THE BALANCE BETWEEN PRIVACY AND SAFETY: THE ETHICS OF PUBLIC VIDEO SURVEILLANCE

Sergiu DOBOȘ[*], Victor BAGRIN

Department of Software Engineering and Automation, group FAF-232, Faculty of Computers, Informatics, and Microelectronics, Technical University of Moldova, Chisinau, Republic of Moldova

*Corresponding author: Sergiu Doboș, sergiu.dobos@isa.utm.md

Tutor/coordinator: **Elena GOGOI**, university lecturer, Department of Software Engineering and Automation, Faculty of Computers, Informatics, and Microelectronics, Technical University of Moldova, Chisinau, Republic of Moldova

Abstract. The following article explores the balance between privacy and safety in the context of public video surveillance from an ethical perspective. It aims to study its impacts on individual privacy, public security, and social norms. This research provide an in-depth investigation of the implications of surveillance through a detailed analysis based on an extensive review of academic literature, press articles, and surveys. While surveillance undeniably aids in crime prevention and investigation, it also raises critical concerns about personal freedom and the risk of mass monitoring. The paper begins with the positive aspects of public video surveillance on the well-being of society and continues with its potential downsides such as privacy violation. Legal considerations are an essential part of the analysis. These findings highlight the importance of a balanced approach between public safety and individual confidentiality, contributing to a comprehensive understanding of public surveillance's ethical aspect and its impact on society. This study enhances the ethical debate on public surveillance, suggesting that achieving an equilibrium between privacy and safety is both a possible and a crucial objective.

Keywords: *crime prevention, mass monitoring, personal freedom, public safety, surveillance ethics.*

Introduction

The roots of video surveillance date back to the mid-20th century, when Closed-Circuit Television (CCTV) technology was developed by Walter Bruch and initially implemented in Germany in 1942 to record live video. During the war, this primitive version of CCTV was used to observe V-2 rockets. It took another seven years, until 1949, for CCTV systems to be sold commercially. However, its widespread application began to take hold gradually with the rapid development of technologies in recent years. Primarily, it served as an essential surveillance tool in high-risk areas, but today it is omnipresent around the world. Still, the majority of the public agrees that the presence of surveillance cameras is essential for their security and the places where they are located. An article from the The New York Times states that “A week after the Boston Marathon attack, which was unraveled after the release of video footage of the two suspects flushed them out of hiding, 78 percent of people said surveillance cameras were a good idea, the poll found” [1]. However, nowadays, the use of Artificial Intelligence (AI) and Facial Recognition Technologies (FRT) is increasing, serving as enhanced tools in detecting and preventing crimes, but on the other hand, when used for non-democratic purposes, they can raise questions regarding the respect for individuals' rights.

These technologies, besides the numerous benefits they bring, can also pose an ethical problem. On one hand, video surveillance enhanced with these technologies serves as an indispensable tool for law enforcement and security agencies, not only by preventing crimes but also for further investigation of them, and a rapid response from authorities in emergencies. Standalone surveillance cameras function as a deterrent to criminal activities, and monitoring and video recording can serve as essential tools in police or legal investigations. On the other hand, these surveillance systems can erode individual freedom and privacy, entail unnecessary surveillance, and foster biased practices through these technologies. Such concerns highlight the need for more research and regulations in this field, especially from a moral and ethical standpoint. We continue to explore this issue from multiple perspectives and propose several solutions to reach a consensus that respects both public interests and the individual's right to freedom and privacy. The surveillance methods that are used include CCTV, license plate recognition, face recognition, social media monitoring, and so on, all aiming to ensure the safety of the public. All these technologies aim to help prevent and solve crimes, but they also raise controversies around privacy risks.

Understanding the Role of Public Video Surveillance

It is undeniable that the emergence of video monitoring systems provides indispensable tools for ensuring public safety in our society. Public video surveillance is valuable in several fields, providing benefits for both law enforcement agencies and the public. One of the primary roles of video surveillance is to prevent and deter criminal activities within the coverage area and beyond, including but not limited to, thefts, break-ins, attacks, vandalism, fights, hooliganism, and more. Studies show that criminal activity in public spaces, where surveillance cameras have been installed, has significantly decreased. A scientific article published in the academic journal "International Journal of Law, Crime and Justice" reports that in South Korea "The number of robberies and thefts in the areas with CCTV installed reduced by 47.4%" [2]. Moreover, unaltered video recordings serve as key evidence in crime investigations. Law enforcement agencies can use footage to identify suspects, reconstruct events, convict the guilty, or even confirm alibis or withdraw charges.

In addition to crime prevention and police investigations, video surveillance plays an important role in accountability in case of an emergency. Video surveillance systems, typically equipped with real-time monitoring capabilities, allow for a rapid response from emergency crews in situations such as accidents, natural disasters, fires, cases of violence, and so on. Thus, with the help of monitoring, emergency assistance can be provided quickly, efficiently, and safely, thanks to the accurate detection of emerging problems. At the same time, public surveillance technologies can serve as a help in safely controlling public events, traffic, mass gatherings, or any other public situations, effectively contributing to the satisfaction of public safety of individuals in public spaces. Facts confirmed by a survey from a study at the University of North Carolina, which states that "A majority [of participants] also expressed that the presence of video surveillance systems made them feel safer" [3].

Concerns and Ethical Considerations

In addition to the undeniable benefits of using video surveillance tools, their continuous development also raises several ethical questions regarding the balance between public safety and privacy concerns. At the core of these considerations is the tension between social safety and individual freedom. The biggest questions revolve around issues such as the infringement of personal freedoms, data security, moral implications such as biased arrests, or a permanent state of surveillance, especially when systems enhanced with Artificial Intelligence are used. Most concerns are about the misuse of these systems, which can pose a potential threat to individual security, privacy, and democratic values.

In most cases, video surveillance, particularly that which employs Facial Recognition Technologies, can pressure autonomy and personal freedom. These tools can impose restrictions on an individual or a group, undermining basic democratic rights such as freedom of expression, association, or belonging to a group or idea. For example, video surveillance systems equipped with Facial Recognition Technologies were used during the protests for democracy in Hong Kong that took place in 2019-2020, to identify and arrest participants, and to facilitate the rapid intervention of law enforcement to stop these protests. According to an article in The New York Times “Many protesters now cover their faces, and they fear that the police are using cameras and possibly other tools to single out targets for arrest” [4]. Additionally, an article by the Hong Kong Free Press mentions that “Hong Kong’s government has announced plans to install 2,000 additional CCTV cameras in public places this year in what it calls a move to fight crime” [5]. Thus, concerns are fueled regarding the guarantee of personal freedom. A study from the Technical University of Munich states that “Remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into individuals’ private lives, with severe effects on the populations’ expectation of being anonymous in public spaces” [6].

Like any information system, video surveillance systems can be vulnerable to security breaches through which collected data can be leaked, falling into the hands of malicious third parties. The risks increase when personal and biometric data of individuals are constantly collected and stored, thus posing risks of unauthorized access to very sensitive data. Furthermore, the lack of transparency in processing this data only increases the risks associated with threats to individual security and privacy rights. A 2024 CNN article presents a similar situation where “About 13,000 users “experienced a security issue” where they saw wrong thumbnails from other users in the Wyze app. About 1,500 users clicked on the tabs showing the other people’s footage, which enlarged the thumbnail and, in some cases, allowed people to view footage from other users' cameras” [7].

The increasing presence of video surveillance systems can also raise ethical and moral issues. For example, the use of surveillance tools combined with Artificial Intelligence and Facial Recognition Technologies can increase the risk of biased arrests, as the training data can be altered with biased data present in our society such as different classifications of the actions of a person or a group of people based on age, gender, skin color, etc. The same study from the Technical University of Munich also states that “Not only is everyone that uses public space under surveillance without being a suspect of any crime, but the process can trigger an automated decision leading to police action. […] Bias in AI is only one of the possible causes” [6]. Thus, in addition to amplifying inequity in our society, these issues can decrease society's trust in public authorities.

As video surveillance becomes more widespread, it can fundamentally alter how an individual behaves in public space, not necessarily signifying something positive, thus potentially infringing on rights to personal freedom of expression, such that “The banalization of surveillance can create a chilling effect that leads to the naturalization of further constraints to individual and public liberties, hampering autonomy by hindering choice and uncoerced decisions and undermining basic democratic practices linked to fundamental rights, such as freedom of association and expression” [6]. Additionally, the problem of consent in using images or personal data without the explicit permission of those monitored adds another layer of complexity to the ethical issue. Individuals are often not aware that their data is collected, how it is used, or whether they have any control over it, thus harming the fundamental principles of autonomy and consent.

Balancing Safety and Privacy

Achieving a balanced equilibrium between ensuring safety and respecting privacy requires a complex approach that includes technical, legal, and ethical considerations. As society becomes increasingly interconnected and reliant on technology, the use of public video surveillance is rapidly accelerating, raising challenges in balancing public security and individual privacy rights.

To address issues surrounding public surveillance, a well-defined regulatory framework is essential. Such a framework should clearly define the purposes for which surveillance can be used, the type of data that can be collected, and the duration for which it can be stored, among other things. For instance, the law could mandate that surveillance data be used solely for public security purposes and not for monitoring peaceful protests or other similar lawful activities. In the European Union, a strict set of guidelines known as the General Data Protection Regulation

(GDPR) governs the processing of personal data and benefits individual rights, enabling one to request access to or control over all personal data concerning them.

Transparency in the use of surveillance technologies is crucial for gaining public trust. Public authorities should disclose the locations of cameras, the technologies used, and the reasons for surveillance, and should also provide individuals with access to and control over the data collected about them. For example, the Regulation on Video Surveillance Within the Public Institution "Technical University of Moldova" stipulates that "Surveillance cameras are placed in visible locations. Any covert use of these cameras is strictly prohibited, except in cases expressly regulated by legislation" [8]. Regular audits and public reports on the effectiveness and impact of surveillance systems can maintain transparency and trust. Moreover, independent entities can be established to oversee the operation of monitoring systems to ensure they operate within legal frameworks and respect human rights. A report by the U.S. National Science and Technology Council proposes several actions to improve transparency in data use and increase trust in law enforcement: "The following federal actions could help improve law enforcement agencies' data practices and contribute to improving trust in police. […] Law enforcement agencies need to build capacity – in technology, human capital, training, and other resources – to effectively capture, use, and publish data, while software vendors need to lower the barriers to the effective use of their tools. […] Making data available and accessible to stakeholders and the public is key to promoting transparency and reducing inequities" [9].

The advancement of technologies also provides solutions to concerns about individual privacy. Privacy-enhancing technologies (PETs), such as automatic blurring of faces in video feeds or algorithms that identify behavioral patterns without identifying individuals, can help minimize privacy intrusions. A 2022 study proposes a similar system that can improve the outcomes of public surveillance by using neutral artificial intelligence algorithms: "In this design, we avoid using algorithms that use identifiable information, such as pixel-based algorithms. The most important parts of the system, such as anomaly detection, action recognition, and global re-identification, use skeleton and abstract feature representation. As a result of this approach toward the algorithm, neither the inputs nor the outputs are identifiable information. Moreover, the outputs are race, gender, age, and ethnicity neutral. This specific aspect of the system addresses the issue of discrimination as a fundamental ethical challenge in the public safety domain" [10]. This approach excludes unnecessary monitoring of individuals, enhancing the efficiency of public video surveillance and reducing concerns about the security of individual privacy.

Involving the public in decision-making about when, where, and how surveillance technologies are implemented can help balance public safety and individual privacy security. Public consultation and debates should be encouraged to assess the community's needs. Additionally, policies that require explicit community consent before the installation or use of surveillance systems can significantly improve public trust and cooperation. For example, in the Republic of Moldova, the protection of personal data is guaranteed by Law 133 of 08-07-2011. Article 5 of this law states: "The processing of personal data is carried out with the consent of the data subject" [11].

Conclusions

In conclusion, the use of technologies for public video surveillance presents an undeniable advantage, significantly aiding in enhancing public security and assisting law enforcement in their work. At the same time, it also brings ethical challenges that should not be underestimated. The balance between security and privacy is extremely delicate, demanding a thorough analysis and careful implementation of regulatory mechanisms from a legal, social, and moral standpoint. As technology grows and improves day by day, including Artificial Intelligence and Facial Recognition Technologies, to protect individual freedoms and privacy, legal frameworks like GDPR should be implemented to guarantee basic human rights. Additionally, the deployment of these tools must also come with the population's trust regarding the respect of their rights, and even more so with an extremely high level of transparency to dispel any suspicions of malicious use of these tools. Therefore, society must be directly involved in this process through participation in decision-making, as well as in surveys and studies in this field. It is vitally important to remember that the key priorities are, ultimately, the protection of democratic values and individual freedoms, while we address the complexities that advanced surveillance capabilities bring in developing a safer society.

References

[1] M. Landler and D. Sussman, "Poll Finds Strong Acceptance for Public Surveillance," *The New York Times*, Apr. 30, 2013. [Online]. Available: https://www.nytimes.com/2013/05/01/us/poll-finds-strong-acceptance-for-public-surveillance.html

[2] H. H. Park, G. Oh, and S. Y. Paek, "Measuring the crime displacement and diffusion of benefit effects of open-street CCTV in South Korea," *International Journal of Law, Crime and Justice*, vol. 40, no. 3, pp. 179–191, Sep. 2012, doi: 10.1016/j.ijlcj.2012.03.003.

[3] B. R. Ardabili *et al.*, "Exploring Public's perception of safety and video Surveillance Technology: A survey approach," *arXiv (Cornell University)*, Dec. 2023, doi: 10.48550/arxiv.2312.06707.

[4] P. Mozur, "In Hong Kong Protests, Faces Become Weapons," *The New York Times*, Jul. 26, 2019. [Online]. Available: https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html

[5] I. Chan, "Hong Kong to install 2,000 more CCTV cameras in 2024," *Hong Kong Free Press HKFP*, Jan. 18, 2024. [Online]. Available: https://hongkongfp.com/2024/01/18/hong-kong-to-install-2000-more-cctv-cameras-in-2024-top-official-says-total-number-in-city-relatively-small/

[6] C. Fontes and C. Perrone, "Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement," *Technical University of Munich*, Dec. 2021. [Online]. Available: https://ieai.mcts.tum.de/wp-content/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf

[7] J. Valinsky, "About 13,000 home security customers were shown someone else's home," *CNN*, Feb. 20, 2024. [Online]. Available: https://edition.cnn.com/2024/02/20/tech/wyze-breach-camera/

[8] "Regulament privind supravegherea prin mijloace video în cadrul Instituţiei Publice 'Universitatea Tehnică a Moldovei'." [Online]. Available: https://utm.md/acte_normative/interne/Reg.supr.video.pdf

[9] "Equity And Law Enforcement Data Collection, Use, And Transparency," 2023. Available: https://www.whitehouse.gov/wp-content/uploads/2023/05/NSTC-Equity-and-Law-Enforcement-Data.pdf

[10] "Lege Nr. 133 din 08-07-2011 privind protecția datelor cu caracter personal." [Online]. Available: https://www.legis.md/cautare/getResults?doc_id=136439&lang=ro

[11] B. R. Ardabili *et al.*, "Understanding ethics, privacy, and regulations in smart video surveillance for public safety," *arXiv (Cornell University)*, Dec. 2022, doi: 10.48550/arxiv.2212.12936.