datasets and their chances of infringing on fundamental rights grows.

Some principles have been written below:

Privacy By design: This concept demonstrates that AI should build from the very start not added later. While considering the Amazon Ring, one must ensure that the data has clear boundaries and protection by limiting the collection of personal information and identification details. Such measures enhance the anonymization techniques, encryption of data which is stored and strict control of data being shared with third parties.

Proportionality: Another significant ethical principle is proportionality. The surveillance must be equal to the actual threat. It becomes unjust when devices such as Ring cameras capture individuals who are not involved in any security matter—such as neighbours or passersby. Proportional surveillance means it must be targeted, required, and utilized only for specific reasons. This protects privacy but still keeps individuals safe.

Accountability: The principle of accountability will be maintained by clear responsibilities at the time of development and deployment. This would encompass the obligations of developers, platform providers, and law enforcement partners who access surveillance data to provide accountability mechanisms which would redress the event of harm cause by surveillance practices

Fairness and Non-discrimination: AI-powered surveillance systems which are related to face recognition and behavioural analytics show some biased results. Studies show algorithms have higher error rates with darker skin tones. AI systems must have bias prediction tools inbuilt to catch any inbuilt bias that might seep in due to diverse training datasets.

The ethical AI must be able to hold on to the principle of Autonomy by allowing individuals to retain their control over the surveillance process by making informed consent at the standard which often is not the case with current smart security applications.

Practical Solutions

Principles provide the foundation for ethics driven AI design. Translating the design into action requires practical implementable solutions. In the context of surveillance technologies such as Amazon Ring, many implementation strategies can be adopted to ensure that ethical considerations are not only being made aware but actively being addressed.

A critical solution would be the adoption of **Privacy Impact Assessments (PIAs).** These assessments measure how a proposed system will affect individual rights like privacy and

analyze the compliance with data security laws and ethical norms. Regular PIAs—especially when new features are added like facial recognition or behavioural tracking which ensure possible rights violations like privacy violation are caught before the launch. Equal priority should be placed on putting opt-in features and informed consent policies in place to further add to the safety.

The users are not only required to consent to being watched but also be made completely aware of the implications of their consent. Amazon Ring, for example, should provide fine-grained consent options, such as the ability to decide what information is given to law enforcement or third-party services. Such consent mechanisms must be easily accessible, comprehensible, and revocable at will to add an extra layer of security.

In order to address the problem of algorithmic bias, developers of AI should conduct algorithmic audits regularly. They entail methodically reviewing the results of AI systems for indications of discrimination or system disadvantage along demographic categories. Where bias is found, measures such as retraining the algorithm using more balanced data should be initiated. External audits by third parties can enhance public confidence and accountability as well making the system more reliable.

A practical solution is to create clear paths for users to complain if privacy is breached. However, people ought to be able to report issues, question why surveillance occurred, and contest it if they believe it was unjust. For instance, if Ring camera recording is employed without authorization, the user ought to be in a position to ask for it to be deleted or file a complaint.

Transparency can be enhanced by providing public updates and engaging with local organizations. Firms such as Amazon ought to periodically publish reports indicating the number of data requests they receive from police, the number they accept, and the data they provide. They should also engage with community organizations to develop equitable regulations and address concerns regarding surveillance.

A good idea is to establish **ethical certification schemes for AI surveillance technology**. Third-party organizations can provide certifications to products that are highly privacy and

fairness compliant. For instance, a Ring device that secures user data well may display a badge, making consumers purchase more ethical products and compelling businesses to adopt better practices.

Technical measures such as data minimization, end-to-end encryption, and edge processing (keeping data on the device) can also minimize the risk of abuse and provide users with greater control.

Innovative methods to resolve the issue

As this technology is being integrated into modern life at an astonishing rate, from the unlocking of mobile devices, and smart city surveillance to law enforcement. While offering unparalleled convenience and efficiency, these systems raise critical ethical and legal issues that have not, and cannot, be resolved today. Society stands at a critical juncture where innovation is to be weighed against privacy, answerability, and rights.

The main focus of problems that need to be solved deal with issues of privacy, consent, surveillance, data security, and discrimination or misuse.

It's not just the technology itself that's problematic, but it's the more extensive system of covert identification without informed user consent. Whether it's a consumer unlocking their phone or a pedestrian unknowingly caught on camera, the issue is not just who uses the technology but also how and under what oversight.

