AI usage on the surveillance system

Team 1

Muhammad Hamza Student ID

Talha Majeed Student ID

Kinwai lee Student ID: 35215436

Xuehua Song (Mia) Student ID: 35473397

Mimansha Devi Ramcharn Student ID: 35437257

Manatrudee Chimmee Student ID 35000842

Abstract (kinwai)

The integration of artificial intelligence (AI) into surveillance systems has helped crime prevention globally. AI technologies, such as facial recognition and license plate recognition, allow surveillance systems to identify individuals and vehicles, providing detailed information including names and other sensitive information. However, the deployment of AI in surveillance raises significant concerns regarding privacy and the potential for misuse. In this article, we will discuss more on how is it impacting to us, and what can we do to mitigate the risk and impact to the society

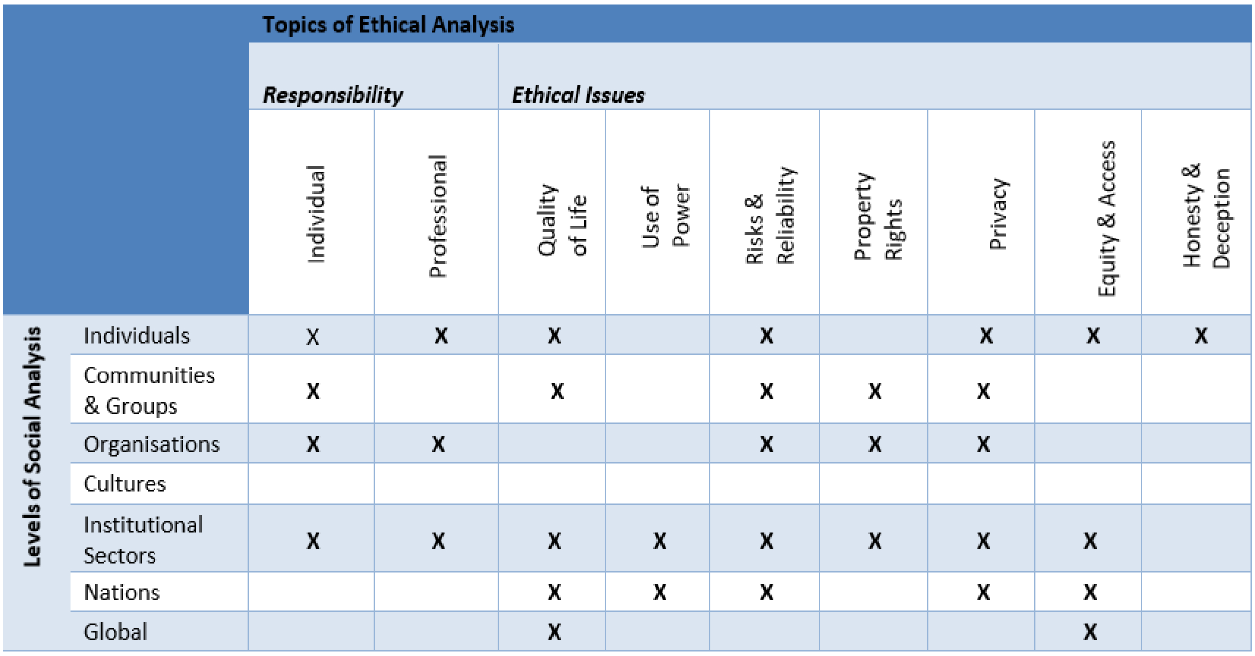
A description/explanation of the chosen technology (kinwai)

Nowadays, the surveillance system is commonly used globally to prevent crime and protect people's lives and property. But since the artificial intelligence (AI) becoming more common now, it is time to review the impact of using the artificial intelligence on surveillance system. When we do that, we need to understand more about what AI can do when applying AI to surveillance systems.

In some countries, the AI was already used on the surveillance system, with the facial recognition and car license recognition technology, the detail of every people, including the name, national ID, can be shown on the surveillance system. With the whole surveillance network, the enforcement can easily locate anyone by searching their name through the system, and it does show the footprint of all the record of a person.

Although it can prevent crime by easily locating a suspect, it also has some impact if improperly using this technology. However, in Australia, a similar technology has started to be commonly used, the Auror, which provides the platform for retailers to apply AI to their surveillance system. The Auror can recognise if a person with some potential risk to the business with face and car license recognition, and their personal detail will then be displayed on the application and inform staff on that person.

How the technology could disrupt the current way society functions: Using appendix A (Muhammad Hamza)



		Topics of Ethical Analysis								
		Responsibility		*Ethical Issues*						
		Individual	Professional	Quality of Life	Use of Power	Risks & Reliability	Property Rights	Privacy	Equity & Access	Honesty & Deception
Levels of Social Analysis	Individuals	X	X	X		X		X	X	X
	Communities & Groups	X		X		X	X	X		
	Organisations	X	X			X	X	X		
	Cultures									
	Institutional Sectors	X	X	X	X	X	X	X	X	
	Nations			X	X	X		X	X	
	Global			X					X	

This matrix evaluates the ethical considerations of AI usage in surveillance systems across various social levels, addressing both responsibility and key ethical issues such as quality of life, use of power, risks, privacy, equity, and honesty.

At the individual level, ethical concerns are significant because surveillance directly impacts privacy and personal freedom. Individuals must consider their own behavior and professional responsibility, while facing potential risks from misuse or errors in AI systems. Issues like privacy and use of power are especially relevant, as individuals are often the targets of AI surveillance.

Communities and groups share similar concerns, with an emphasis on collective privacy, fairness, and how AI surveillance may influence social dynamics. Ethical issues such as equity and honesty are important in ensuring that surveillance is applied justly and transparently within groups, preventing bias or discrimination.

For organisations, responsibility is critical, especially in the use and management of surveillance data. Professional ethics are key in preventing abuse of power, ensuring system reliability, and protecting the privacy of both employees and customers. Issues like risks and property rights come into play when organisations utilize AI surveillance, requiring careful management to avoid harm.

At the level of cultures and nations, AI surveillance can influence social norms and raise concerns about the use of power and government control over citizens.

National and cultural contexts determine how acceptable or invasive surveillance is perceived to be, with privacy and equity concerns spanning across different societies.

Finally, at the global level, AI surveillance raises questions of international standards, human rights, and global privacy protections. Issues such as quality of life, professional responsibility, and honesty are relevant, especially as surveillance technology becomes more widespread and integrated into daily life across borders.

Identify what risks and opportunities the technology provides (Xuehua Song (Mia))

Identified Opportunities and Risks

Social opportunity and risk categorisation						
HIGH	Very likely to occur				Privacy Concerns and Legal/Ethical Challenges	Enhanced Detection and Monitoring
Likelihood of Occurring	Likely to occur			Security Vulnerabilities	Improved Accuracy and Predictive Analytics	
	Possible to occur	Lack of Accountability and Technical Errors	Dependence on Technology and Misuse	Resource Optimization and Data Integration		
	Unlikely to occur			Facial Recognition and Identification		
LOW	Very unlikely to occur					
		LOW	Opportunity / Impact / Consequence			HIGH
		Incidental	Minor	Significant	Major	Severe
		Local, small-scale, easily reversible change on social characteristics or values of the communities of interest or communities can easily adapt or cope with change. Local small-scale opportunities emanating from the technology	Short-term recoverable changes to social characteristics and values of the communities of interest or community has substantial capacity to adapt and cope with change. Short-term opportunities emanating from the technology.	Medium-term recoverable changes to social characteristics and values of the communities of interest or community has some capacity to adapt and cope with change. Medium-term opportunities emanating from the technology.	Long-term recoverable changes to social characteristics and values of the communities of interest or community has limited capacity to adapt and cope with change. Long-term opportunities emanating from the technology	Irreversible changes to social characteristics and values of the communities of interest or community has no capacity to adapt and cope with change.

	that the community can readily pursue and capitalise on				

Appendix B. helps to visualize the potential social impacts of AI in surveillance, categorizing them by their likelihood and severity. Continuous assessment and community engagement are essential to navigate these opportunities and risks effectively.

Opportunities:

1. **Enhanced Detection and Monitoring**: AI can quickly process vast amounts of data, improving real-time detection of suspicious activities that might be overlooked by human operators.
2. **Improved Accuracy and Predictive Analytics**: Machine learning algorithms can reduce false positives and negatives in threat detection, allowing for more reliable outcomes and enabling proactive measures by predicting potential incidents before they occur.
3. **Resource Optimization and Data Integration**: AI systems can integrate data from various sources (cameras, sensors, databases) to provide a comprehensive view of security scenarios, helping agencies allocate resources more effectively to high-risk areas.
4. **Facial Recognition and Identification**: Advanced facial recognition technologies can assist in identifying suspects and missing persons, enhancing security at public events and sensitive locations.

Risks:

1. **Privacy Concerns and Legal/Ethical Challenges**: The use of AI in surveillance raises significant privacy issues, as it may lead to constant monitoring without consent. This creates complex legal and ethical questions about data ownership and permissible surveillance. This is a long-term risk.
2. **Security Vulnerabilities**: AI surveillance systems can be vulnerable to hacking or misuse, potentially leading to breaches of sensitive data or manipulation of surveillance outputs.
3. **Dependence on Technology and Misuse**: Overreliance on AI can diminish human oversight and judgment, increasing the risk of unauthorized monitoring or tracking by authorities or third parties.
4. **Lack of Accountability and Technical Errors**: Automated systems may make it difficult to determine accountability in cases of wrongful identification or surveillance errors, which can adversely affect innocent individuals.

Balancing the opportunities and risks associated with AI in surveillance systems is essential. This framework highlights various potential benefits and challenges. While short-term opportunities can enhance security and foster community collaboration, long-term risks—especially those related to privacy and social norms—present significant concerns.

Stakeholders must proactively address these risks to ensure that the benefits of AI in surveillance are maximized while minimizing negative impacts. Continuous monitoring and adaptation will be crucial throughout the project lifecycle to uphold ethical standards and maintain public trust.

Identify what ethical responsibilities the existing ICT workforce must support for the integration of these technologies into businesses and daily life (Mimansha)

The **ICT workforce** refers to professionals working in the Information and Communications Technology (ICT) sector. These professionals involved are responsible for developing, managing, and implementing technologies, including AI integrated systems. The roles include Software Developers and Engineers, System Administrators and IT Managers, Data Scientists and Analysts, Cybersecurity Professionals and Project Managers.

Ethical responsibilities refer to the moral obligations and duties that individuals and groups within the ICT workforce have in ensuring that their actions, decisions and technologies developed by them, align with moral principles. The existing ICT workforce must implement ethical standards to safeguard user privacy, ensure fair data usage, prevent bias in AI systems, and ensure accountability when designing, deploying and managing these systems.

Hence, the **ICT workforce plays a crucial role in ensuring the responsible integration of AI surveillance technologies into businesses and daily life**. The ethical responsibilities relate to different stakeholders of the system such as; System Administrators, Business Owners, the General Public, and Governments, ensuring that technology enhances efficiency without compromising privacy, fairness and human rights.

Current Ethical Responsibilities of the ICT Workforce -

The existing ethical responsibilities of the ICT workforce regarding AI usage in surveillance systems include:

1. Data Privacy & Protection: Ensuring that personal data collected through surveillance is encrypted, anonymized, and used according to data protection regulations. This is done through the implementation of firewalls and data anonymisation techniques.
   Example: System administrators ensure that the data collected from AIA surveillance systems is securely stored and accessed only by autorised personnel.

2. Fairness and Bias prevention: Avoiding bias in AI systems though monitoring to detect and mitigate biases that may lead to unfair treatment of certain individuals or groups.
   Example:

- Facial recognition algorithms must be trained on diverse datasets to prevent misidentification or discrimination against minorities.
- Detection tools are deployed to ensure that facial recognition algorithms in AI surveillance do not misidentify people based on race or gender

3. Transparency & Accountability: Clearly communicating how AI systems operate, what data is being collected, and how decisions are made by the AI system. Ensuring there is a clear line of accountability if these systems malfunction or cause harm.
   Example: Businesses implement cookie and privacy notices explaining AI surveillance in use on their websites.

4. Legal Compliance: the ICT workforce ensures that AIA surveillance systems comply with regulations such as GDPR, HIPAA, as well as international protection laws.
   Example: AI systems are designed with built-in features to allow compliance audits, making sure data usage follows legal frameworks.

Ethical Responsibilities for the Stakeholders -

In the context of:

1. **Businesses**:
   Here, AI surveillance may be used for security, performance tracking or customer behaviour analysis. The stakeholders involved: ICT professionals, Business owners and managers, Employees and Customers/clients.

   - Privacy Protection for Employees and Customers:
     Businesses must ensure that AI surveillance systems are only used for legitimate purposes, such as improving security or optimizing services, without violating personal privacy. They must disclose surveillance practices and request consent for tracking customer behaviour on websites or in physical locations.

   - Preventing Discrimination:
     AI systems should not be used to unfairly discriminate in hiring, promotions, or customer service. Developers and analysts must work to ensure algorithms are free from biases.

   - Preventing exploitation:
     Surveillance systems should not be used to exploit employees such as by using productivity data to unethically increase workloads or terminate employees unfairly. Businesses are using AI-driven analytics to improve

operational efficiency but are starting to realize the need for more oversight on bias.

- Security and data usage:
  Businesses should ensure that customer and employee data collected through surveillance is securely stored and not misused in any way.

2. **Everyday Life**:
   AI surveillance technologies are integrated into public spaces, social media, personal devices and even smart homes. The stakeholders involved: ICT professionals, Government and law enforcement, the general Public and Civil Rights organisations.

   - Respecting Individual Autonomy and Privacy:
     The ICT workforce must develop AI systems that respect individual privacy and autonomy in daily activities. AI surveillance in homes and public spaces should not infringe on personal freedoms. Data minimisation techniques and user consent mechanisms are applied to prevent unnecessary data collection.

   - Ensuring Fair Use of AI Surveillance in Public Spaces:

   AI surveillance should not create a constant state of monitoring for ordinary citizens. Governments and local authorities must balance public safety with respect for civil liberties. Surveillance systems are being implemented for security and public safety in various areas, like public transportation and shopping centres.

Strategic Recommendations for AI Integration in Surveillance Systems (Manatrudee Chimmee Nina)

The integration of AI in surveillance systems offers significant benefits for public safety and crime prevention. However, it also presents notable challenges concerning ethical considerations, privacy, and data security. To maximize the benefits while mitigating risks, the following recommendations are proposed:

1. **Enhance Data Privacy and Security Measures:** Organizations employing AI in surveillance should prioritize protecting personal data. Implementing advanced data encryption and anonymization techniques is essential to prevent unauthorized access and misuse of sensitive information. Additionally, organizations should establish clear data access protocols, ensuring only authorized personnel can view or manage surveillance data.

2. **Develop an Ethical Framework for AI Implementation:** A comprehensive ethical framework should be established to guide the deployment and use of AI in surveillance systems. This framework must address ethical issues such as data privacy, bias, and the potential misuse of AI technology. AI models should be tested and validated using diverse datasets to ensure fairness and transparency, reducing the risk of biased outcomes that could disproportionately impact certain demographic groups.

3. **Promote Transparency and Accountability:** Enhancing transparency in AI-driven surveillance is crucial by providing regular reports on its use, impact, and performance. Organizations should communicate with the public regarding how AI technology is being used and the type of data being collected. Furthermore, a mechanism for holding individuals and organizations accountable should be established, particularly in cases where the technology is misused or violates individuals’ privacy rights.

4. **Encourage Community Engagement and Awareness:** To foster public trust, organizations should engage with the community and involve them in discussions about the deployment of AI in surveillance. Awareness campaigns should be conducted to educate the public on the benefits and limitations of AI surveillance and their rights concerning data privacy and security.

5. **Establish Robust Legal and Policy Frameworks:** Policymakers should revise and strengthen existing laws and regulations to address the evolving landscape of AI in surveillance. This includes defining acceptable use cases, setting precise data collection and retention boundaries, and establishing penalties for privacy rights violations. By providing a robust legal foundation, the responsible use of AI can be ensured while protecting individual rights.

6. **Continuous Monitoring and Evaluation:** AI surveillance systems should undergo constant monitoring and evaluation to identify emerging risks or unintended consequences. Organizations should establish a dedicated team responsible for regularly auditing the system's performance, assessing its compliance with ethical standards, and updating policies to adapt to technological advancements and societal changes.

By implementing these recommendations, organizations can leverage AI technology to enhance public safety without compromising ethical standards or privacy. These proactive measures will ensure that the deployment of AI in surveillance is both responsible and aligned with societal values, ultimately fostering a safer and more secure environment for all.

Conclusion (Talha Majeed)

In conclusion, the use of AI in surveillance systems can greatly improve security and help prevent crime. By recognizing faces and vehicle license plates, AI can quickly identify suspects and allow authorities to respond faster to incidents. This makes public places, businesses, and communities feel safer. However, AI in surveillance also has some serious challenges, especially when it comes to privacy and fairness. There is always the risk that AI could be used in ways that invade people’s privacy or lead to unfair treatment, such as misidentifying innocent people.

To deal with these challenges, it is important to have strong rules and ethical guidelines in place. These rules should focus on protecting people's personal information and ensuring that AI is used fairly and responsibly. Organizations that use AI for surveillance should be open and honest about how the technology works and what data is being collected. They should also involve the community in discussions about the use of AI to make sure everyone understands its benefits and risks.

Additionally, AI systems should be regularly monitored and checked to make sure they are working correctly and not causing harm. If there are problems or mistakes, there should be a clear process for fixing them quickly. It is also important that the use of AI in surveillance follows local laws and respects human rights.

In the end, AI can make a big difference in keeping people safe, but it must be used carefully. By balancing security with privacy and fairness, we can enjoy the benefits of AI in surveillance without risking the loss of trust or violating people's rights. With clear guidelines, transparency, and continuous monitoring, AI in surveillance can create a safer and more just society for everyone.