Original Article

Ethical Implications of Advanced Surveillance Technologies on Law Enforcement: A Case Study of National Police Service in County of Nairobi, Kenya

Benjamin Kisio[1]* & Prof. Ndikaru wa Teresia, PhD[1]

[1] The Technical University of Kenya, P. O. Box 52428 – 00200, Nairobi, Kenya.

* Correspondence ORCID ID: https://orcid.org/0000-0001-8824-6352; email: jndikaru@gmail.com.

ABSTRACT

The study's research objectives included examining the effects of advanced surveillance technologies on law enforcement by NPS in Nairobi County and evaluating the ethical implications of using these technologies by the NPS. The social contract theory was used to understand the ethical implications of using advanced surveillance technologies in law enforcement. The research population includes the 4.7 residents of Nairobi County affected by the implementation of advanced surveillance technologies both overtly and covertly. The data was collected from a sample of 50 randomly sampled participants. The respondents were engaged using a qualitative questionnaire. Therefore, both qualitative and quantitative data were collected in the study. The study was analyzed using Statistical Package for Social Science (SPSS) and the thematic analysis method. The study concluded that the use of advanced surveillance technologies such as CCTV systems, facial recognition, license plate recognition, drones, forensic tools, and biometric systems in law enforcement and public safety are widely acknowledged. The ethical considerations regarding these technologies include data security, privacy, freedom of expression, transparency, and accountability. These, however, do not negate the fact that the technologies are necessary for enhancing public safety and emergency response. It is, therefore, imperative to establish clear guidelines and regulations for using advanced surveillance technologies in law enforcement.

INTRODUCTION

Advanced surveillance technologies have become an integral part of law enforcement in the quest to maintain public safety and combat criminal activities (Laufs & Borrion, 2022), particularly in an increasingly interconnected and digitized world. These technologies can potentially enhance law enforcement's effectiveness (Hill et al., 2022) and provide invaluable tools for crime prevention and investigation. Their use, however, has also raised various ethical concerns and challenges, particularly when it comes to safeguarding individual rights, privacy (Ezzeddine et al., 2023; Fussey & Sadhu, 2022), and the potential for abuse of power by law enforcement agencies (Laufs & Borrion, 2022). This study delved into the ethical implications of advanced surveillance technologies on law enforcement, specifically referring to the National Police Service (NPS) in the County of Nairobi, Kenya.

The study's relevance was premised on the fact that as technology continuously evolves at an unprecedented pace, the ethical landscape surrounding surveillance practices within law enforcement agencies invariably calls for critical examination. Notably, as is the case in other countries across the globe, the advancements in surveillance technologies have proliferated, thereby presenting both risks and opportunities (Fussey & Sadhu, 2022). The study, therefore, explored the complexities of NPS adopting and implementing these technologies for law enforcement while also upholding a framework of ethical conduct and accountability. The study was, therefore, guided by the following research questions:

- How do advanced surveillance technologies affect law enforcement practices by the National Police Service in Nairobi County?

- What are the ethical implications of using advanced surveillance technologies in law enforcement by the National Police Service in Nairobi County?

EMPIRICAL LITERATURE REVIEW

Advanced Surveillance Technologies for Law Enforcement

Advanced surveillance technologies are cutting-edge techniques and tools that are used for gathering information (Fussey et al., 2022), tracking objects or individuals (Hill et al., 2022), and monitoring activities (Zheng, 2016). Advanced surveillance technologies are used for various purposes, including data collection, security, and law enforcement (Manes, 2019). Ezzeddine et al. (2023) noted that advanced technologies have evolved significantly recently and incorporate a broad scope of sophisticated capabilities and features.

Advanced surveillance technologies are invaluable for enhancing safety and security, particularly when employed ethically and responsibly (Raposo, 2022). The systems effectively provide real-time information (Fussey & Sadhu, 2022) and help law enforcement officers respond to emergencies and threats more effectively (Laufs & Borrion, 2022). More specifically, surveillance cameras effectively deter criminal activities since criminals are aware they are being observed and may be identified during or after the crime (Urquhart & Miranda,

2022). This enhances public safety and has significantly reduced rates of crime.

Advanced surveillance systems are also helpful for real-time monitoring. Law enforcement offices use real-time videos to monitor locations and respond swiftly to ongoing emergencies or security incidents such as crime, fires, or accidents (Raposo, 2022). Law enforcement officers have also used advanced surveillance technologies to collect evidence in criminal investigations (Laufs & Borrion, 2022). Such evidence includes images and video footage that are later presented in court when prosecuting criminal offenders and have contributed to having more convictions and enhancing security and safety in communities (Fussey & Sadhu, 2022).

A more common use of advanced surveillance has been in traffic management, where systems have been installed, including traffic cameras and license plate recognition systems (Urquhart & Miranda, 2022). These systems help monitor the flow of traffic, respond quickly to accidents, enforce traffic rules, and reduce road-related injuries and fatalities (Fussey & Sadhu, 2022). Advanced surveillance systems have also been adopted in crowd management, particularly for large crowds such as protests or public events (Raposo, 2022). The systems monitor the crowd's behavior and identify any potential safety concerns or security threats that need to be addressed before they escalate (Laufs & Borrion, 2022).

Apart from that, advanced surveillance systems have been used to conduct searches and rescue missions by law enforcement officers. This has involved using drones in searching locations and rescue operations to acquire an aerial view of areas that are hard to access (Fussey & Sadhu, 2020). The technology has been particularly useful in responding to natural disasters, tracking terrorists, and locating missing persons (Urquhart & Miranda, 2022).

According to Laufs and Borrion (2022), advanced surveillance technologies are also used for predictive policing, whereby they help law enforcement officers analyze data, thereby identifying patterns and trends regarding particular issues, such as crime. In this way, law enforcement agencies effectively allocate resources for preventing and controlling crime (Laufs & Borrion, 2022). Law enforcement agencies have also used advanced surveillance systems to monitor and protect critical infrastructure against terrorist activities (Raposo, 2022). The systems have also proved invaluable in monitoring and protecting public spaces and transportation hubs against potential terrorist threats (Fussey & Sadhu, 2020).

Examples of advanced surveillance technology include closed-circuit television (CCTV) (Hill et al., 2022). CCTVs are commonly used in commercial and non-commercial locations (Zheng, 2016). Hill et al. (2022) noted that modern CCTV systems have high-resolution cameras with features that include object tracking, license plate recognition, and facial recognition. CCTV systems are often connected to centralized rooms (Hill et al., 2022) or cloud systems to facilitate real-time monitoring of locations (Manes, 2019).

Advanced surveillance technology also includes facial recognition technologies that use machine learning algorithms to identify and track individuals based on their facial features (Ezzeddine et al., 2023). Facial recognition technologies are often used for security purposes, access control, and public surveillance (Fussey et al., 2022). Law enforcement agencies could use facial recognition technology to identify individuals from surveillance footage of photos (Zheng, 2016). The technology can also be used to locate missing persons and crime suspects and enhance security in public locations (Hill et al., 2022).

Besides, advanced surveillance technology includes license plate recognition systems, which use cameras and optical character recognition to capture and identify motor vehicle license numbers (Ezzeddine et al., 2023). Law enforcement officers use this system to scan vehicle number plates, track stolen vehicles,

monitor traffic, and identify suspects (Fussey et al., 2022).

Drones are another technology that employs unarmed aerial vehicles (UAVs) equipped with cameras and sensors to conduct aerial surveillance (Manes, 2019). Drones will also be equipped with thermal imaging technology to provide invaluable situational awareness (Ezzeddine et al., 2023). Drones provide a bird's eye view of a particular location that could otherwise be difficult to monitor (Ezzeddine et al., 2023; Hill et al., 2022). law enforcement officers use drones to conduct searches, surveillance, and rescue missions (Zheng, 2016). They also use drones to monitor large events that could be prone to security threats (Manes, 2019).

The other advanced technologies used by law enforcement include forensic technologies, which are used for processing and analyzing evidence, such as ballistics, fingerprint recognition systems, and DNA analysis (Hill et al., 2022). There are also biometric identification systems that use fingerprints, palm print recognition, and iris technologies, which law enforcement officers use in identifying individuals (Fussey et al., 2022). Additionally, law enforcement officers also conduct social media monitoring as a way of tracking and analyzing social media content and use. In this case, they track trends, monitor public sentiments, and identify potential threats to public safety and security (Zheng, 2016). Audio surveillance is another technology that captures and analyzes audio data, particularly from phone conversations, for various purposes (Fussey et al., 2022). The technology includes gunshot detection, speech recognition, and eavesdropping detection, which law enforcement officers use to identify suspects or track the composition between suspects (Hill et al., 2022).

Ethical Implications of Using Advanced Surveillance Technologies in Law Enforcement

Extant literature has indicated that various ethical issues come with using advanced surveillance technology in law enforcement practices. Care considerations must be made to ensure that the adopted technologies are used accurately and responsibly for the benefit of all stakeholders (Ezzeddine et al., 2023). Almeida et al. (2023) pointed out that one of the major ethical concerns regarding these technologies is privacy and data protection. This is evident considering the vast amount of data about individuals that can be collected, which often occurs without their knowledge or consent.

Harper et al. (2021) pointed out that using these technologies does not provide individuals with opportunities for consenting to being tracked or recorded, which is a potential gross violation of their personal freedoms and autonomy. Schuck (2015) concurs, adding that the lack of consent in collecting the data is compounded by the possibility of using the data for more than what was originally intended. This is possible considering that we live in an information age, and the data could be sold to organizations interested in understanding particular issues, such as consumer behaviors within particular contexts. Almeida et al. (2023) observed that in most cases, law enforcement agencies are not transparent about their operations, leaving alone the technologies they use. This creates significant loopholes for the technologies to be abused, particularly considering these agencies often operate in contexts with insufficient oversight to ensure that they appropriately use the technologies.

According to Alfonsi and Berliri (2021), using advanced surveillance systems in law enforcement creates the risk of evolving into a surveillance state in which citizens are constantly monitored by the government, not so much to enhance safety and security as to restrict personal freedoms. Ezzeddine et al. (2023) agreed that the use of these systems could lead to a situation where citizens feel that they are constantly under the scrutiny of the government, and this may restrict them from full participation in their democratic duties through picketing, demonstrations, and expression of personal opinions about contentious issues affecting governance.

Alfonsi and Berliri (2021) observed that one of the ethical concerns regarding using advanced surveillance systems in maintaining law and order involves the possibility of bias and discrimination perpetrated by law enforcers. They cited evidence that indicates that many surveillance technologies, such as face recognition, have been used to perpetuate biases, particularly against certain ethnic and racial groups. Almeida et al. (2023) further note that the technologies themselves may be biased in their configuration, leading to discriminatory outcomes that further entrench the existing inequalities. Ezzeddine et al. (2023) further observed that in cases where these technologies fail in accuracy and accountability, the risk of misidentification invariably increases, exposing innocent individuals to unjustified consequences. They noted that ensuring accountability for such errors is still an ongoing concern in the technology industry.

Guidelines and Regulations Regarding the Use of Advanced Surveillance Technologies

Previous literature has captured the need for guidelines and regulations that moderate the implementation of advanced surveillance systems. Alfonsi and Berliri (2021) noted that uploading such guidelines and regulations is instructive in striking a balance between protecting individual rights and civil liberties on the one hand and ensuring public safety and security on the other hand. Saheb (2022) pointed out that specified guidelines and regulations are necessary for ensuring that transparency and accountability are achieved by using advanced surveillance technologies to maintain law and order. Establishing such buildings would ensure that law enforcement agencies publicly disclose the types of equipment they are using and for what purposes they are using them. The guidelines and regulations will also moderate independent oversight and accountability in the use of the technologies as a way of preventing abuse.

According to Gstrein et al. (2019), the use of advanced surveillance technologies should be guided by some specified legal structures, such as search warrants, that law enforcement agencies should obtain before they use the technologies. Singh (2022) further noted that regulations should specify how and when particular technologies can be used to prevent them from being used arbitrarily for purposes that may not necessarily advance the security and safety of the larger public.

Power et al. (2021) also recommended establishing guidelines and regulations concerning data privacy and security that specify how law enforcement agencies collect data using surveillance technologies. In this case, the regulations also need to specify how the collected information should be stored, shared, and accessed, outlining the people responsible at each stage. This will ensure that personal information is adequately protected, and there should also be a limit on how long the data could be stored to prevent it from being accessed for unauthorized purposes. Hill et al. (2022) noted that regulations should require law enforcement officers to ensure the security of the data they collect and that the agencies develop adequate measures for preventing unauthorized access and data breaches that could compromise the security and privacy of personal information.

Ezzeddine et al. (2023) also advocated for the provision of guidelines concerning the use of biometric technologies such as iris scanning, DNA analysis, and facial recognition. They also noted that establishing clear and strict guidelines was necessary to prevent law and forces from making wrongful arrests and protect them against conducting mass surveillance. Harper et al. (2021) also established that guidelines and regulations would help delineate between using surveillance technologies in private and public spaces. In this regard, the use of surveillance technologies in private spaces, such as homes, should be based on stringent regulations to protect the privacy rights of the users of those spaces.

Public Education on the Use of Advanced Surveillance Technologies

Previous studies have looked at public education's relevance in using Advanced surveillance

technologies in law enforcement. For instance, Maliphol and Hamilton (2022) noted that public education increases public awareness about surveillance technologies, ensuring that law enforcement agencies observe transparency and accountability in using the technology. When the public is aware of the technologies, how they can be used and their potential impact on civil liberties and privacy, they are invaluable and a better place for holding law enforcement agencies accountable for their use. According to Alfonsi and Berliri (2021), public education helps people appreciate their rights regarding law enforcement and understand how they can protect those rights. This is necessary because any improper use of advanced surveillance technologies can infringe on individuals' civil liberties and privacy rights.

Fussey & Sadhu (2022) noted that public education helps to help people make informed decisions about whether they should allow the use of advanced surveillance technologies in their neighborhoods. The public is also informed about circumstances in which law enforcement agencies should obtain consent from individuals or communities before installing or using particular surveillance technologies.

According to Laufs and Borrion (2022), the ethical issues surrounding the use of surveillance technologies make it imperative for the public to be engaged through educational programs to know the role they need to play to ensure the use of the technologies is ethical. If anything, surveillance technologies present ethical questions that demand a balance between security and privacy. Public education provides a forum through which public members are engaged in informed debates and discussions on the ethical approaches that should be adopted in using advanced surveillance technologies to maintain law and order.

Power et al. (2021) concurs that public education forums on the use of surveillance technologies enhance a sense of community engagement whereby law enforcement agencies and any other relevant stakeholders are brought on board to discuss issues on the use of new technologies. The

involvement of the public in these discussions makes all stakeholders, more particularly members of the public, better informed. Besides, the forums also provide the opportunity for law enforcement agencies to get feedback from the public and make better policies or adopt best practices concerning the use of the technologies.

In the same vein, Urquhart and Miranda (2022) noted that a more informed public is highly likely to engage in advocacy efforts regarding privacy, safety, and security. Such a public is better placed to help the authorities develop effective policies for regulating surveillance technologies and ensuring that they are not used in ways that could undermine individual rights and public interests. Fussey & Sadhu (2022) also found that public education is necessary for keeping people informed about the continuous changes in surveillance technologies. This is essential because technology is evolving fast, and those who keep abreast of these developments stand to benefit more from using the technologies.

THEORETICAL FRAMEWORK

The social contract theory was adopted for this study to understand the ethical implications of using advanced surveillance systems in law enforcement. The theory suggests that individuals come together to form a society and create a governing structure based on a mutual agreement (Liaropoulos, 2020), which is referred to as a social contract (Seabright et al., 2021). This particular contract establishes the government's and its citizens' rights and responsibilities (Sapp et al., 2021). Various philosophers have developed the social contract theory throughout history, including Thomas Hobbes, John Locke, Jean-Jacques Rousseau, and Immanuel Kant (Liaropoulos, 2020), with different variations and interpretations.

Social contract theory underscores the significance of ethical issues associated with using advanced surveillance systems in law enforcement, such as individual consent. This implies that under the social contract, citizens should go to government authority in exchange for protection of their rights, including privacy (Van

Brakel & Hert, 2011). Therefore, using technologies such as facial recognition and mass data collection, which bring up issues of consent and individual privacy, can only be ethical if citizens express consent about their use to collect data about them.

Besides, under the social contract, the government is obligated to ensure the security and safety of its citizens (Seabright et al., 2021). Advanced surveillance technologies can enhance law enforcement agencies' capacity to combat crime and ensure public security and safety (Liaropoulos, 2020). By extension, the social contract also obligates the government to balance between the use of surveillance technologies for security and protecting the rights and freedoms of the citizens as a central ethical concern (Sapp et al., 2021).

METHODOLOGY

The study adopted a descriptive research design, which Johnson and Christensen (2018) recommended that seeks to observe and describe the relationship between characteristics or behavior of a research phenomenon without manipulating them. Descriptive research design is often used in cases where the researcher is keen on providing a detailed and accurate account of the existing relationships and patterns within specific contexts (Creswell & Creswell, 2018). The study sought to understand the relationship between the use of advanced surveillance Technologies and law enforcement by the NPS in Nairobi County. The design is instructive in understanding the nature of research variables and their relationships in particular contexts (Kothari, 2014). It has been adopted by decision-makers in fields including public policy to inform choices based on a clear understanding of the prevailing conditions (Creswell & Creswell, 2018). Notably, this study informed policy issues concerning adopting advanced surveillance technology in law enforcement by the NPS in Kenya. Therefore, the adoption of descriptive research design was considered necessary in this study to provide a comprehensive understanding of the relationship between law enforcement and the use of advanced surveillance technology. The design adopted both quantitative and qualitative approaches in the collection and analysis of data.

The population of the study was the 4.7 million people living in Nairobi County. A simple random sampling method was used to determine the study participants. The method was considered because of its representativeness in ensuring each member of the target population has an equal chance of being included in the study (Kothari, 2014). A sample size of 50 respondents was used in the study. The sample was determined based on the accessibility of the respondents in the study. The data was collected using a qualitative questionnaire, including quantitative and qualitative questions. The qualitative questionnaire is considered for its flexibility in adapting and refining questions during the data collection process (Johnson & Christensen, 2018) and its capacity to provide in-depth insight, enabling the respondents to explain their quantitative responses (Creswell & Creswell, 2018). The researcher administered the questionnaire, ensuring 100% of the response rate for the target sample size. The data was analyzed using both qualitative and quantitative means. The quantitative data was cleaned and keyed into the Statistical Package of Social Science (SPSS) for further analysis using descriptive methods, namely frequencies and percentages. The qualitative data was analyzed using thematic analysis, including data cleaning, coding, sub-theme generation, major themes generation, interpretation, and report writing (Creswell & Creswell, 2018).

RESULTS AND FINDINGS

The demographic data showed that both genders were involved in the study. They included 30 men (60%) and 20 women (40%). The respondents were also drawn from various age groups: 20% were aged between 18 – 25 years, including one male and nine women; 18% were aged between 26 – 35 years, including eight men and one woman; another 18% were aged between 36 – 45 years including three men and six women; 22% of the respondents were aged between 46 – 55 years

including seven men and four women, while another 22% were men aged from 56 years and above. More men than women were included in the study because most women who were reached did not want to participate.

Table 1: Demographic Information of the Respondents

	18- 25 Yrs.	26 – 35 Yrs.	36 – 45 Yrs.	46 – 55 Yrs.	56 Yrs. & Above	Total
Male	1	8	3	7	11	30
Female	9	1	6	4	-	20
Total	(10) 20%	(9) 18%	(9) 18%	(11) 22%	(11) 22%	50

Elements on the Use of Advanced Surveillance Technologies in Law Enforcement

Familiarity with Advanced Surveillance Technologies

Most respondents (66%) were familiar with the advanced surveillance technologies. However, 34% of the respondents claimed they were unfamiliar with the technologies (See Table 2.0 below). The respondents identified some advanced surveillance technology, such as CCTV systems, facial recognition, license plate recognition installed on highways, drones, forensic technology used for DNA analysis, fingerprint recognition, and biometric systems. These findings concurred with those of previous studies, such as Hill et al. (2022), who pointed out that CCTV systems have features that include object tracking, license plate recognition, and facial recognition. Fussey & Sadhu (2022) established that facial recognition technologies are sometimes used for security purposes, access control, and public surveillance. Ezzeddine et al. (2023) found that license plate recognition systems are intended to capture and identify motor vehicle license numbers. Law enforcement officers use drones to conduct searches, surveillance, and rescue missions (Zheng, 2016). Fussey et al. (2022) further noted that biometric identification systems helped identify individuals.

The respondents also listed audio surveillance and social media tracking as additional advanced surveillance technologies they were familiar with. Extant literature, such as Zheng (2016), acknowledges using social media tracking systems to monitor public sentiments and identify potential threats to public safety and security. Hill et al. (2022) also pointed out that audio surveillance is helpful in gunshot detection, speech recognition, and eavesdropping detection to identify suspects or track the composition between suspects.

Ethical Implications of Using Advanced Surveillance Technologies in Law Enforcement

Most of the respondents (56%) were aware of the ethical implications involved in the use of advanced surveillance technologies in law enforcement, while 44% claimed that they were not aware of them (See Table 2.0 below).

Need for Enhancing Public Safety and Security

As shown in Table 2.0 below, most respondents (28%) were neutral about the need to enhance public safety and security; 26% disagreed; another 26% agreed, while 20% strongly agreed. Cumulatively, those who agreed and strongly agreed that there was a need for enhancing public safety and security using advanced surveillance technologies 46%. This indicated that most respondents acknowledged the need to use the technologies to enhance safety and security. Those who acknowledged as such cited reasons findings from previous studies have also acknowledged the relevance of advanced surveillance technologies in enhancing safety and security. Fussey & Sadhu, 2020) found that the systems were effective in providing real-time information and monitoring traffic flow and incidents; Laufs and Borrion (2022) found that the system helped collect evidence and respond to emergencies and threats more effectively; Urquhart & Miranda (2022) found that systems such as CCTV effectively deterred criminal activities. Other studies, such as Raposo (2022), claimed that their systems helped law enforcement agencies monitor locations and

respond swiftly to any ongoing emergencies or security incidents.

Those who were neutral argued that they did not have adequate information about surveillance technologies, their capabilities, and their potential implications in law enforcement. Therefore, they could not rightly indicate that they were good or bad adoptions in law enforcement. Others indicated that they have not experienced the positive or negative effects of using these technologies, and they, therefore, have specific opinions about their use in law enforcement. Some claimed that they were unsure about how the use of the technologies would affect privacy, security, and civil liberties, and they needed more information before they could provide a decisive opinion.

The disagreed respondents cited various issues, including data security that the technology will collect, which they feared could be vulnerable to breaches, hacking, and misuse by law enforcement or unauthorized users. Some indicated that the surveillance systems could restrict freedom of expression and assembly, which would curtail people's constitutional right to voice their ascending opinions or participate in demonstrations if they knew they were being constantly monitored. Some argued that the collected data could be used for purposes rather than or beyond the intended purpose, and this would result in more intrusion. Others doubted the transparency and accountability that law enforcement would uphold in the use of advanced surveillance systems; they noted that they could use their systems to abuse their power by profiling people ethnically, advancing discrimination, and targeting marginalized communities. These findings concur with those by previous studies such as Almeida et al. (2023), who found that the major ethical concerns regarding the use of these technologies include privacy and data protection, which is because of the vast amount of data of personal data that is collected without the knowledge or consent of individuals.

Ethical Concerns on the Use of Advanced Surveillance Technologies

The findings showed that most of the respondents (84%) were concerned about ethical violations that could accompany advanced surveillance technologies in law enforcement, while 16% were not concerned (See Table 2.0 below). The respondents raised various ethical concerns regarding the adoption of advanced surveillance systems in the enforcement of laws. Amongst them was privacy and data protection, in which some indicated that the use of the system would invade their privacy. Some were concerned that using advanced surveillance systems would lead to the collection of personal data without the consent of individuals, thereby exposing their privacy. Some respondents were concerned that the government would abuse such a system and result in a state where people are under constant scrutiny so that they cannot express themselves online or offline. Some are concerned with the accuracy of the advanced surveillance system in terms of identifying people; they noted that the system could also be abused in the sense that law enforcement officers will use it to target people who are marginalized or whose communities are associated with terrorism or civil rights demonstrations. Additionally, other respondents were more concerned that the data collected may not be secure and could fall into the hands of the wrong people, who may use it to blackmail or con people. They noted instances where some rogue law enforcement officers collaborated with criminals to victimize members of the public.

Previous studies have also generated similar findings regarding the ethical challenges of using advanced surveillance technologies in law enforcement. They include Schuck (2015), who found that the data could be used for purposes other than originally intended, including commercial and criminal activities. Almeida et al. (2023) found that the lack of transparency in law enforcement agencies creates avenues for the collected data to be abused and that this challenge is complicated by the fact that there is insufficient oversight for ensuring the data is appropriately

used. Alfonsi and Berliri (2021) and Ezzeddine et al. (2023) acknowledged the risk of having a surveillance state in which citizens are constantly monitored by the government, which restricts them from exercising their freedom and civil liberties. Ezzeddine et al. (2023) also found that the possible accuracy and accountability hitches regarding the use of the systems could translate into misidentification of individuals, leading to victimization.

Guidelines and Regulations for NPS to Use Advanced Surveillance Technologies

Most respondents (66%) agreed that there should be guidelines and regulations regarding the use of advanced surveillance technologies by the NPS, while 34% did not consider such guidelines as necessary (See Table 2.0 below). The respondents cited transparency and accountability as the key benefits of using guidelines and regulations when implementing advanced surveillance technology in law enforcement. Some specified that the use of the technology should be based on some legal authority, such as warrants, to prevent it from being used arbitrarily or for extortion by law enforcement agencies. They also noted that establishing specific guidelines and regulations will ensure that the data is safe and is only used for the purpose for which it is collected. Other respondents noted that the guidelines will specify how and when law enforcement officers can share the data they have collected, which will help prevent any data misuse.

These findings are corroborated by previous studies such as Alfonsi and Berliri (2021), who found the need to establish guidelines and regulations to balance protecting individual rights and civil liberties and public safety and security. Saheb (2022) found that guidelines and regulations are necessary for ensuring that transparency and accountability are achieved in using advanced surveillance technologies for law enforcement. This may include compelling law enforcement agencies to disclose the types of equipment they are using publicly and for what purposes they are using them. Additionally, Gstrein et al. (2019) established that advanced

surveillance technologies should be guided by some specified legal structures that specify how and when law enforcement agencies acquired some particular data and how they also use and destroy the data.

Public Education on the Use of Advanced Surveillance Technologies

The findings showed that 66% of the respondents supported the provision of public education about the use of advanced surveillance technologies in law enforcement by the NPS. However, 34% of the respondents did not see such a program as necessary (See Table 2.0 below). The respondents cited various reasons for their support for public education about law enforcement agencies' use of advanced surveillance technologies. This included understanding how law enforcement agencies will collect and use data from the public for their law enforcement purposes; they also needed to be informed of how the data will be safeguarded to have confidence in the system. The respondents also indicated that public education would help them understand how the enforcement officers will handle ethics regarding the data collected from the public and the measures they have put in place to ensure that the information is not misused. Some respondents considered public education an extension of civic practice because, through such forums, they could raise any questions about the surveillance systems and get feedback on them. Besides, the respondents noted that public education will increase awareness of the technologies currently being used and how they can potentially affect their civil liberties and individual rights.

These findings align with previous studies such as Maliphol and Hamilton (2022), who found that public education increases public awareness about surveillance technologies, ensuring that law enforcement agencies observe transparency and accountability in using the technology. Alfonsi and Berliri (2021) found that public education helps people appreciate their rights regarding law enforcement and understand how they can protect them. Fussey & Sadhu (2022) found that public education helps guide people to make informed

decisions about whether they should allow the use of advanced surveillance technologies in their neighborhoods.

Table 2: Responses on various elements of the use of advanced surveillance technologies in law enforcement

	YES	NO
Familiarity with Advanced Surveillance Technologies	(33) 66 %	(17) 34%
Ethical Implications of Using Advanced Surveillance Technologies in Law Enforcement	(28) 56%	(22) 44%
Privacy Violation Concerns	(42) 84%	(8) 16%
Guidelines and Regulations for NPS to Use Advanced Surveillance Technologies	(33) 66%	(17) 34%
Public Education on the Use of Advanced Surveillance Technologies	(33) 66%	(17) 34%

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Need for Enhancing Public Safety and Security	(10) 20%	(13) 26%	(14) 28%	(13) 26%	-

SUMMARY AND CONCLUSION

There is broad awareness of the advanced surveillance technologies used in law enforcement and public safety. These technologies include CCTV systems, facial recognition, license plate recognition, drones, forensic technology, and biometric systems. There is also increased awareness about the ethical implications of advanced surveillance technologies in law enforcement, including data security, privacy, freedom of expression, transparency, and accountability. Most reservations about using these technologies are based on concerns such as potential misuse, profiling, and intrusion. However, there is a need for using the technologies to enhance public safety and emergency response.

There are, however, ethical concerns associated with the adoption of these technologies. They include privacy violations, government abuse, a surveillance state, data security, these systems' accuracy, and potential data misuse. This calls for establishing guidelines and regulations for using advanced surveillance technologies in law enforcement. This will go a long way in ensuring transparency and accountability, and preventing arbitrary use of these technologies, thereby addressing concerns like data security and misuse. Besides, the need for public education about using advanced surveillance technologies in law enforcement cannot be overstated. This is one of the most effective approaches that the public, as the key stakeholder, can be involved in improving public safety and emergency response.

Recommendations

The following recommendations were made based on the findings and conclusions of the study:

- There is a need to develop and implement comprehensive public education programs for education members of the public about advanced surveillance technologies, including their capabilities, applications, and potential ethical concerns.

- The NPS should promote transparency by sharing information on how they use these technologies and how they can impact civil liberties and individual rights.

- The NPS should provide law enforcement officers with ongoing ethics training about the evolving advanced surveillance technologies. This will equip them with the requisite skills to use them best. The training should also enhance their understanding of ethical considerations and legal boundaries when using advanced surveillance technologies.

- The NPS and other relevant government authorities should establish and implement clear and robust guidelines and regulations governing the use of advanced surveillance technologies in law enforcement. They should ensure that the stipulated guidelines emphasize the necessity of obtaining warrants and legal authority for surveillance activities to prevent arbitrary use.

- The government should establish relevant authorities to oversee the implementation of mechanisms for oversight and accountability. These mechanisms will be invaluable for monitoring law enforcement agencies' use of advanced surveillance technologies.

REFERENCES

Alfonsi, A., & Berliri, M. (2021). Science, Ethics, and Responsible Research – The Case of Surveillance. In R. Iphofen & D. O'Mathúna (Eds.), *Ethical Issues in Covert, Security and Surveillance Research* (Vol. 8, pp. 17–28). Emerald Publishing Limited. https://doi.org/10.1108/S2398-601820210000008003

Almeida, D., Shmarko, K., & Lomas, E. (2023). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *Ai and Ethics,* 2(3), 377–387. https://doi.org/10.1007/s43681-021-00077-w

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* SAGE Publications.

Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). Safety, privacy, or both: Evaluating citizens' perspectives around artificial intelligence use by police forces. *Policing and Society*, 33(7), 861– 876. https://doi.org/10.1080/10439463. 2023.2211813

Fussey, P., & Sandhu, A. (2022). Surveillance arbitration in the era of digital policing. *Theoretical Criminology*, 26(1), 3–22. https://doi.org/10.1177/1362480620967020

Gstrein, O. J., Bunnik, A., & Zwitter, A. (2019). Ethical, Legal and Social Challenges of Predictive Policing. (SSRN Scholarly Paper 3447158). https://papers.ssrn.com/abstract=3447158

Harper, D. J., Ellis, D., & Tucker, I. (2021). Covert Aspects of Surveillance and the Ethical Issues They Raise. In R. Iphofen & D. O'Mathúna (Eds.), *Ethical Issues in Covert, Security and Surveillance Research* (Vol. 8, pp. 177–197). Emerald Publishing Limited. https://doi.org/10.1108/S2398-601820210000008013

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management,* 24(3), 325–335. https://doi.org/10.1177/14613557221089558

Johnson, B., & Christensen, L. (2014*). Educational Research: Quantitative, Qualitative, and Mixed Approaches.* SAGE Publications.

Kothari, C. R. (2014). *Research Methodology: Methods and Techniques*. New Age International Ltd.

Laufs, J., & Borrion, H. (2022). Technological innovation in policing and crime prevention: Practitioner perspectives from London. *International Journal of Police Science & Management,* 24(2), 190–209. https://doi.org/10.1177/14613557211064053

Liaropoulos, A. (2020). A Social Contract for Cyberspace. *Journal of Information Warfare*, 19, 2 (2020). 29, 1–11.

Maliphol, S., & Hamilton, C. (2022). Smart Policing: Ethical Issues & Technology Management of Robocops. *2022 Portland International Conference on Management of Engineering and Technology (PICMET),* 1–

15. https://doi.org/10.23919/PICMET53225. 2022.9882871

Manes, J. (2019). Secrecy & Evasion in Police Surveillance Technology. *Berkeley Technology Law Journal*, 34(2), 503–566.

Power, D. J., Heavin, C., & O'Connor, Y. (2021). Balancing privacy rights and surveillance analytics: A decision process guide. *Journal of Business Analytics,* 4(2), 155–170. https://doi.org/10.1080/2573234X.2021.1920 856

Raposo, V. L. (2022). The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal. *European Journal on Criminal Policy and Research, 29(4),* 515– 533. https://doi.org/10.1007/s10610-022-09512-y

Saheb, T. (2023). Ethically contentious aspects of artificial intelligence surveillance: A social science perspective. *AI and Ethics*, 3(2), 369– 379. https://doi.org/10.1007/s43681-022-00196-y

Sapp, S. G., Dorius, S. F., Bertelson, K. A., & Harper, S. B. (2021). Public support for government use of network surveillance: An empirical assessment of public understanding of ethics in science administration. *Public Understanding of Science,* 31(4), 489–506. https://doi.org/10.1177/09636625211049531

Schuck, A. (2015). Prevalence and Predictors of Surveillance Cameras in Law Enforcement: The Importance of Stakeholders and Community Factors. *Criminal Justice Policy Review,* 28. https://doi.org/10.1177/0887403415570631

Seabright, P., Stieglitz, J., & Van der Straeten, K. (2021). Evaluating social contract theory in the light of evolutionary social science. *Evolutionary Human Sciences,* 3, e20. https://doi.org/10.1017/ehs.2021.4

Singh, D. (2022). The Causes of Police Corruption and Working towards Prevention in Conflict-Stricken States. *Laws*, 11(5), Article 5. https://doi.org/10.3390/laws11050069

Urquhart, L., & Miranda, D. (2022). Policing faces: The present and future of intelligent facial surveillance. *Information & Communications Technology Law,* 31(2), 194– 219. https://doi.org/10.1080/13600834. 2021.1994220

Van Brakel, R., & Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology-based strategies. *Journal of Police Studies,* 20, 163–192.

Zheng, T. (2016). Advanced Surveillance Technologies: Privacy and Evidentiary Issues. *Cornell Law School J.D. Student Research Papers.* https://scholarship.law.cornell.edu/lps_papers/37