Some organizations, policymakers, and business leaders are now trying to solve the issues by creating new ethical principles and technical policies and those frameworks shore up best practices by ensuring that biometric data is collected only after written consent is obtained, fostering transparency via public announcements, and instituting audits. It is essential that facial data ascribed to users be editable, modifiable, or removable by the Developers must adopt privacy-first design principles, conduct regular bias audits, and consult ethics review boards before large-scale deployment.

Beyond technical improvements like 3D imaging, CNNs, and liveness detection, industry innovation is shifting toward responsible design. On-device processing, where data is stored

securely on the user's hardware, offers excellent privacy by minimizing external data exposure. Real-time consent indicators (visual or audio cues when facial scanning is active) can empower users with awareness and control. The integration of blockchain technology into audit logs, open-sourced bias detection algorithms, and external auditing frameworks would enhance public trust and improve accountability.

Though, solely having technological solutions will not be sufficient. There needs to be additional contextual legal and social frameworks, specifically those that deal with consumers' rights and protection. Attempting to outlaw the use of facial recognition technology in certain areas or proposing a nationwide policy shows increased uneasiness with intrusive monitoring. That said, admitting the existence of the issue, face recognition, fails to address the wider range of surveillance systems and stealth identification methods used.

In comparison, an all-encompassing approach could involve:

Controlling the activities of data vendors,

Improving public information regarding consumers' rights, and

Promoting free debate about surveillance and privacy.

Consumer protection laws offer a powerful, existing framework to rein in harmful surveillance practices. Surveillance companies, particularly those colluding with law enforcement, must observe the same standards of transparency and advertising practices as other business domains. These relationships should be made public and (in case any exists) promotional materials must ensure that it is revealed whether or not there is an attempt to cover the goals and functions of the surveillance programs.

Some cities already integrate private camera feeds, such as those from smart doorbells, into public surveillance centers, often without public awareness or consent. Real-time streaming of such footage by law enforcement agencies raises serious questions about individual rights, particularly for bystanders who are recorded without ever opting in.

In the absence of an all-encompassing federal privacy legislation, the very step that can be taken immediately is to employ consumer protection law, which offers provision for gaining

transparency and pushing back against excess surveillance. This method helps consumers, yes, but it raises awareness, invites debate, and reduces the harmful effect on privacy in an increasingly monitored society.

The problem is not simply how to make facial recognition more advanced technology; fairness, justice, and responsibility are equally vital. It is possible to construct a surveillance society where humane values are not undermined, but achieving that requires well-thought-out regulations, purposeful design, shared oversight, and informed use of facial recognition technology.

References

- Binns, R. (2018). *Algorithmic accountability and public reason*. Philosophy & Technology, 31(4), 543–556. https://doi.org/10.1007/s13347-017-0263-5
- Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification*. Proceedings of the Conference on Fairness, Accountability and Transparency, 77–91.
- Choudhary, A., Mosa, M., & Patrick, R. (2024). *Towards Ethical AI Governance: A Review of Algorithmic Regulation*. Ethics in Practice Journal, 5(2), 45–68.
- Coeckelbergh, M. (2019). *Artificial intelligence, responsibility attribution, and a relational justification of explainability*. Science and Engineering Ethics, 26, 2051–2068. https://doi.org/10.1007/s11948-019-00146-8

- Frascella, C. (2020). *Amazon Ring: Master of the surveillance circus*. Harvard Journal of Law & Technology, 33(2), 611–646.
- Gunkel, D. J. (2017). *Mind the gap: Responsible robotics and the problem of responsibility*. Ethics and Information Technology, 22(4), 307–320. https://doi.org/10.1007/s10676-017-9428-2
- Mosa, M., Patrick, R., & James, L. (2024). *Privacy by Design in Surveillance Tech: Principles and Challenges*. Journal of AI Ethics, 6(1), 33–50.

- Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
- Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., Domisch, S., Felländer, A., Langhans, S. D., Tegmark, M., & Nerini, F. F. (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. Nature Communications, 11(1), 233.
- *6 guidelines for facial recognition to build trust*. (2023, June 12). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/facial-recognition-regulation
- Gangarapu, K. R. (n.d.). *Ethics of Facial Recognition: key issues and solutions*. https://learn.g2.com/ethics-of-facial-recognition
- *Facial recognition history*. (2023, June 12). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition