UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF POLITICAL SCIENCE, LAW, AND INTERNATIONAL STUDIES

Master's degree in Human Rights and Multi-level Governance



Surveillance vs. Privacy

Assessing the Implications of CCTV Cameras for Crime Prevention on the Right to Privacy in the United Kingdom

Supervisor: Prof. Andrea Maria Maccarini

Candidate: Niki Jabbari

Matriculation No.: 2014325

Abstract

The right to privacy is recognized as a fundamental human right in international human rights law and is crucial to the protection of personal autonomy and dignity. The concept of privacy has been a long-standing issue in society, and its importance has increased with the advent of new technologies that allow for the collection and analysis of personal data on an unprecedented scale. Technological advancements have led to significant changes in the way privacy is perceived and protected. Al-powered surveillance systems have made it possible to monitor people's movements, activities, and behavior. While these technologies considerably help public and private agencies identify criminals and safeguard public order, they may violate people's privacy in relation to their communications, actions, and other elements. This research study examines the impact of using CCTV cameras for the purpose of crime prevention on the right to privacy in the United Kingdom. With the growing implementation of surveillance technologies, such as CCTV cameras, there is a need to critically assess their implications on individual privacy rights. This research focuses on understanding the balance between enhanced security measures and the potential infringement on privacy rights.

Keywords: CCTV Cameras, crime prevention, privacy

Introduction

Each individual possesses fundamental human rights outlined in international law. One of the indispensable human rights which all human beings should own is the right to privacy. As well, states must implement all measures to protect, preserve, and respect people's privacy rights.

However, in certain conditions, the right to privacy could be restricted. As indicated in international human rights law, state parties can constrain people's lives, movements, and behaviors if this restriction is essential to prevent criminal activities, ensure national security, and provide a sense of personal safety among people.

In this modern age, the majority of states in the world use surveillance systems to review people's life and collect, use, and share their personal information. A wide range of Artificial Intelligence-powered surveillance systems are employed by people or any organizations in houses, workplaces, and public areas to monitor people's behaviors in the community.

Technological improvement in surveillance system technologies can significantly impact people's right to privacy. These technologies are valuable instruments for preventing crimes, detecting potential offenders, and protecting people in society.

However, the extensive surveillance systems in public and private places by people or organizations could monitor all individual movements and intrude on people's right to privacy. Therefore, it gives people the impression that they are under massive surveillance and they would not be able to lead their everyday activities as usual.

Closed Circuit Televisions (CCTV) cameras are a critical surveillance system commonly used in numerous countries. CCTV is a network of cameras that can capture people's images and surroundings in a specific area. Besides CCTV cameras, there are several control rooms. The control room is an ample space where competent operatives watch CCTV footage on several screens. The recorded footage can be observed in real-time or later for various purposes.¹

Many countries worldwide use a considerable percentage of CCTV cameras in public places. For instance, a substantial number of CCTV cameras exist in the United Kingdom, particularly in crowded cities like London. The statistics show approximately 6 million Closed Circuit Televisions (CCTV) cameras throughout the country. This number demonstrates that the United Kingdom has the highest concentration of camera surveillance systems compared to European countries.

CCTV cameras provide several benefits and have contributed to beneficial impacts in many aspects of people's lives. Individuals are under massive surveillance by network cameras. The CCTV cameras record every people's movement in many places, like streets, roads, transportation infrastructures, and private properties. The recorded footage can prevent crime before it is committed, provide evidence for police and law enforcement authorities in the investigation process, and improve public order.

CCTV cameras serve as an effective instrument to prevent property and personal crimes. If the potential offenders are aware that the camera surveillance systems in society will monitor all their activities, they will likely avoid committing crimes. CCTV systems in many places can significantly reduce certain types of crimes, such as vehicle crimes, robbery, and even terrorist attacks.

¹ CameraFTP.com offers home monitoring, computer monitoring, Kids Monitoring, PC monitoring /screen recording and cloud recording services.

https://www.drivehq.com/features/personal/cameraftp.aspx

In addition, CCTV cameras are crucial instruments in criminal investigations. The police and law enforcement authorities could use CCTV footage to collect evidence and uncover all information about illegal behaviors. They can track crimes committed within the view of CCTV cameras and receive relevant information they seek, including specific time, location, and date of the criminal behaviors.

As a result, all people are under constant surveillance in many places. CCTV cameras ensure people that all their activities are monitored by police and security authorities, and they can implement effective measures to prevent all kinds of crimes. Thereby, it can spread the feeling of personal safety throughout the community.

Although increasing Al-powered surveillance systems, specifically CCTV cameras, improve community safety, it may result in privacy concerns. Many people might believe that their activities are constantly being viewed by government officials, non-governmental organizations, and other individuals without their prior consent and knowledge.

CCTV cameras installed in the United Kingdom have profoundly impacted individual privacy rights. Some argue that video surveillance technologies can record all individuals' movements, behaviors, and communications and capture their personal information, which can be considered an intrusion into the right to privacy.

Therefore, technological developments substantially changed human beings' private lives. The Legislative and judicial bodies have the power to establish a set of rules and regulations to protect people's private lives and help them keep their rights to privacy when new monitoring technologies systems challenge it.²

In this research, first of all, we look into the concept of privacy and then examine international human rights treaties which protect individual's right to privacy, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights (ECHR), the Convention for the Protection of Individuals concerning Automatic Processing of

_

² Anderson, S. A. (2008). Privacy without the Right to Privacy. *The Monist*, *91*(1), 81–107. http://www.jstor.org/stable/27904067

Personal Data, and General Data Protection Regulation (GDPR).³ Besides that, we discuss the circumstances based on which the states would be able to constrain the right to privacy.

Furthermore, we examine the percentage of CCTV cameras in the United Kingdom and compare it with other countries in the world. According to recent statistics, following China and the United States, the United Kingdom has the most significant CCTV surveillance cameras, and major cities comprised of London, Liverpool, and Manchester have a high density of CCTV cameras per person.

Finally, we assess how CCTV cameras influence people's right to privacy. Indeed, many critics argue that the installation of cameras surveillance systems can result in privacy concerns, which include:

Firstly, CCTV footage should be stored for a reasonable time based on each case. However, some individuals or groups, private or public, might store CCTV footage that provides information about individuals' facial features, movements, and communications for more than they need for the stated purpose in a searchable database.

Secondly, individuals or groups are likely to use numerous surveillance technologies, particularly CCTV cameras, to prevent crime occurrences in the community without clear, specific, and informed consent from the monitored people. Many people are not notified of the existence of camera surveillance systems, and it could be considered an intrusion into an individual's privacy rights.

Thirdly, CCTV footage should be collected for specific purposes. However, in the United Kingdom, there is 1 CCTV camera for every ten people, and the images captured by CCTV cameras are probable to be misused for other purposes other than for which they initially intended, which can significantly influence people's privacy rights.

Fourthly, the other challenge is a need for more transparency or accountability regarding CCTV footage in most countries, like the United Kingdom. People should be made aware of the CCTV camera process, and there needs to be more

³ State of Privacy Mexico | Privacy International. https://privacyinternational.org/state-privacy/1006/state-privacymexico

information on how footage is captured by video surveillance, how it is processed, and ultimately who can access an individual's images and footage.

Ultimately, one of the problems of CCTV cameras with privacy rights is that closed circuit cameras situated in public spaces might need to be correctly managed because people's personal information is subject to cyber-attacks. It means that unauthorized persons would be able to access an individual's private information and intrude on people's personal lives.⁴

The Concept of Privacy

The notion of "Privacy" is a controversial concept in international human rights law. Different countries have a multitude of opinions on the constitutional right to privacy. There are arguments among policymakers and law enforcement officials about how "privacy" is defined and distinguished from other fundamental human rights.

Although the provision of a precise definition of the word "privacy" could be challenging, many scholars on human rights law attempt to constitute specific criteria and establish borders between "privacy" and other individuals' human rights, such as the right to expression, speech, thought, and freedom.⁵

All individuals in the world are entitled to possess the right to privacy. The right to privacy provides all human beings with the constitutional right to control their own private lives, and no individual or group could access an individual's private areas, belongings, and information in an illegal manner.⁶

Moreover, according to Scott A. Anderson, it is the legal responsibility of state parties to decide and take into account issues like what facts about one's own life someone could reveal, to whom, and under what circumstances to set boundaries that safeguard a person's private information from disclosure by others.⁷

⁴ Turtiainen, Hannu & Costin, Andrei & Hämäläinen, Timo. (2022). CCTV-Exposure: System for measuring user's privacy exposure to CCTV cameras.

⁵ Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/10.2307/3481326

⁶ Alibeigi, Ali & Munir, Abu & Karim, Md. (2019). Right to Privacy, A Complicated Concept to Review. SSRN Electronic Journal. 10.2139/ssrn.3537968.

⁷ Anderson, S. A. (2008). Privacy without the Right to Privacy. *The Monist*, *91*(1), 81–107. http://www.jstor.org/stable/27904067

Each individual can control their personal information on different aspects of their life. As Serohin Vitalii mentioned: "information privacy is a certain «imprint» of a person's private life in the form of certain information (data) about the relevant facts, phenomena, and events that relate to a person's private life, and therefore this information is a priori confidential, and the access mode can only be changed (weakened) by itself."

As a result, as outlined in international human rights law, every human being in the world has a constitutional right to control their personal matters concerning all aspects of their life. As well, all state parties are obligated to respect, protect and promote people's personal information, communications, family life, and correspondence. They also should prevent any unlawful interference with people's privacy rights.

The Right to Privacy in International Human Rights Law

In international human rights law, there are many international conventions that ensure people's basic human rights and fundamental freedoms. State parties should comply with human rights treaties ratified in international law and prevent any human rights violations in the future.

Human rights are fundamental rights inherent to all individuals without discrimination worldwide. According to Article 2 of the Universal Declaration of Human Rights: "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." ¹⁰

Moreover, International Covenant on Civil and Political Rights is one of the critical international conventions in human rights law. Article 2(1) of the convention states: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as color, sex, language, religion, political or other opinions, national or social origin, property, birth or other status." This article emphasizes that all

⁸ Vitalii, Serohin. (2021). INFORMATION PRIVACY: A CONCEPTUAL APPROACH. Constitutional and legal academic studies. 52-60. 10.24144/2663-5399.2020.2.06.

⁹ McCloskey, H. J. (1980). Privacy and the Right to Privacy. *Philosophy*, *55*(211), 17–38. http://www.jstor.org/stable/3750973

¹⁰ The Universal Declaration of Human Rights, 1948. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

¹¹ "International Covenant on Civil and Political Rights." *Human Rights Quarterly*, vol. 7, no. 1, 1985, pp. 132–54. *JSTOR*, https://doi.org/10.2307/762040. Accessed 20 Jul.2022.

human beings have equal rights and should not be discriminated against based on their personal characteristics.¹²

According to international human rights law, all people are entitled to all fundamental rights and freedoms set forth in international documents. These rights include the right to work, education, fair trial, etc. The right to privacy is one of the critical human rights recognized by all international and regional human rights conventions.

Each individual possesses the legal right to privacy. A range of international documents outlines fundamental rights, specifically the right to privacy. These treaties include the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights (ECHR), the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data, and the General Data Protection Regulation (GDPR).

State should attempt to inform everyone of their privacy rights outlined in international treaties and encourage people to realize the significance of this right, incorporate them into their daily lives, and intervene to enhance and defend others' rights on a national and international level which can contribute to the improvement of society, both individually and collectively.¹³

The state parties will be obligated to provisions to which they have agreed, and all individuals should be entitled to private life, the home, and correspondence. Also, at national, regional, and international levels of governance, several human rights monitoring institutions are established to evaluate how well national human rights obligations are implemented and to hold governments accountable for their commitment to prevent, protect and fulfill people's rights to privacy.¹⁴

The widespread use of surveillance systems prompted international organizations and states to create a set of rules and regulations to preserve, protect and respect

¹² Waltz, S. (2002). Reclaiming and Rebuilding the History of the Universal Declaration of Human Rights. *Third World Quarterly*, *23*(3), 437–448. http://www.jstor.org/stable/3993535

¹³ Patel, Jayantibhai. (2007). Human Rights Education.

¹⁴ Huffstetler, Hanna & Mesquita, Judith & Meier, Benjamin. (2020). Monitoring and Review to Assess Human Rights Implementation. 10.1093/oso/9780197528297.003.0008.

people's right to privacy against any infringement upon their private life, behaviors, and communications.

Some of these conventions protect all fundamental rights of individuals, including the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR), the Convention on the Rights of Persons with Disabilities (CRPD), the American Convention on Human Rights (ACHR), at the same time, a number of them specifically refer to protect and promote the right to privacy, like the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and General Data Protection Regulation (GDPR).

1. General International Conventions

International organizations have enacted a wide range of international human rights agreements and treaties to respect and preserve people's fundamental human rights, including the right to privacy. These critical conventions are:

1-1. Universal Declaration of Human Rights (UDHR)

The UN's General Assembly introduced the Universal Declaration of Human Rights on December 10, 1948.¹⁵ This declaration is the most important document in international human rights law. The UDHR ensures that all people worldwide possess fundamental rights and freedoms.

Based on UDHR, each person has the right to privacy. On the basis of article 2: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." ¹⁶

Therefore, all individuals have a legal right to live their own private lives. In addition, state parties are obliged to implement measures to respect, preserve, and protect people against any infringement upon their private life.

1-2. International Covenant on Civil and Political Rights (ICCPR)

¹⁵ How many days until Human Rights Day 10 December?. https://www.daysuntil.net/december-10-2023

¹⁶ Is the Right to Privacy a Human Right? - Klinik Hukumonline. https://www.hukumonline.com/klinik/a/is-the-right-to-privacy-a-human-right--lt63d0eaa88a7ae/

International Covenant on Civil and Political Rights (ICCPR) is the second human rights treaty. This convention was ratified by the United Nations General Assembly on December 16, 1996, and entered into force on 23 March 23, 1976.¹⁷

Conforming to Article 17 of ICCPR:

- "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor and reputation.
- 2. Everyone has the right to the protection of the law against such interference or attacks."

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) recognizes the right to privacy as one of the basic human rights and protects all people against any illegal breach of their private lives.¹⁸

1-3. European Convention on Human Rights (ECHR)

European Convention on Human Rights is a crucial international convention that became open for signature on 4 November 1950 and entered into force in 1953.¹⁹ This convention aims to protect the fundamental rights and freedoms of people, including freedom of religion, expression, speech, and freedom from any arbitrary interference with people's privacy rights.²⁰

As mentioned in Article 8 of the European Convention on Human Rights (ECHR):

- "1. Everyone has the right to respect for his private and family life, his home, and his correspondence.
- 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."²¹

Article 8 of the ECHR prohibits infringement upon an individual's personal information and activities and provides the right to respect for private and family

¹⁷ Louanne Meunier, Author at mcalisterhallam.com. https://mcalisterhallam.com/author/louanne-meunier/

¹⁸ Anderson, A., Miller, D., & Newman, D. (2018). Canada's Residential Schools and the Right to Integrity. Dalhousie Law Journal, 41(2), 301A.

¹⁹ Knowledge Center | Human Rights Defense Curaçao. https://humanrightsdefense.org/knowledge-center/

²⁰Coblentz, W. K., & Warshaw, R. S. (1956). European Convention for the Protection of Human Rights and Fundamental Freedoms. *California Law Review*, *44*(1), 94–104. https://doi.org/10.2307/3478312

²¹ ECHR Art. 8 - Africa's Business. https://africasbusiness.com/echr-art-8/

life. Although Article 8 of the Convention protects the right to respect private and family life, home, and correspondence, all state parties should also implement positive measures to respect privacy rights, particularly against technological surveillance systems which monitor all behaviors, activities, and movements of people in the society and intrude into individual's lives.

1-4. Convention on the Rights of Persons with Disabilities (CRPD)

The Convention on the Rights of Persons with Disabilities (CRPD) is an international treaty adopted by the United Nations General Assembly in 2006 and approved by over 180 countries to protect, promote, and ensure the human rights and fundamental freedom of people with disabilities.

According to article 22 of this convention:

- "1. No person with disabilities, regardless of the place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honor and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.
- 2. States Parties shall protect the privacy of personal, health, and rehabilitation information of persons with disabilities on an equal basis with others."

Therefore, as we declared, although researchers could not agree upon the boundaries of privacy, everyone in the world would concur that each person, without any discrimination based on personal characteristics, has a legal right to privacy. All individuals, including persons with disabilities, have the right to the protection of the law against such unlawful interference or attacks against his or her privacy, family, home or correspondence, or other types of communication or to unlawful attacks on their honor and reputation.

1-5. American Convention on Human Rights (ACHR)

The other crucial international instrument is American Convention on Human Rights (ACHR). This convention was ratified by the Organization of American States (OAS) member states in 1969 to protect, promote, and respect all individual human rights.

The American Convention on Human Rights is one of the international conventions which protect individuals' privacy. Article 11 of ACHU states:

"1. Everyone has the right to have his honor respected and his dignity recognized.

- 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
- 3. Everyone has the right to the protection of the law against such interference or attacks."

2. Specific International Conventions

The advancement in technology has resulted in significant changes in human rights law. It has prompted international organizations to create several conventions related to data protection and privacy issues to respect, protect, and preserve all people's right to privacy. There are two essential conventions about the protection of people's personal information. These conventions include:

2-1. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

The first international convention is the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data. This convention is one of the legally binding international agreements adopted by the Council of Europe in 1981 and aims to protect individuals' right to privacy and personal data in the context of automated processing of personal data.

It introduced a set of rules and regulations to ensure that in automatic procession, an individual's personal data is protected by member states, and no one could have unlawful access to any identifiable or identifiable individual's information. According to article 2(c) of this convention: ""automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination."²²

Indeed, it was ratified to protect, promote, and ensure every person's basic human rights and fundamental freedoms, especially the right to privacy. It includes a set of principles related to the duties of parties, quality of data, additional safeguards for the data subject, data security, special categories of exceptions and restrictions, sanctions, and remedies that all state parties should respect.

²² Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28 L1981

Therefore, as one of the essential laws, the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data establishes a range of rules to protect, preserve, and safeguard people's personal information in the context of automated procession.

2-2. General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) is the most crucial instrument for protecting personal information. This convention was adopted by the European Union and set out fundamental principles to guarantee personal data and individuals' private lives. In 1995, the European Union introduced the Data Protection Directive 95/46/EC to enforce rigorous guidelines to preserve, promote and defend individuals' privacy and personal data against unlawful or illegal intrusions by individuals or other organizations.

As new technologies emerged, the 1995 regulation failed to take into consideration critical factors that impact data protection and privacy, so in response to the deficiencies of the previous regulation, the European Union adopted the new proposal, General Data Protection Regulation in 2012, which was specifically designed to address the crucial issues concerning data protection and privacy rights.²³

The General Data Protection Regulation (GDPR) is one of the important data protection laws that aim at providing legal protection to preserve personal data and imposes several strict obligations on organizations throughout European countries for those who violate individual privacy rights.²⁴ This regulation states a series of principles with regard to the processing of personal data, the lawfulness of processing, conditions for consent, criminal offenses, and rights of the data subject.²⁵

The Restriction to the Right to Privacy

²³ Dorraji, Seyed & Barcys, Mantas. (2014). Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations. Social Technologies. 4. 306-317. 10.13165/ST-14-4-2-05.

²⁴ Timan, T., Mann, Z. (2021). Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In: Curry, E., Metzger, A., Zillner, S., Pazzaglia, JC., García Robles, A. (eds) The Elements of Big Data Value. Springer, Cham. https://doi.org/10.1007/978-3-030-68176-0_7

²⁵ Call for Views on GDPR derogations closes - 5RB Barristers. https://www.5rb.com/data-protection/government-call-views-gdpr-derogations-closes-tomorrow/

All human beings in the world should possess the right to privacy. However, in some circumstances, states can restrict an individual's private life for several purposes. International human rights agreements and national laws might enforce a set of rules and regulations based on which the public and private authorities would be able to limit individuals' privacy rights. States can constrain people's personal lives only in exceptional circumstances.

For instance, in the modern age, the majority of states, including the United States, the United Kingdom, and China, use mass technological surveillance systems in the community and restrict the privacy rights of individuals to prevent any criminal activities, assist in criminal investigation and ultimately ensure national security. As noted in the report published by Human Right Watch in the United Kingdom, "Any new legislation should ensure that communications data is intercepted only in exceptional circumstances and that any decision authorizing such interception is subjected to independent scrutiny by a judicial authority. The law needs to be clear on what is authorized and for what purpose and avoid broad categories such as "the interests of national security" or the economic well-being of the United Kingdom."²⁷

According to human rights law, all states should preserve, protect, and respect people's right to privacy. However, in certain conditions, they would be able to constrain people's private lives. These conditions are:

1. In accordance with the law

First of all, as noted in the article mentioned above, state officials or private groups can constrain the right to privacy and interfere with a person's home, correspondence, and personal and family life when this restriction is lawful and legitimate. Thereby, neither individuals nor groups would not be able to intrude into people's private lives if it is not compliant with human rights law.

2. One of these circumstances

In addition, the restriction of the right to privacy by the public authority can be adopted if one of the below circumstances is fulfilled:

²⁶ Bonello, Rita (2016), Mass Surveillance and the Right to Privacy. Master of Laws Thesis submitted in partial fulfillment of the requirements for the degree of ADVANCED MASTERS IN EUROPEAN AND INTERNATIONAL HUMAN RIGHTS LAW, Universiteit Leiden. Available at:

https://www.academia.edu/28728849/Mass Surveillance and the Right to Privacy

²⁷ UK: Provide Clear Answers on Data Surveillance | Human Rights Watch.

2-1. National security

One of the reasons based on which states would be able to limit one's right to privacy is security concerns. It can justify the restriction of this right to more important values to regulate who is able to access, use, and modify personal data.²⁸ For instance, many states use CCTV cameras and other video surveillance technologies to monitor and control people's movements to prevent, detect, and identify terrorist activities and ensure the security of the country.

Indeed, international agreements and treaties provide equal value to all fundamental human rights. For instance, article 8 of the European Convention on Human Rights recognizes "the right to respect for private and family life," besides other fundamental rights, however in some cases, the public authorities might sacrifice people's private lives and restrict this provision to address more security concerns that are deemed to be more important than the restriction in the right to privacy.²⁹

Therefore, national security is one of the important conditions based on which states are authorized to restrict an individual's privacy rights. Today, numerous states constrain people's life, activities, and communications because this restriction is necessary to protect everybody's security throughout the country.

2-2. public safety

The government can also constrain people's right to privacy if this restriction is necessary for public health. During a public health emergency, states could establish temporary laws and regulations to protect everyone's health in a community and eliminate any potential health risks.

One of the recent examples is the creation of extensive restrictions by most governments during the outbreak of the Coronavirus. As the Covid-19 sickness began to spread globally, many states worldwide established strict regulations to prevent coronavirus infection. For instance, in some countries, which includes the United Kingdom, the government decided to collect, use, and share personal information like people's travel history to prevent further spread of infectious diseases. ³⁰ According to

²⁸ BAMBAUER, D. E. (2013). PRIVACY VERSUS SECURITY. *The Journal of Criminal Law and Criminology (1973-), 103*(3), 667–683. http://www.jstor.org/stable/43895376 page 13 or 678

²⁹ Friedewald, Michael & Cas, Johann & Bellanova, Rocco & Burgess, J. & Peissl, Walter. (2017). Surveillance, Privacy and Security: Citizens' Perspectives. 10.4324/9781315619309.

³⁰OECD (2020), OECD Policy Responses to Coronavirus (COVID-19)Using artificial intelligence to help combat COVID-19.

the report published by Human Rights Watch, any restriction to the right to privacy should be in accordance with the law to protect an individual's public health. Also, Deborah Brown, senior digital rights researcher at Human Rights Watch, said:

"COVID-19 is an unprecedented health crisis, but governments must not use the virus as cover to introduce invasive or pervasive digital surveillance."

States implement intelligence-powered monitoring systems to access real-time data to assist in monitoring, tracking, and eradicating disease transmission to protect individuals in the country.³¹ They used numerous digital technologies, including contact tracing applications, real-time location tracking, travel history and biometric data, mobile platform, Bluetooth or GPS technologies, contact tracing applications, and other types of digital surveillance, which effectively restricted individuals' privacy rights to prevent the spread of Coronavirus pandemic.³²

2-3. The economic health of the country

States could place an exemption on individuals' right to privacy for the economic well-being of the country. Nowadays, employers use many artificial intelligence-powered surveillance systems, like CCTV cameras. Although AI surveillance systems can evaluate and enhance workers' productivity, these systems potentially lead to privacy concerns.

Employers are entitled to control their employees' performance in the workplace. Managers can watch Web use, observe downloaded files, filter websites, block employee access to particular websites, and determine how much time employees spend on various websites through a variety of computer-based monitoring tools.³³ Employers specifically intend to manage the workplace so they can position

Available at: https://www.oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-ae4c5c21/

³¹ Grace Fox, Trevor Clohessy, Lisa van der Werff, Pierangelo Rosati, Theo Lynn,

Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications, Computers in Human Behavior, Volume 121, 2021, 106806, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2021.106806.

⁽https://www.sciencedirect.com/science/article/pii/S0747563221001291)

³² Ioannou A, Tussyadiah I. Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. Technol Soc. 2021 Nov;67:101774. doi: 10.1016/j.techsoc.2021.101774. Epub 2021 Oct 8. PMID: 34642512: PMCID: PMC8497958.

³³ Hartman, Laura. (2002). Technology and Ethics: Privacy in the Workplace. Business and Society Review. 106. 1 - 27. 10.1111/0045-3609.00099.

employees in appropriate places, ensure effective or productive performance, and they need to know what their platform workers are doing.³⁴

There are some ways through which employers could monitor the status of platform workers, including CCTV cameras, audio surveillance, GPS tracking, and time-tracking software, which restrict the privacy rights of employees to monitor the amount of time workers spend on tasks. These technologies allow employers to assess productivity and review the employees' functions and performance, which can be important to ensure that the work is efficiently being completed and lead to organizational growth and economic prosperity as a whole in the country.

3. One of these goals:

Along with this, states are allowed to constrain people's private life, activities, and communications for one of these goals:

3-1. Prevention of disorder or crime

The public authorities may restrict people's right to privacy to prevent disorder or crime in society. The governments would be able to interfere with an individual's privacy rights and constrain this right through the use of surveillance systems, particularly CCTV cameras, across the country to prevent any forms of violence, disorder, or criminal acts in the country, such as terrorist attacks.

Additionally, one of the crucial regulations with regard to the restriction of the right to privacy for crime prevention is the Law Enforcement Directive (LED), which was adopted by European Union. This legislation established a set of rules and regulations to protect, preserve and ensure people's personal information, which is obtained, used, and shared by criminal justice entities.

The most crucial point is that all kinds of intrusion into the private lives of individuals to prevent any criminal acts, disorders, and illegal behaviors should be necessary, proportionate, and in accordance with human rights law. The states are not authorized to impose arbitrary restrictions on the individual's fundamental rights to privacy and freedom as set forth in international human rights law.

3-2. Protection of health or morals

³⁴ Hartman, Laura. (2002). Technology and Ethics: Privacy in the Workplace. Business and Society Review. 106. 1 - 27. 10.1111/0045-3609.00099.

The other purpose based on which states can limit the right to privacy is health or moral issues. The right to privacy can be constrained because the public authority intends to protect society's shared values. Public morals are individuals' fundamental norms whose lives are intertwined with culture, the state, or the political system.³⁵

Although many states have ratified international human rights treaties, some governments assert that certain human rights norms outlined in the international treaties contradict their traditional, cultural, and religious values, and they may restrict human rights norms, including the right to privacy which conflict with their traditional, cultural or religious values.

Cultural and religious traditions existing in communities cannot justify any breach of fundamental freedoms and human rights, such as the right to privacy, and this restriction should be necessary, adequate, and proportionate and ensure that they should not arbitrarily violate individuals' privacy rights and fundamental human rights.

3-3. Protection of the rights and freedoms of others

The other purpose which gives states authorization to constrain the right to privacy in certain circumstances and interfere with private life, family, and communication's individuals is the protection of other people's fundamental rights and freedoms.

According to international human rights law, all people should own the rights and freedoms set forth in human rights treaties, regardless of race, gender, and religion. For instance, as stated in the preamble of UDHR, "recognition of the inherent dignity and of equal and inalienable rights of all members of the human family is the foundation of freedom, justice, and peace in the world."³⁶

As a result, states have the legal right to limit people's private lives when this restriction is necessary to maintain, protect, and respect other people's fundamental freedoms of people living in the community, comprising freedom of religion, thought, speech, consciousness, and so on.

The Closed Circuit Cameras (CCTV)

³⁵ Lovin, Robin. (2021). Public Moral Discourse. Religions. 12. 255. 10.3390/rel12040255.

³⁶ United States: Advance Human Rights of People around Us, Urges Secretary-General on Message for Day of Observance. (2016). MENA Report, n/a.

In human rights laws, Privacy and Data Protection are not absolute rights. The states might use numerous technological surveillance systems which are powered by artificial intelligence across the country and intrude on people's rights to privacy to prevent any criminal activities in the community.³⁷

In the modern age, Artificial Intelligence is used in many sectors. According to Gheorghe Tecuci, "Artificial Intelligence (AI) is the Science and Engineering domain concerned with the theory and practice of developing systems that exhibit the characteristics that we associate with intelligence in human behavior, such as perception, natural language processing, problem-solving and planning, learning and adaptation, and acting on the environment." 38

Moreover, a broad range of surveillance systems is powered by artificial intelligence. As Ibrahim Sutrisno states, "Intelligent surveillance system (ISS) is a surveillance system that has the intelligent capability to automatically analyze surveillance data and perform necessary actions such as generating alarm or warning." The most common surveillance systems are video surveillance technologies, audio surveillance systems, biometric systems, and network surveillance. Al-based surveillance systems are able to automatically obtain, use, and share an individual's personal data from different sources. 40

One of the important instruments commonly used to monitor individuals' behaviors in public and private properties is Closed Circuit Televisions (CCTV) systems. CCTV systems refer to the use of a network of cameras to monitor and record people's movements, behaviors, and communications and their surroundings in certain places, like highways, roads, schools, airports, and public transportation.⁴¹

Closed Circuit televisions (CCTV) installed in many places, comprising public infrastructures, services, equipment, facilities, and vehicles, use advanced

³⁷ Bonello, Rita (2016), Mass Surveillance and the Right to Privacy. Master of Laws Thesis submitted in partial fulfillment of the requirements for the degree of ADVANCED MASTERS IN EUROPEAN AND INTERNATIONAL HUMAN RIGHTS LAW, Universiteit Leiden. Available at:

https://www.academia.edu/28728849/Mass_Surveillance_and_the_Right_to_Privacy

³⁸Tecuci, Gheorghe. (2012). Artificial intelligence. Wiley Interdisciplinary Reviews: Computational Statistics. 4. 10.1002/wics.200.

³⁹ Ibrahim, Sutrisno. (2016). A comprehensive review on intelligent surveillance systems. Communications in Science and Technology. 1. 10.21924/cst.1.1.2016.7.

⁴⁰ J. Curzon, T. A. Kosa, R. Akalu and K. El-Khatib, "Privacy and Artificial Intelligence," in *IEEE Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 96-108, April 2021, doi: 10.1109/TAI.2021.3088084.

⁴¹ Olatunji, Iyiola & Cheng, Chun Hung. (2019). Video Analytics for Visual Surveillance and Applications: An Overview and Survey. 10.1007/978-3-030-15628-2_15.

algorithms and machine learning without any human intervention to autonomously observe the activities, movement, and communications as they occur in real-time.⁴²

In the past years, the cameras in these early CCTV systems were typically extended to connect up to four cameras to monitor static images and had a fixed focal length; however, over the years, as technology developed, the video recorder was added to CCTV cameras, allowing the image displayed on the monitor to be recorded on videotape and played back at a later time.⁴³

Along with CCTV cameras, there are several control rooms. The control room is an ample space where the operatives watch CCTV footage on several screens. The images captured by CCTV cameras are evaluated in the control room by competent persons, and these images could be recorded on videotape or stored as digital information.⁴⁴ For instance, in the United Kingdom, the Sheffield Wide Image Switching System (SWISS) has a control room with several staff working 24 hours a day with up to six operators watching CCTV footage on the screens at any one time and can now control over 150 cameras installed across streets.⁴⁵

There are different types of CCTV cameras. Some are Dome Cameras, Bullet Cameras, PTZ (Pan-Tilt-Zoom) cameras, Thermal Cameras, Wide Dynamic Range (WDR) Cameras, and Fish-Eye Cameras. Surveillance cameras have different technical characteristics. For example, In the United Kingdom, CCTV cameras are commonly equipped with facial and audio recognition software, which can gather auditory signals from the surrounding environment and then amplifies them so that

⁴² Kumaravel, Rasadurai. (2023). AI Based Smart Surveillance System. International Journal of Scientific Research in Science, Engineering and Technology. 10. 10-15. 10.32628/IJSRSET229672.

⁴³ Norris, Clive Norris (2009), A REVIEW OF THE INCREASED USE OF CCTV AND VIDEO-SURVEILLANCE FOR CRIME PREVENTION PURPOSES IN EUROPE. Department of Sociological Studies, University of Sheffield, UK Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS), Brussels. Available at: https://www.statewatch.org/media/documents/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf

⁴⁴ Moyo, Sheperd (2019), EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG By submitted in accordance with the requirements for the degree of MAGISTER TECHNOLOGIES in SECURITY MANAGEMENT at the UNIVERSITY OF SOUTH AFRICA. Available at: https://core.ac.uk/download/pdf/286383944.pdf

⁴⁵ Norris, Clive Norris (2009), A REVIEW OF THE INCREASED USE OF CCTV AND VIDEO-SURVEILLANCE FOR CRIME PREVENTION PURPOSES IN EUROPE. Department of Sociological Studies, University of Sheffield, UK Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS), Brussels. Available at: https://www.statewatch.org/media/documents/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf

even extremely weak signals can be recognized, and we can clearly identify who is being observed.⁴⁶

A wide range of CCTV cameras are being used in many countries. The extent of these systems varies between nations; for instance, although the majority of autocratic governments, like China, have some of the most extensive surveillance infrastructures, democratic states like the United Kingdom have also invested in monitoring technologies, including CCTV systems as well as traffic enforcement cameras.⁴⁷

Many researchers believe that the United Kingdom was the first country to develop CCTV surveillance systems worldwide and inspired the spread of this technology throughout other countries. As Nowadays, these cameras are being used by many countries. But in several countries, there are many camera control systems. For instance, there are approximately 6 million CCTV in the United Kingdom.

The British government initially intended to use CCTV to prevent crimes, detect offenders, and reduce perceived fear of crime, and over time, this policy has shifted so that the purpose of CCTV policy is to mitigate unlawful, anti-social, and all kinds of undesirable behavior in residential area, city centers, and other public places to ensure community's national security.⁴⁹

CCTV was once primarily used for police surveillance in the 1980s, however, as more advanced technology has emerged, individuals have begun to use surveillance systems in the streets, stores, shops, and private properties to review people's movements.⁵⁰ The recorded videos can be observed in real-time or later for crime prevention, defender identification, and investigation purposes.

⁴⁶ Swami, Kedar & Bhuma, Bhardwaz & Mondal, Semanto & Lokam, Anjaneyulu. (2020). Audio Surveillance System. 10.1007/978-981-15-1366-4 28.

⁴⁷ Richards, N. M. (2013). THE DANGERS OF SURVEILLANCE. *Harvard Law Review*, *126*(7), 1934–1965. http://www.jstor.org/stable/23415062

⁴⁸ Small or medium-scale focused research project (2012), Increasing Resilience in Surveillance Societies. IRISS, 290492, EP7-SSH-2011-2. Available at:

https://www.academia.edu/26586909/IRISS D1 MASTER DOCUMENT 17Dec?email work card=view-paper

⁴⁹C. William; R Webster, Interconnections Between Technological and Policy Innovation: Re-evaluating the Evidence-Base Supporting the Provision of CCTV in the UK. University of Stirling. Available at:

https://dspace.stir.ac.uk/bitstream/1893/2703/1/interconnection%20 between%20 technological%20 and%20 policy%20 innovation%2009.pdf

⁵⁰ Yeganegi, Kamran & Moradi, Dawood & Obaid, Ahmed. (2020). Create a wealth of security CCTV cameras. Journal of Physics: Conference Series. 1530. 012110. 10.1088/1742-6596/1530/1/012110.

The United Kingdom, as one of the countries which are known for its widespread application of CCTV cameras, uses these systems to monitor and record individual activities to prevent any crimes and other anti-social behaviors in the community in many places, like houses, workplaces, and public areas:

(1) Houses

Nowadays, in the United Kingdom, many people install CCTV surveillance systems in their private properties for security reasons. These cameras can be beneficial to enhance residential properties' safety, prevent common crimes such as robbery, theft, and burglary, and identify the thief in case of house robbery.

CCTV systems can cause several privacy concerns. Home video surveillance systems may even infringe upon individuals' private lives. Because these cameras can capture and record all people's movements in public spaces or surrounding houses. The owners would be able to access the recorded footage of surveilled persons without their consent.

According to Guidelines 3/2019 on the processing of personal data through video devices, Adopted on 10 July, Before installation of a video surveillance system, the controller should constantly evaluate if this measure is primarily suitable to attain the desired goal and secondly adequate, relevant, and necessary for its purposes and less intrusive mean to the fundamental rights of the data subject.

Therefore, it is crucial to note that in order to prevent property-related crimes, the controller has the option to employ alternative security measures, including securing the property with fences, implementing regular security patrols, employing gatekeepers, improving lighting conditions, installing robust security locks, reinforcing windows and doors against tampering, and applying anti-graffiti coatings or protective foils on walls which can be equally effective compared to the use of CCTV surveillance systems. Therefore, the use of CCTV cameras in private properties should be less intrusive way compared to other alternative measures, necessary, and adequate for its purposes.

(2) Workplace

_

⁵¹ Guidelines 3/2019 on the processing of personal data through video devices, Adopted on 10 July.

Video surveillance systems are broadly used in major cities, and numerous employers would like to embrace CCTV cameras in their workplace to observe their employees' behaviors.

The companies might implement video surveillance systems to evaluate employees' performances and prevent a broad range of crimes, such as theft. However, the application of CCTV cameras can result in several privacy concerns, which include:

Firstly, the use of CCTV cameras by several employers in the workplace presents some privacy issues because video monitoring might be carried out without the individuals' consent and knowledge. These cameras can review, record and preserve confidential conservations between employees. Thus, workers might believe that organizations are observing their activities without their prior consent, and the collection, use, and sharing of this information without the employee's consent can be considered an infringement upon their privacy rights.

Secondly, the personal information obtained through CCTV cameras can be used for objectives that were not initially intended. Many individuals believe that they are under constant surveillance by organizations and that the recorded footage could be misused for other purposes.⁵² Therefore, Using CCTV footage for unintended purposes creates distrust between the company and its employees and infringes on an individual's privacy rights.

Thirdly, Video surveillance systems used in workplaces can record all individual's activities, behaviors, and movements. The CCTV cameras can even collect personal information about those who are not employees or who are not involved in the work environment. It is important to note that many of them are unaware of the presence of workplace cameras, their intended use, and how doing so may violate even non-participant people's privacy rights.

(3) Public places, like streets, hospitals, etc:

The majority of public places are equipped with camera surveillance systems. As observed in statistics, In the United Kingdom, we can observe a large number of CCTV cameras in many public places. The British government installs video

⁵² Ball, Kirstie. (2010). Workplace Surveillance: An Overview. Labor History. 51. 10.1080/00236561003654776.

surveillance systems in public places to protect people's safety from terrorist attacks or other criminal activities.

Numerous surveillance cameras are designed in public spaces which are accessible to the public, such as streets, parks, squares, public transport, and shopping center, to record and monitor an individual's activities.⁵³ It can contribute to public authorities to implement appropriate measures to prevent crime, enhance public security, and spread personal safety throughout the community.

Therefore, we could observe that the presence of extensive CCTV cameras, specifically in crowded cities such as London, can result in numerous benefits for society. It can deter potential criminals, identify perpetrators, and ultimately create a sense of security among all citizens throughout the country. However, this technology should not interfere with people's right to privacy.

The History and Evolution of CCTV Cameras in the United Kingdom

Many CCTV cameras are used in the United Kingdom. The British government initiated the first CCTV cameras in the 1960s. During the last years, a significant amount of CCTV systems in numerous places, particularly in crowded cities, were installed. We examine the history and evolution of CCTV cameras in the United Kingdom.⁵⁴

Firstly, in 1927, Russian physicist Leon Theremin created an early mechanical CCTV system with scanning-transmitting cameras and wireless shortwave technology and installed it in the Moscow Kremlin courtyard to monitor all visitors approaching the court.⁵⁵

In the 1960s, the British government used the first CCTV cameras when the Metropolitan Police implemented two temporary cameras in Trafalgar Square to monitor activities on "Guy Fawkes Day" and subsequently, numerous cities in the United Kingdom started to install CCTV systems to monitor streets, retail outlets, and public areas. ⁵⁶

⁵³ Zabłocki, Michał & Gościewska, Katarzyna & Frejlichowski, Dariusz & Hofman, Radosław. (2014). Intelligent video surveillance systems for public spaces – a survey. Journal of Theoretical and Applied Computer Science. 8. 13-27.

⁵⁴ https://www.firstcountymonitoring.co.uk/the-history-of-cctv-in-the-uk/

⁵⁵ same

⁵⁶ same

In the 1970s, CCTV cameras were used for traffic monitoring in and around London, including the London underground; additionally, the 1980s experienced the implementation of video surveillance systems in parking garages and council estates owned by local authorities. This investment aimed to enhance security and deter criminal activities. During the 1990s, the United Kingdom allocated a significant portion of its crime prevention budget to CCTV systems, particularly in crowded city centers.

In the 2000s and beyond, facial detection technology experienced rapid development, enabling efficient identification and tracking of individuals, and Law enforcement agencies gained access to forensic databases in 2009.⁵⁸ Camera resolution also witnessed substantial improvements during this period, enhancing image quality and enabling more accurate surveillance.

In the United Kingdom, the government initially intended to use CCTV surveillance systems to prevent crimes in society. CCTV policy aims to reduce crimes and any antisocial behavior in residential areas, towns, and city centers.⁵⁹ Overall, from 1927 until today, the proportion of CCTV cameras has significantly increased nationwide. The British government installed all kinds of CCTV cameras in public areas; today, the United Kingdom is among those countries which have a substantial number of CCTV cameras.

The percentage of CCTV cameras

In this section, we elaborate on the percentage of CCTV cameras in the world, which includes:

1. The Countries with the most CCTV Cameras in the world

In the modern age, in many countries, states may decide to use CCTV cameras for many purposes. For instance, police officers might install CCTV cameras in public spaces, including streets, highways, schools, and airports, to prevent all kinds of

⁵⁷ same

⁵⁸ same

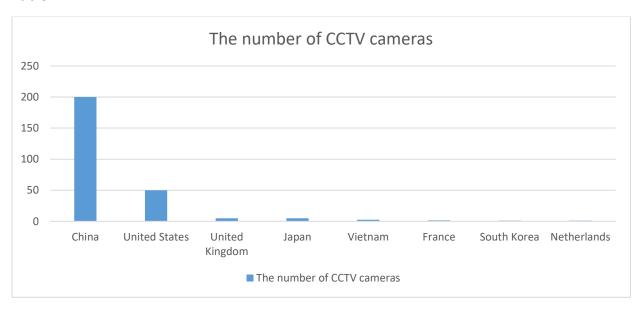
⁵⁹C. William; R Webster, Interconnections Between Technological and Policy Innovation: Re-evaluating the Evidence-Base Supporting the Provision of CCTV in the UK. University of Stirling. Available at:

https://dspace.stir.ac.uk/bitstream/1893/2703/1/interconnection%20 between%20 technological%20 and%20 policy%20 innovation%2009.pdf

crimes, review their movements and assist investigatory authorities in identifying perpetrators.

However, in some countries, there are innumerable CCTV systems installed everywhere. The table below provides information regarding CCTV cameras in 8 countries that use the highest number of video surveillance systems in the world. The data below indicates the importance of camera surveillance systems in the United Kingdom and compares the percentage of CCTV numbers in the UK and other countries worldwide.⁶⁰

Table:



Source: www.earthweb.com

Firstly, in the provided table, we can observe that the most considerable amount of CCTV cameras belongs to China. China has installed 200 million surveillance cameras to monitor all individuals' activities, behaviors, and communications. This is also an enormous amount with regard to the other countries on this list.

Further, the United States is the second country that uses the highest number of video surveillance. The statistics show that approximately 50 million CCTV cameras are employed in the United States. The US government installed many video systems in crowded cities to prevent criminal activities, terrorist attacks, and other serious crimes.

⁶⁰ https://earthweb.com/who-has-the-most-cctv-in-the-world/

Recent statistics illustrate that 5 million CCTV cameras are operating throughout the United Kingdom to monitor people's movements. The British government uses a network of cameras to monitor and record people's movements, behaviors, communications, and surroundings in certain places, like highways, roads, schools, airports, and public transportation.⁶¹

Moreover, Japan installed 5 million cameras in innumerable places, including streets, towns, cities, schools, and public areas. As indicated in the table above, there can be seen approximately 2.6, 1.65, and 1 million CCTV cameras in Vietnam, France, Netherlands, respectively. France and Netherlands are the other European countries that have implemented a huge number of CCTV cameras to ensure the country's safety.

Therefore, there can be seen more camera control systems in the UK in regard to other European countries. There are approximately 6 million CCTV cameras in the United Kingdom, the highest number behind China and the United States. UK uses CCTV cameras as a critical instrument to preserve the country's national security.

According to a report published by Watchdog, although the UK only has 1% of the world's population, with approximately 68 million, 20% of the CCTV cameras in the world are in this country, and the United Kingdom presently holds the record as well for having the most CCTV cameras per person.⁶²

2. The Cities with the highest CCTV Cameras in the world

According to recent research,⁶³ surveillance camera control systems have become increasingly prevalent worldwide, with many cities investing in these technologies to monitor people's movements and enhance public safety. The given table indicates the cities with the most CCTV cameras per 1,000 inhabitants in 2021:⁶⁴

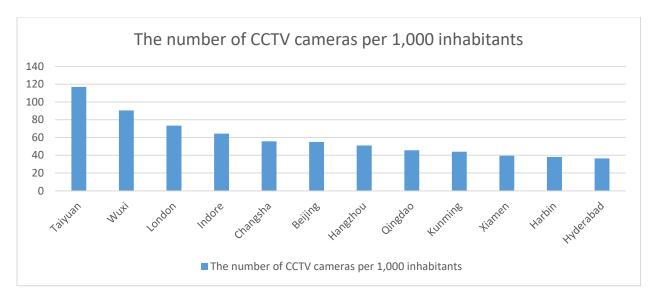
Table:

⁶¹ Olatunji, Iyiola & Cheng, Chun Hung. (2019). Video Analytics for Visual Surveillance and Applications: An Overview and Survey. 10.1007/978-3-030-15628-2_15.

⁶² Loughran, Jack (Published Tuesday, January 9, 2018). Britain's network of CCTV cameras are vulnerable to attack by hackers according to a watchdog. Available at: https://eandt.theiet.org/content/articles/2018/01/britain-s-vast-network-of-cctv-cameras-is-vulnerable-to-hacks-watchdog-warns/

⁶³ https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

⁶⁴ https://www.statista.com/chart/19256/the-most-surveilled-cities-in-the-world/



Source: www.statista.com

Firstly, two major cities in China are Taiyuan and Wuxi. The highest percentage of CCTV cameras is related to Taiyuan and Wuxi, with 117.0 and 90.5 cameras per 1,000 inhabitants, respectively. This exemplifies China's commitment to pervasive surveillance practices for purposes such as social control, crime prevention, and public security. Several other Chinese cities on the list, including Beijing, Qingdao, and Kunming, highlight the nation's dedication to extensive surveillance measures.

Among the cities listed, London stands out as the European city with a notable concentration of CCTV cameras, ranking third with 73.3 cameras per 1,000 inhabitants in 2021.⁶⁵ London has the highest CCTV camera density outside of Asia, which demonstrates the importance of surveillance systems to prevent serious criminal activities in the United Kingdom.

Apart from China, Indore in India also features prominently on the list, ranking fourth with 64.4 cameras per 1,000 inhabitants. This demonstrates the increasing adoption of CCTV systems in Indian cities for enhancing safety and addressing security concerns.

Therefore, in London, there are a substantial number of CCTV surveillance systems in public places, including in sports stadiums and tourist attractions; London's transport infrastructure consists of the London Underground, Mainline railway

⁶⁵ same

station, national road network, and airports to capture and record individuals' activities to combat terrorism and other forms of crime.⁶⁶

In 1993, the IRA's terrorist attack on Bishopsgate served as the first motivation for the introduction of CCTV in central London, and a network of cameras was installed to keep an eye on the City of London's gateways and following this event; the number of CCTV systems in the United Kingdom has substantially increased to prevent all kinds of crimes, including terrorist attacks and ensure the security and public order of the country.⁶⁷

Overall, the comparative analysis of cities with the most CCTV cameras per 1,000 inhabitants highlights China's dominance in pervasive surveillance practices. However, London is the only city outside China and India that entered the list, and London's presence on the list demonstrates the significant use of CCTV systems in European cities, emphasizing their commitment to enhancing public safety.

3. The Cities with the most CCTV Cameras in Europe

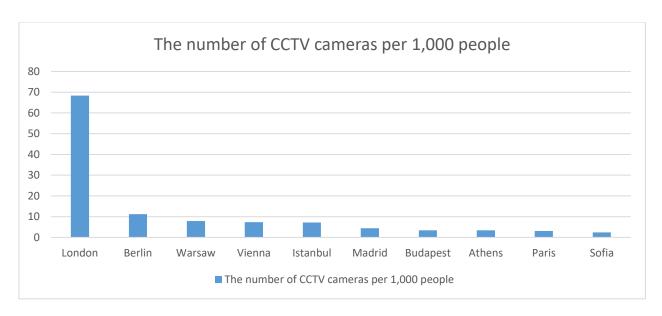
In Europe, in recent years, many states installed a significant number of CCTV cameras in numerous places. The governments intend to monitor the movements of their residents and all people who come to the country. They would be able to prevent serious crimes and protect individual safety in society. The table outlines the number of CCTV cameras in European cities.⁶⁸

Table:

⁶⁶ McCahill, Michael; Norris, Clive (2002). CCTV in London, Centre for Criminology and Criminal justice, University of Hull, Working paper no.6. Available at: http://www.urbaneye.net/results/ue_wp6.pdf

⁶⁷ Norris, C., & McCahill, M. (2006). CCTV: BEYOND PENAL MODERNISM? *The British Journal of Criminology, 46*(1), 97–118. http://www.jstor.org/stable/23639334

⁶⁸ https://www.statista.com/chart/19268/most-surveilled-cities-in-europe/



Source: www.statisca.com

The statistics demonstrate that in London, there are around 68.6 CCTV cameras. London, the United Kingdom's capital, has the highest density of CCTV cameras in Europe. Also, there has been a dramatic increase in camera surveillance control systems over the last few years. This rise was particularly noticeable in 2019, during which time the number of CCTV cameras tripled. The data above show a substantial number of CCTV cameras in London, which is far higher than in other European cities.

Following London, Berlin embraced 11.2 CCTV cameras per 1,000 inhabitants, which is the second surveilled city in the provided table.⁶⁹ Nowadays, innumerable CCTV cameras are being installed in Berlin everywhere, including streets, schools, libraries, and public transportation to prohibit criminal behaviors.

The amount of CCTV cameras in Warsaw, Vienna, and Istanbul reached 7.9, 7.4, and 7.2 per 1,000 people, respectively. Additionally, Madrid, Spain's capital, owns 4.4 CCTV cameras. The provided table delineates the trends of video surveillance systems that are similar in Budapest and Athens, with 3.4 cameras per 1,000 people.

There are 3.1 cameras in Paris. Paris has the most significant proportion of CCTV cameras in France. Furthermore, in Sofia, the capital of Bulgaria, there are almost

_

⁶⁹ same

2.4 CCTV cameras which is the least number in comparison with the cities in the provided graph.

The total number of CCTV cameras in London is 691,000, with 1 CCTV camera for every 13 people. Although many European cities, including Berlin, Warsaw, and Vienna, embraced a massive number of CCTV cameras, the gap between the United Kingdom's capital city, London, and other European cities has considerably increased over the years. Thereby, London has the highest level of surveillance by CCTV cameras in European countries.

4. The Cities with the highest number of CCTV cameras in the United Kingdom

Moreover, countless CCTV cameras are installed in other cities in the United Kingdom for different purposes. The increasing use of surveillance cameras can bring a multitude of benefits. Closed Circuit Television (CCTV) is a camera surveillance system that can monitor any individual's suspect activities, movements, and communications and prevents further threats to society in specific areas. This table compares the five cities which have a high number of CCTV cameras in the United Kingdom in 2020.⁷⁰





Source: www.earthweb.com

⁷⁰ https://earthweb.com/how-many-cctv-cameras-in-london-are-there/

In the United Kingdom, the major cities are equipped with camera control systems. Firstly, before 2022, there were approximately 628,000 CCTV cameras installed in London. This number demonstrated that there is one camera for every 14 residents. As shown in the given graph, 809,000 CCTV cameras were used in 2020, and they reached 942,000 units installed in London in 2022, which equates to one camera for every 10 people.⁷¹

Manchester has 248,000 CCTV units, which is approximately one camera for every 11 residents. Behind London, Manchester has the largest proportion of CCTV cameras. As well, Birmingham has 109,000 CCTV units, around one camera for every 26 residents or 36.5 units per 1,000 members of the population.

Liverpool and Newcastle are the other cities that have the most heavily CCTV cameras. In Liverpool, there are 82,000 CCTV units, corresponding to around one camera for every 20 residents or 34.5 units per 1,000 members of the population. Also, Newcastle has 74,000 CCTV units, which is approximately one camera for every 19 residents or 45.6 units per 1,000 members of the population.

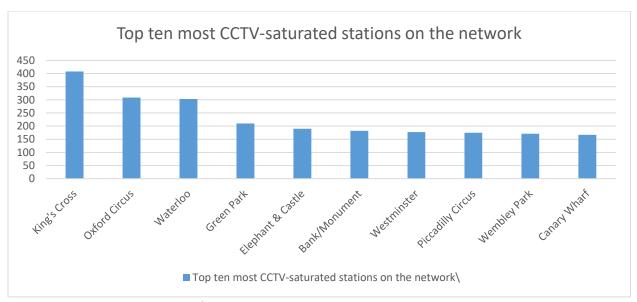
5. The CCTV Cameras in Underground's London⁷²

The data provided highlights the top ten most CCTV-saturated stations on the London Underground network. These numbers represent the total count of CCTV cameras present at each station, indicating the extent of surveillance in these locations. We analyze and compare the data to create comprehensive and comparative information on the number of CCTV cameras in Underground London.

Table:

⁷¹ https://earthweb.com/how-many-cctv-cameras-in-london-are-there/

⁷² https://www.aaisecurity.co.uk/news/cctv-london-underground/



Source: www.aaisecurity.co.uk

At the top of the list is King's Cross St. Pancras on the Metropolitan Line, with an impressive 408 CCTV cameras. This high number signifies the substantial surveillance infrastructure deployed in one of London's busiest and most interconnected stations. The large number of cameras reflects the importance of maintaining security and monitoring activities in a station that serves as transportation hub.

Oxford Circus on the Bakerloo Line follows closely with 309 CCTV cameras. As one of the most famous shopping areas in London, this station attracts a significant number of commuters and tourists. The high surveillance density highlights the importance of ensuring public safety and preventing potential threats in a crowded and bustling location.

Waterloo on the Jubilee Line takes the third spot with 303 CCTV cameras. Being one of London's busiest stations, this high number of cameras demonstrates the need for vigilant monitoring and surveillance to manage the large volume of passengers passing through the station on a daily basis.

Green Park on the Piccadilly Line ranks fourth with 210 CCTV cameras. As a major interchange station, it connects several lines and experiences heavy footfall. The substantial surveillance presence emphasizes the priority placed on maintaining a secure and safe environment for commuters.

Elephant & Castle on the Bakerloo Line follows with 190 CCTV cameras. This station's significant surveillance infrastructure likely serves to address security concerns in an area that has undergone significant urban redevelopment and experiences diverse foot traffic.

Bank/Monument on the Central Line ranks sixth with 182 CCTV cameras. Being a vital financial district station, this high surveillance density is expected, given the need to ensure the safety and security of commuters and businesses in the vicinity.

Westminster on the Jubilee Line is the seventh-most CCTV-saturated station with 177 cameras. Its location in the heart of London's political and administrative hub necessitates a robust surveillance infrastructure to safeguard against potential security threats.

Piccadilly Circus on the Bakerloo Line follows closely with 175 CCTV cameras. As a popular tourist and entertainment destination, the station's high surveillance density serves to ensure the safety and well-being of the large number of visitors and commuters frequenting the area.

Wembley Park on the Jubilee Line ranks ninth with 171 CCTV cameras. With its proximity to Wembley Stadium, a major sports and events venue, the presence of a significant number of cameras is essential to maintain security during large-scale gatherings and events.

Canary Wharf on the Jubilee Line completes the list with 167 CCTV cameras. Being one of London's key financial districts, the station's high surveillance density is in line with the security needs of this important business hub.

In summary, the data reveals the top ten most CCTV-saturated stations on the London Underground network, with varying levels of surveillance across different locations.

The Impact of CCTV Cameras on Crime in the United Kingdom

In the United Kingdom, we could observe a significant number of camera control systems across the country. Recent research illustrated that there are around 6 million CCTV cameras in the United Kingdom. There is mass surveillance in almost all cities in the United Kingdom, with 1 CCTV camera for every ten people, which is the highest number compared to European countries.

The increasing use of CCTV cameras can bring a multitude of benefits. Closed Circuit Television (CCTV) is a camera surveillance system that can monitor any individual's suspect activities, movements, and communications and prevents further threats to society in specific areas.

In the United Kingdom, CCTV surveillance systems have become more accessible in houses, schools, hospitals, public transportation, and numerous public places. The British government uses cameras in all places as an effective instrument to address criminal activities.

The widespread use of CCTV cameras substantially affects crime prevention, criminal identification, and the spread of feelings of personal safety in the community. In this section, we discuss three ways that illustrate how closed-circuit televisions influence criminal behaviors, including: ⁷³

(1) Prevention of crime

Crime prevention is one of the important concepts in the international framework. Many individuals or groups, private or public organization, seek to prevent all kinds of criminal activities before it is committed. For instance, the United Nations, as an intergovernmental organization, attempt to create international principles to combat crimes, analyze the problems in crime prevention implementation, and provide practical recommendations to address the challenges which states might face in the criminal justice system.⁷⁴

All states implement numerous measures to prevent all forms of criminal behaviors in the country. The high crime rate can result in innumerable destructive effects on society. Multiple factors can influence the crime rate in the community. Three main causes can result in crimes, which include economic conditions (lack of educational facilities, poverty, inadequate job opportunities), social environment (unequal social power, lack of access to social services, limited leadership in the community), and family environment (dysfunctional family condition).⁷⁵

⁷³ https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf

⁷⁴ Kolomiiets, Nataliia & Senchenko, Nadiia & Petryk, Olena & Ivankov, Ihor & Olga, Ovsiannikova & Geperidze, Davit. (2023). International Legal Standards in Crime Prevention. WSEAS TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT. 19. 110-118. 10.37394/232015.2023.19.10.

⁷⁵ THE ROOT CAUSES OF CRIME, CS&CPC Statement on the Root Causes of Crime approved in 1996. Available at: https://preventingcrime.ca/wp-content/uploads/2014/08/Causes_of_Crime.pdf

States implement different measures to mitigate the factors which lead to the commission of criminal acts. All international agencies, states, and non-governmental organizations embrace a range of policies to prevent all forms of future criminal activities. The prevention of crime can result in numerous benefits in society and increase people's quality of life in numerous aspects.⁷⁶ There are three primary levels of crime prevention:⁷⁷

Firstly, most states make efforts to address the main reasons for crimes and prevent any adverse conditions which bring about the high crime rate in society; for instance, they examine all forms of anti-social, abusive, and aggressive behavior of individuals from childhood, invest in education, economic condition, family environment, social and cultural norms and implement different approaches to help people reduce delinquency and criminal activities at an early age.⁷⁸

Secondly, in some countries, legislative bodies might impose more substantial punishment, like longer prison sentences, on offenders to deter them from committing crimes.⁷⁹ Indeed, if the potential offenders know that criminal courts will strictly convict them, it is more probable that they will not engage in or repeat a crime in the future.

Thirdly, several states intend to install certain "warning signs" in numerous places to deter criminals from committing crimes. For instance, some countries, particularly the United States, China, India, France, and the United Kingdom, use signs to convey the message "CCTV in operation," which warns people that all their behaviors are monitored by competent officials in specific places to prevent people from committing crime and ensure national security.

Therefore, many states, such as the United Kingdom, use CCTV cameras everywhere, including streets, schools, libraries, and public transportation. The massive use of CCTV cameras in numerous places can prevent crime occurrences. People commit crimes because they are aware that nobody is observing them and

Nory Research. (November 2021). Essay on Crime Prevention. Retrieved from https://www.ivoryresearch.com/samples/essay-on-crime-prevention/

⁷⁷ https://preventingcrime.ca/wp-content/uploads/2014/08/Causes of Crime.pdf

⁷⁸ Whitecross, Richard & Levy, Liz & Santhakumaran, Dharshi. (2014). What Works to Reduce Crime: A Summary of the Evidence.

⁷⁹ Whitecross, Richard & Levy, Liz & Santhakumaran, Dharshi. (2014). What Works to Reduce Crime: A Summary of the Evidence.

they will not be arrested by the police.⁸⁰ While CCTV is a visible deterrent to prevent potential criminals from future criminal acts. ⁸¹

The British government supported using CCTV cameras as one of the fundamental plans to reduce crimes in the community. In 1995, a challenge fund for closed circuit television (CCTV) was initiated in the United Kingdom. This project highlighted the importance of physical presence, ensuring the appropriate location, and research on the effects of CCTV cameras on crime reduction in major cities in the United Kingdom.⁸²

The United Kingdom is one of those countries which considerably invested in CCTV cameras. They heavily invest in CCTV cameras to protect all individuals from global risks, such as terrorism, serious crimes, and organized crime, which necessitate more efficient countermeasures.⁸³ The implementation of CCTV surveillance cameras is the most heavily funded method used in the United Kingdom, with almost three-quarters of all state expenditures on crime prevention.⁸⁴

According to the report published For the Information Commissioner by the Surveillance Studies Network on September 2006 in the United Kingdom: "During the 1990s the Home Office spent 78% of its crime prevention budget on installing CCTV and an estimated £500M of public money has been invested in the CCTV infrastructure over the last decade."85

Indeed, they believe that the potential offenders know that their activities, behaviors, and movements are continuously monitored by video surveillance systems installed everywhere.⁸⁶ Therefore, they will be more likely to refrain from

⁸⁰ WowEssays. (2020, April, 03) Free Cctv In The UK Essay Example. Retrieved July 01, 2023, from https://www.wowessays.com/free-samples/free-cctv-in-the-uk-essay-example/

⁸¹ Baoyan, Kenard Vic. (2023). CLOSED CIRCUIT TELEVISION (CCTV): A TOOL IN CRIME PREVENTION AND DETECTION. 10.13140/RG.2.2.32896.81928.

⁸² Laycock, Gloria & Clarke, Ronald. (2001). Crime Prevention Policy and Government Research: A Comparison of the United States and United Kingdom. International Journal of Comparative Sociology - INT J COMP SOCIOL. 42. 235-255. 10.1177/002071520104200110.

⁸³ Möllers, Norma & Hälterlein, Jens. (2013). Privacy issues in public discourse: The case of "smart" CCTV in Germany. Innovation: The European Journal of Social Sciences. 26. 10.1080/13511610.2013.723396.

⁸⁴ Brandon C. Welsh & David P. Farrington (2009) Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis, Justice Quarterly, 26:4, 716-745, DOI: <u>10.1080/07418820802506206</u>

⁸⁵ A Report on the Surveillance Society, op. cit., para 9.5.3. https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf

⁸⁶ https://core.ac.uk/download/pdf/286383944.pdf

engaging in criminal activities because they will be afraid of being arrested by police officers.

According to a University of Cambridge study, implementing CCTV cameras in public areas can reduce crime rates by 7%; as a result, many people choose to install CCTV in their houses to mitigate the likelihood of all kinds of crimes, such as theft.⁸⁷ As well, the physical presence of CCTV cameras reduced certain crimes, such as theft and general crimes in the casinos and parking lots, by 51%, as potential criminals know that they would be brought to the law court and become convicted of a crime.⁸⁸ This percentage demonstrates that camera surveillance systems have substantially resulted in crime prevention in the United Kingdom.

Although CCTV cameras have positively affected crime prevention, their impact on several types of crimes in numerous locations might differ. For instance, as indicated in the research carried out in the United Kingdom, The College of Policing's Crime Reduction Toolkit suggests that CCTV is "associated with a statistically significant decrease in crime" The meta-analysis indicates that CCTV in places in which CCTV cameras were used compared to places did not have camera surveillance systems, drug-related crimes declined by 20% and vehicle and property crime decreased by 14%, while there was no statistically significant effect was observed for violent crime or disorder.

Nowadays, many researchers claim that the use of CCTV cameras has a significant role in the deterrence of offenders and the reduction of crime rates. However, some argue that recent statistics show that using CCTV cameras has not consistently decreased criminal and anti-social behaviors. Reasonably, they believe the reduction in crimes might not directly result from the presence of CCTV cameras, and many factors, including education, economic conditions, and cultural and social characteristics, can influence the United Kingdom's crime rates. For instance, many investigators believe that although there is a considerable

WowEssays. (2020, April, 03) Free Cctv In The UK Essay Example. Retrieved July 01, 2023, from https://www.wowessays.com/free-samples/free-cctv-in-the-uk-essay-example/

⁸⁸ Peterson Kelly (Author), 2012, Effectiveness of CCTV in Crime Prevention, Munich, GRIN Verlag, https://www.grin.com/document/280648

⁸⁹ Khan, Md & Aziz, Moonmoon & Faruk, Omar & Talukder, Md.Ishtiaq. (2020). Impact of CCTV Surveillance on Crime Prevention: A Study in Dhaka City. 6. 48-59.

⁹⁰ UK CCTV and crime prevention statistics: your FAQs answered. https://www.calipsa.io/blog/cctv-statistics-in-the-uk-your-questions-answered

⁹¹ UK CCTV and crime prevention statistics: your FAQs answered. https://www.calipsa.io/blog/cctv-statistics-in-the-uk-your-questions-answered

percentage of CCTV cameras in London to watch people, these cameras could not prevent the terrorist attacks carried out in July 2005 in London.⁹²

The research conducted by Brandon C. Welsh and David P. Farrington on the impact of CCTV cameras in three places, comprising city center or public housing, public transport, and car parks, demonstrates that the use of camera surveillance systems in car parks was substantially effective to decrease a wide range of crimes, however, in other places which had CCTV cameras, the evidence of desirable effect was minimal.⁹³

Therefore, although installing surveillance control cameras can provide more benefits to the country's national security, the effectiveness of CCTV cameras in reducing crime rates is controversial among scholars. Research shows that the beneficial impacts of surveillance cameras in the reduction of crime rates are questionable, and even some studies suggest that CCTV cameras can create a false sense of personal safety among residents.

Case Study

The UK's parliamentary office in Science and Technology discussed three cases to understand CCTV's specific effects and limitations in three cities, Airdrie, Glasgow, and Birmingham.⁹⁴

Positive: Airdrie95

Airdrie is a town in North Lanarkshire, Scotland. A group of researchers installed CCTV cameras in Airdrie. They intended to evaluate the impact of camera surveillance systems on crime prevention. The statistics show the positive impact of CCTV camera installation in Airdrie over a two-year period. In the first year after installation, there was a significant 21% reduction in recorded crime, surpassing the expected crime reduction trends in surrounding areas, and crimes involving dishonesty, including housebreaking, shoplifting, and theft of and from motor

⁹² Agisilaou, V. H. (2009). Information overload: CCTV, your networks, communities and crime. Australian Security and Intelligence Conference 2009.

⁹³ https://monaulnay.com/wp-content/uploads/2009/03/hors252.pdf

Parliamentary Office Science of and Technology (2002),Postnote. Available at: https://www.parliament.uk/globalassets/documents/post/pn175.pdf Parliamentary Office of Science and Technology (2002),Postnote. Available at:

https://www.parliament.uk/globalassets/documents/post/pn175.pdf

vehicles, decreased by an impressive 48%.⁹⁶ Additionally, there was a noteworthy 16% increase in the crime clear-up rate, primarily for vandalism, drugs, petty assault, and breach of the peace.⁹⁷

As a result, the data indicates that there was little evidence to suggest that crimes were displaced to non-CCTV areas or transformed into different kinds of crime. This suggests that the presence of CCTV cameras had a positive impact on deterring and addressing criminal activities within the town center of Airdrie.

Negative: Glasgow⁹⁸

As we've observed, using CCTV cameras could result in crime reduction in Airdrie. However, recent research demonstrates the negative findings associated with installing 32 CCTV cameras in the city center of Glasgow. Despite the implementation of CCTV cameras, there was an overall increase in the total percentage of crime, which included offenses not directly targeted by the cameras, such as fraud. While certain types of offending saw slight reductions, crimes of dishonesty and indecency increased.⁹⁹

Furthermore, the presence of CCTV had little impact on clear-up rates. This research indicates that public awareness of the CCTV system was low, and 15 months after installation, only 41% of participants were aware of the cameras; as a result, the structure of CCTV did not lead to improved feelings of safety in the city center, and there was no difference in awareness of CCTV between those who felt safe and those who did not. 100

These negative findings from Glasgow highlight the complexities and limitations of CCTV surveillance as a crime prevention measure. While some offenses may see slight reductions, other categories may experience increases. Additionally, the presence of CCTV may not significantly influence public awareness and perceptions of safety. These findings underscore the need to comprehensively evaluate CCTV systems to understand their efficacy and potential limitations in specific contexts.

Parliamentary Office of Science and Technology (2002), Postnote. Available at: https://www.parliament.uk/globalassets/documents/post/pn175.pdf

⁹⁷ Same

⁹⁸ Same

⁹⁹ Same

¹⁰⁰ Same

Mixed: Birmingham¹⁰¹

The third research presents the mixed findings associated with installing 14 CCTV cameras in the city center of Birmingham in the metropolitan country of West Midlands in England during the early 1990s. While the overall crime levels were not reduced, the recorded crime statistics indicated a reduction in robbery and theft from persons; however, the absence of CCTV in car parks led to an increase in theft from vehicles. There was also some evidence of crime displacement to surrounding areas.

Surveys conducted before and after the installation of CCTV showed minimal changes in general feelings of safety for individuals using the city center during the day, however, for those using the city center after dark, there was an increase in feelings of safety among those who were aware of the CCTV cameras. The effects on safety cannot be solely attributed to CCTV, as the area was undergoing redevelopment at the same time.

These mixed findings from Birmingham highlight the complex nature of CCTV's impact on crime prevention and safety. While certain types of offenses may see reductions, others may experience an increase. The absence of CCTV in specific areas, such as car parks, can lead to unintended consequences. The influence of CCTV on feelings of safety may vary depending on the time of day and individual awareness. Overall, a comprehensive evaluation is necessary.

These three cases indicate that CCTV cameras can bring about distinct outcomes. In some places, like Airdrie, certain crimes involving dishonesty, including housebreaking, shoplifting, and theft of and from motor vehicles, crime rates substantially decreased. However, in some conditions, like in Glasgow, the implementation of CCTV in city centers even increased total recorded crime.

In addition, in some cities, there may be decreases in certain offense classifications while the rate of certain crimes might increase. Although installing CCTV cameras did not help reduce the overall crime level, the recorded crime statistics indicated a reduction in a wide range of crimes, like robbery and theft from persons, and the absence of CCTV in car parks led to an increase in theft from vehicles.

¹⁰¹ Same

¹⁰² Same

¹⁰³ Same

Therefore, as recent research indicates, closed-circuit televisions can reduce specific crimes. In contrast, many other factors can result in more desirable effects in numerous conditions. Indeed, CCTV cameras are not the only instrument that could decrease the crime rate in the United Kingdom.

(2) The identification of Criminals

One of the essential elements in criminal justice systems is the identification of offenders engaged in criminal acts. When a crime occurs, the police officers, court, and all correspondent stakeholders implement many measures to search, interrogate, and collect relevant evidence, to detect all individuals who participated in criminal activities.

Closed circuit televisions (CCTV), which have been put in many locations across the country, can be substantially helpful in crime detection. As Dr. Emmeline Taylor stated, the term "detection" is related to using CCTV footage after a crime has occurred, either to bring attention to an unreported incident or to aid police officers in the investigation process.

In the United Kingdom, CCTV cameras are important preventative approaches to address criminal behaviors. The British government uses CCTV cameras to collect information about where the offenders were at the time of the crime, how likely they were to commit crimes and address criminal cases in court.¹⁰⁴

As well, according to the UK's Code of Practice on the Management of Police Information (ACPO), the police have a legal right to obtain information from different sources. The footage obtained by the surveillance system, including CCTV cameras, is one of the common instruments for discovering offenders.

Police and investigatory authorities can review the images obtained by these cameras and serve as valuable evidence to identify individuals involved in criminal acts. Also, Michael Howard, a British politician who launched the Partners Against Crime initiative in 1994, said: "he is absolutely convinced that CCTV has a major part to play in helping detect and reduce crimes and to convict criminals". ¹⁰⁵

¹⁰⁴ Sociology crime prevention essay, South Gloucestershire and Stroud College, Criminology (Crime202), Academic year: 2021/2022. Available at: https://www.studocu.com/en-gb/document/south-gloucestershire-and-stroud-college/criminology/sociology-crime-prevention-essay/45753330

¹⁰⁵ https://www.bbc.com/news/magazine-30793614

CCTV cameras can aid the police and investigatory authorities in the identification of offenders involved in criminal activities. The extensive use of CCTV cameras in the United Kingdom can capture images of criminal incidents as they happen; hence, the recorded videos can be monitored, reviewed, and analyzed to help police forces during investigations to detect more details about criminal activities and identify offenders.

One of the crucial cases which shows the importance of CCTV cameras occurred in the United Kingdom. On February 1993, in Bootle, Liverpool, James Bulger, a two-year-old boy, was abducted and murdered by two boys, Jon Venables and Robert Thompson, while his mother briefly entered a butcher's shop. The offenders took the young boy from the Bootle Strand shopping center to a place where he was subjected to torture and ultimately murdered. The importance of CCTV cameras occurred in the United Strange occurred in the

On 14 February 1993, James' mutilated body was discovered on a railway track. Police could identify perpetrators when they watched images recorded by CCTV cameras. CCTV cameras captured the perpetrators leading James Bulger out of the shopping center, freezing at the moment of their exit.¹⁰⁸ This crucial footage was broadcast nationally, serving as a critical piece of evidence in the investigation and leading to the identification of the suspects.

Following the arrest of Jon Venables and Robert Thompson on February 20, 1993, forensic tests were conducted on their clothing, and these tests revealed the presence of paint samples that matched those found on James' body, further solidifying the link between the perpetrators and the crime scene.¹⁰⁹

The broadcast of this footage brought the issue of CCTV cameras to the forefront of public consciousness and highlighted its effectiveness in providing evidence in criminal cases. The James Bulger case demonstrated the crucial role of CCTV in crime prevention and control. The CCTV cameras installed in many sensitive places, including shopping stores which are heavily susceptible to criminal activities,

¹⁰⁶ Detainment – FILM & TELEVISION BUSINESS. https://film-business.com/tag/detainment/

¹⁰⁷ Barrie Sheldon (2011) Camera surveillance within the UK: Enhancing public safety or a social threat?, International Review of Law, Computers & Technology, 25:3, 193-203, DOI: <u>10.1080/13600869.2011.617494</u>

https://inews.co.uk/news/uk/james-bulger-what-happened-death-murder-killers-jon-venables-robert-thompson-907387

¹⁰⁹ https://inews.co.uk/news/uk/james-bulger-killers-jon-venables-robert-thompson-murder-now-221759

helped prosecutors to present strong proof before the court.¹¹⁰ The images of the moment of James Bulger's exit from the shopping center assisted the police in conducting a successful investigation, identifying potential suspects, and matching the paint samples on James' body with the perpetrators.

The footage not only aided in identifying the suspects but also helped establish their movements and actions during the abduction. The footage captured on CCTV cameras in James Bulger's incident could also significantly reinforce the public conception that the perpetrators will be brought to justice. ¹¹¹ By showcasing the capabilities of CCTV in capturing crucial moments, the incident emphasized the importance of using surveillance technology to deter potential criminals and provide evidence for investigations.

CCTV cameras enable police officers to recognize the offender's face, mainly when there is a high-quality shot of their face, or even gesture, body language, and voice. ¹¹² In addition, police officers would be able to eliminate suspects who are not involved in criminal activities; thereby, it can prevent any unnecessary investigation and saving police time and resources in the line of investigation that would be useful. ¹¹³

Police officers usually use CCTV footage in the first stage to respond to criminal acts, and they would be able to collect all necessary information about the area of crime, the time of crime occurred, and any other relevant information which could help criminal justice actors provide practical evidence in legal proceedings in criminal courts.¹¹⁴

Therefore, the police and investigatory authorities use facial recognition in criminal investigations to track down perpetrators and associate them with particular

LawBirdie. (2023, March 23). Why Public Surveillance Cameras Should Be Banned. Retrieved from https://lawbirdie.com/why-public-surveillance-cameras-should-be-banned/

¹¹¹ Goold, B., Loader, I., & Thumala, A. (2013). THE BANALITY OF SECURITY: The Curious Case of Surveillance Cameras. *The British Journal of Criminology*, *53*(6), 977–996. http://www.istor.org/stable/23639949

¹¹² David P. and others (2010). Feasibility Study on the Impact of CCTV on Criminal Justice Outcomes. Report to National Policing Improvement Agency.

Available at: https://www.crim.cam.ac.uk/sites/www.crim.cam.ac.uk/files/cctvnpia.pdf

¹¹³ David P. and others (2010). Feasibility Study on the Impact of CCTV on Criminal Justice Outcomes. Report to National Policing Improvement Agency. Available at:

https://www.crim.cam.ac.uk/sites/www.crim.cam.ac.uk/files/cctvnpia.pdf

¹¹⁴ Association of chief police officers (ACPO), National Policing Improvement Agency (NPIA), 2011. Practice advice on the use of CCTV in criminal investigations. Available at: https://zakon.co.uk/admin/resources/downloads/cctv-practice-advice-on-the-use-of-cctv-in-criminal-investigations.pdf

activities or places.¹¹⁵ A good-quality recording could be helpful in a significant proportion of cases to allow investigators to watch an entire incident in detail, such as providing information about the sequence of events, the time, location, and the entry and exit routes taken by the offender, victims, and witness.¹¹⁶

Case study

Professor Fiona Brookman and other collaborators conducted research to demonstrate the significance of CCTV cameras in criminal identification. ¹¹⁷ In this research, there were 62 offenders in the 44 homicide cases which were examined. One of these offenders was never found (or charged), and another was found but never put on trial. ¹¹⁸ 32 of 61 offenders were identified, and 51 of 60 were charged by the court through the use of one or more FSTs, including CCTV, DNA, and Phone data. ¹¹⁹

Table 1

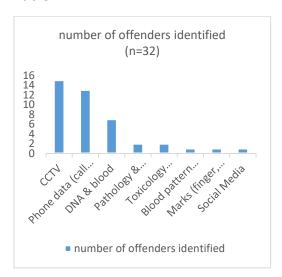


Table 2



¹¹⁵ Bose, Palash & Kabir, Mohammad. (2017). Fingerprint: A Unique and Reliable Method for Identification. Journal of Enam Medical College. 7. 29. 10.3329/jemc.v7i1.30748.

¹¹⁶ Ashby, Matthew. (2017). The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. European Journal on Criminal Policy and Research. 23. 10.1007/s10610-017-9341-6.

¹¹⁷ Brookman, Fiona, and others (2020). The Use of CCTV during Homicide Investigations: Contributions, Challenges and Risks, RESEARCH INSIGHT. Available at:

 $https://pure.southwales.ac.uk/ws/portalfiles/portal/3994343/HIFS_Project_Research_Insight_3._The_Use_of_CCT\\ V_during_Homicide_Investigations_Contributions_Challenges_and_Risks_April_2020_.pdf$

¹¹⁸ Same

¹¹⁹ Same

These tables¹²⁰ demonstrate that 15 of 32 and 35 of 51 were identified and charged by CCTV cameras, which is the biggest number compared to other Forensic science and technologies (FSTs). Therefore, closed-circuit cameras could substantially aid criminal justice actors in detecting crime and identification of offenders.

There should be strong cooperation between CCTV owners, including government officials and private organizations, victims, and criminal justice authorities from the beginning of the investigation process until the imposition of criminal punishment in court. ¹²¹ If all stakeholders work together proficiently, using CCTV cameras can lead to favorable outcomes in detecting criminal behaviors.

However, the benefits of CCTV cameras should not be overstated, though, as many crimes cannot be addressed as a result of camera surveillance systems because criminals can easily conceal their faces by putting on hats, scarves, or glasses; they additionally have the potential to interfere with cameras; and they may even cause malfunctions in cameras shortly after engaged in a crime.¹²²

(3) The spread of feelings of personal safety in the community

According to international human rights law, all individuals are entitled to feel safe in the community, and also states have the legal responsibility to ensure people's safety and protect them against all forms of crimes, violence, and harassment. States use a broad range of measures to ensure people's safety. Many states install CCTV cameras to spread the feeling of personal safety and reduce the fear of crime in society.

The widespread use of CCTV cameras can ensure that all individuals' behaviors, movements, and communications are continuously watched, recorded, and stored by police and security authorities. Thereby, people know that police officers monitor anti-social behaviors, public disorder, and criminal activities and help them detect crime and arrest offenders.

¹²⁰ Same

¹²¹ Baoyan, Kenard Vic. (2023). CLOSED CIRCUIT TELEVISION (CCTV): A TOOL IN CRIME PREVENTION AND DETECTION. 10.13140/RG.2.2.32896.81928.

¹²² Taylor, Emmeline (2020). Understanding the effectiveness of CCTV: Displacement, Deterrence, and Detection: An overview of research prepared for Sevenoaks District Council. School of Arts and Social Sciences City, University of London. Available at: https://cds.sevenoaks.gov.uk/documents/s43565/Appendix%202%20-%20Dr.%20Taylors%20Review%20-%20CCTV evidence%20and%20impact%20overview.pdf?J=1

As technology develops, the modern video surveillance system can provide more information, increase the speed of CCTV information collection, and enable law enforcement authorities to respond immediately when the security indicator is detected.¹²³

For instance, in the United Kingdom, the Sheffield Wide Image Switching System (SWISS) has also integrated other public and privately owned camera systems, including those of an out-of-town shopping mall, tram system, and university, and its cameras are linked to Automatic Number Plate Recognition (ANPR) software that records every people's movement to check vehicles suspected of involvement in criminal activity, and also they have direct communication with police and investigatory authorities where live footage can be released, viewed and where appropriate decisions are taken to prevent crime occurrences and help people make safer.¹²⁴

As a result, CCTV installation can spread feelings of personal safety in society and each individual feels safer. States would be able to establish a safe community, a better living environment and ultimately create a society in which people feel safer. As well, the improvement in crime prevention and a safe environment can bring about Social cohesion, informal social control, and community pride. 126

In the United Kingdom, many people firmly believe that the existence of CCTV cameras can be useful. For instance, as revealed in the Home Office public attitude survey in Glasgow, 95% of respondents said they supported the implementation of CCTV in the city center; in Airdrie, 89 percent of respondents stated CCTV cameras would decrease the fear of crime, and Sutton, in south-east London, 85% of participants believed that the use of CCTV in the town center can strengthen the personal safety in the community.¹²⁷

¹²³ Sung, Chang-Soo & Park, Joo. (2021). Design of an intelligent video surveillance system for crime prevention: applying deep learning technology. Multimedia Tools and Applications. 80. 10.1007/s11042-021-10809-z.

¹²⁴ https://www.statewatch.org/media/documents/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf

Webster, C.. (2009). CCTV policy in the UK: Reconsidering the evidence base. Surveill. Soc. 6. 10.24908/ss.v6i1.3400.4

¹²⁶ Moyo, Sheperd (2019), EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG By submitted in accordance with the requirements for the degree of MAGISTER TECHNOLOGIES in SECURITY MANAGEMENT at the UNIVERSITY OF SOUTH AFRICA. Available at: https://core.ac.uk/download/pdf/286383944.pdf

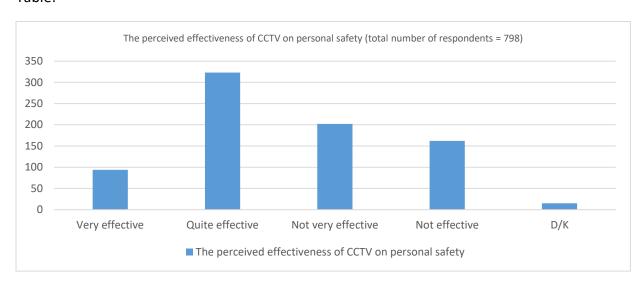
¹²⁷ Fyfe, N. R., & Bannister, J. (1996). City Watching: Closed Circuit Television Surveillance in Public Spaces. *Area*, 28(1), 37–46. http://www.jstor.org/stable/20003625

Many factors play a significant role in the amount of fear of crime among people. CCTV cameras are just one of the instruments to reduce fear of crime. For instance, in the United Kingdom, the impact of closed-circuit televisions in railways on people's personal safety with regard to most serious crimes, including terrorist attacks, is lower compared to the presence of police and other preventative activities, comprising stop and search.¹²⁸

Case study

Terry Honess and Elizabeth Charman researched to examine the potential impact of CCTV cameras on feelings of personal safety. They asked 798 participants whether the presence of CCTV cameras can make them feel safer. The table below shows the results of the survey.

Table:



The research revealed that the majority of respondents, 323 out of them (41%), argued that CCTV camera is quite effective for personal safety. ¹³⁰ They thought that

¹²⁸ Joon Tag Cho, Jisun Park, Exploring the effects of CCTV upon fear of crime: A multi-level approach in Seoul, International Journal of Law, Crime, and Justice, Volume 49,2017, Pages 35-45, ISSN 1756-0616, https://doi.org/10.1016/j.ijlcj.2017.01.005.

⁽https://www.sciencedirect.com/science/article/pii/S1756061616301598)

¹²⁹ Honess, Terry; Charman, Elizabeth, CLOSED CIRCUIT TELEVISION IN PUBLIC PLACES: ITS ACCEPTABILITY AND PERCEIVED EFFECTIVENESS. POLICE RESEARCH GROUP CRIME PREVENTION UNIT SERIES: PAPER NO.35 LONDON: HOME OFFICE POLICE DEPARTMENT.

Available at: http://www.casa.ucl.ac.uk/cyberspace/fcpu35.pdf ¹³⁰ Same

camera surveillance systems could result in a substantial increase in the spread of personal safety, reduce the fear of crimes, and create a safe community.

As well that, 94 out of 798, with 12%, assumed that the use of CCTV cameras is very effective on their feelings of personal safety. As they indicated, if the states use CCTV cameras in numerous places such as streets, highways, schools, hospitals, etc. It can create a safe and secure environment and people feel safer in their community.

However, It is reported that 202 respondents (25%) felt that CCTV cameras could have been more effective, and 162 (20%) stated that putting CCTV in public places is inadequate for personal safety. They might believe that other factors, like the presence of police officers, can substantially affect the level of personal safety in society.

Therefore, most of the respondents, 52% as a whole, positively perceived the effectiveness of CCTV installation on personal safety. It demonstrates that most of the participants in the survey expressed that the presence of CCTV cameras is helpful in feelings of personal security among people.

Overall, we could observe that CCTV surveillance systems enabled police and other agencies to monitor people's behaviors remotely and it has become video surveillance systems an indispensable component of law enforcement strategies to prevent crimes, spread a sense of safety, and identify offenders. Moreover, Politicians and policy-makers continuously highlight the benefits derived from CCTV cameras, which has led to the widespread belief among the public that CCTV cameras can play a substantial role in reducing crimes. 133

CCTV cameras and the right to Privacy in the National Laws of the United Kingdom

In the modern age, we live in a world of technology. As technology advances, states are obliged to establish a set of rules and regulations to protect against any infringement upon a person's privacy brought on by the use of their personal data.

¹³¹ Same

¹³² Same

¹³³ Webster, C.. (2004). The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK. Surveillance and Society. 2. 10.24908/ss.v2i2/3.3376.

¹³⁴ As well, according to a report by Amnesty International, each state is obliged to enact legislation in accordance with international human rights law that protects the right to privacy, confirms its effective implementation, and ensures that any legal provisions to protect national security, including those that allow interference with the right to privacy, are strictly defined and conform to international standards.¹³⁵

For instance, state officials and even private organizations could be allowed to use surveillance technology systems in conformity with international human rights law. State parties monitor individuals' personal lives and should establish rules and regulations to protect people's right to privacy. In addition, as noted in the General Data Protection Regulation (GDPR): "There should be 'binding corporate rules' which means a set of personal data protection rules and guidelines established by a member state."

As a result, there should be personal data protection policies that are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

In the United Kingdom, several laws and regulations specifically outline a wide range of fundamental rights and freedoms for all people regarding the use of surveillance systems, including Closed Circuit Televisions (CCTV) cameras. A number of national laws govern the increasing use of CCTV cameras in the United Kingdom. Most of the United Kingdom's laws deal with many kinds of technological surveillance systems, such as video systems, audio recorders, fingerprints, and facial recognition, which intrude into people's lives.

These regulations are the Human Rights Act (1998), the Regulation of Investigatory Powers Act (2000), the Data Protection Act (1998), the Freedom of Information Act (FOI), and the Protection of Freedoms Act (POFA). ¹³⁶ In this part, we look into these conventions in detail and provide more information on how these rules and

¹³⁴ Tripathi, Keyur and Mubarak, Usama, Protecting Privacy in the Era of Artificial Intelligence (March 24, 2020). Available at SSRN: https://ssrn.com/abstract=3560047 or http://dx.doi.org/10.2139/ssrn.3560047

¹³⁵ Amnesty International (2020). OUT OF CONTROL: FAILING EU LAWS FOR DIGITAL SURVEILLANCE EXPORT.

¹³⁶ McCahill, Michael; Norris, Clive (2002). CCTV in Britain, Centre for Criminology and Criminal justice, University of Hull, Working paper No.3. Available at: http://www.urbaneye.net/results/ue_wp3.pdf.

regulations can preserve the right to privacy of all individuals against any unlawful intrusion through camera surveillance systems.

(1) The Human Rights Act 1998

The first important law which is related to the use of technological surveillance systems in the United Kingdom, comprising CCTV cameras, is the Human Rights Act. This Act was passed in 1998. It introduced the European Convention on Human Rights (ECHR) principles into British law to protect human rights, derogations and reservations, and judicial decisions.

Although the CCTV camera system can prevent human rights violations and aid police officers in criminal investigations, the excessive use of these technologies could be challenging. Because they can infringe upon human rights laws, including the right to privacy, and the personal information obtained through camera surveillance systems can detect separate images of people in crowded places without their consent.¹³⁷

Therefore, the Human Right Act of 1998 was designed in the United Kingdom to preserve, protect, and ensure individuals' privacy. CCTV cameras are extensively installed throughout the country to provide a safe environment and prevent criminal activities. The presence of these cameras can substantially challenge people's privacy and the Human Right Act of 1998 is an inseparable component in the UK's legal framework to preserve the right to privacy.

(2) The Regulation of Investigatory Powers Act 2000 (RIPA)

The second important legislation related to protecting individuals' human rights regarding the use of new technological developments is the Regulation of Investigatory Powers Act. Tony Blair's Labour government introduced this Act to the United Kingdom's House of Commons and it was passed in 2000.

It provides a legal framework for the use of a number of covert investigatory powers. As stated in this Act, the public authorities should use covert investigatory powers compliant with the United Kingdom's obligations under the ECHR, thereby,

¹³⁷ Pauwels, E. (2020). Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention: Opportunities and Challenges for the International Community. Global Center on Cooperative Security. http://www.jstor.org/stable/resrep27551

the use of the powers is always closely supervised and constantly reassessed to ensure that what is being done is justified. 138

This Act establishes a set of rules and regulations to ensure that all surveillance systems used in the investigation process, article 8 of the ECHR, which respects each individual's right to privacy and the use of these covert techniques will only be permitted if it is deemed legal, necessary, and proportionate. Therefore, CCTV cameras that watch people's movements, conservations, and other communications should align with UK law.

(3) The Data Protection Act 1998

One of the most important pieces of legislation in British law is the Data Protection Act. The Parliament of the United Kingdom enacted this Act to protect an individual's personal data. The Data Protection Act was enacted in 1998 and came into force in March 2000 to protect individuals' personal information.

According to this act, the use of CCTV cameras for crime prevention should comply with specific rules and regulations. First of all, there should be clear and visible signs which demonstrate the presence of surveillance schemes, the fair and lawful gathering of data, the relevance of captured images, and the specific and limited use of recorded data, and the Act also prompted the Information Commissioner's Office (ICO) to publish a 'CCTV code of practice' to guide those operating CCTV systems in public access areas.¹⁴⁰

Therefore, as stated in this act, people have the legal right to know what information is held about them, and it establishes a legal framework to ensure that the personal data captured by CCTV cameras in the United Kingdom is processed properly, protects people's private lives and prevents any interference with an individual's the right to privacy.¹⁴¹

(4) The Protection of Freedoms Act (POFA):

The Protection of Freedom Act is the other crucial document in United Kingdom's law. The Protection of Freedoms Bill gained royal assent on 1 May 2012 and has

https://www.gov.uk/government/publications/regulation-of-investigatory-powers-act-2000-ripa/regulation-of-investigatory-powers-act-2000-ripa

https://www.gov.uk/government/publications/regulation-of-investigatory-powers-act-2000-ripa/regulation-of-investigatory-powers-act-2000-ripa

¹⁴⁰ https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf

¹⁴¹ https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf

become the Protection of Freedoms Act 2012. The bill was introduced into the House of Commons on 11 February 2012 and passed into the House of Lords on 12 October 2011.

This Act focuses on several concerns related to human rights and new surveillance technologies. For instance, there are some provisions with regard to closed circuit television and automatic number plate recognition systems, introducing a statutory code of practice, appointing a surveillance camera commissioner who has the responsibility to monitor, review, and report the compatibility of the proliferation of CCTV cameras with the code of practice.¹⁴²

(5) The Freedom of Information Act (FOI):

The Freedom of Information Act is an important Act that was passed on 30 November 2000 and came into force on 1 January 2005 in the United Kingdom. Moreover, after 10 years, the United Kingdom's Cabinet Office established the Independent Commission on Freedom of Information to evaluate the implementation of this act and issued 21 recommendations to ensure that the aims of the original act are properly fulfilled.

This Act highlights that the public authorities should release all information acquired by a public authority in England, Wales, and Northern Ireland, and by United Kingdom-wide public authorities based in Scotland, including drafts, emails, notes, recordings of telephone conversations, and CCTV recordings. ¹⁴⁴ In addition, people have the legal right to access their personal information. The Freedom of Information Act (FOI) is an important legislation that preserves people's right to privacy.

The Impact of CCTV Cameras on the Right to Privacy in the United Kingdom

The United Kingdom is the most surveilled country with regard to European countries. The report published by British Security Industry Association (BSIA)

¹⁴² https://www.gov.uk/government/publications/protection-of-freedoms-bill

¹⁴³ Freedom of Information (FoI) - West Lancashire Borough Council. https://www.westlancs.gov.uk/about-the-council/information-governance/freedom-of-information.aspx

¹⁴⁴ Freedom of Information | The Wilbraham Surgery. https://wilbrahamsurgery.nhs.uk/freedom-of-information/

stated that there are almost 6 camera control systems across the country, meaning there are almost 10 cameras for each person.

The high number of CCTV cameras in the United Kingdom has both benefits and drawbacks. On the one hand, using CCTV systems can be useful to prevent criminal activities, help police and investigatory authorities watch the entire incident to detect different types of crimes, and improve public safety. For instance, CCTV cameras have been instrumental in solving 7/7 bombings in London and the 2017 Manchester Arena attack.

However, all specialists are continuously concerned about the consequences of surveillance technology, including CCTV cameras on persons who are monitored and on democratic society as a whole. ¹⁴⁵ The technical improvement in surveillance system technologies, particularly video recognition, can have a significant impact, specifically on people's privacy rights.

Although CCTV cameras continue to be useful instruments to prevent crimes, identify potential offenders, and protect people in society, the massive use of CCTV surveillance systems in public and private places by people or any organizations could increase the risk of infringement upon an individual's privacy rights.

In addition, Civil liberty counsel raises concerns that the increased use of surveillance systems, specifically closed circuit cameras (CCTV), can infringe individual rights to privacy because the CCTV systems can access personally identifiable information containing people's images is under scrutiny.¹⁴⁶

As indicated in the Report of the United Nations High Commissioner for Human Rights on The right to privacy in the digital age: "The operation of AI systems can facilitate and deepen privacy intrusions and other interference with rights in a variety of ways. These include entirely new applications as well as features of AI systems that expand, intensify or incentivize interference with the right to privacy, most notably through increased collection and use of personal data." ¹⁴⁷

Throughout the United Kingdom, we can observe approximately 6 million CCTV cameras in every place, which is the highest number following China and the United

¹⁴⁵ Friedewald, Michael & Cas, Johann & Bellanova, Rocco & Burgess, J. & Peissl, Walter. (2017). Surveillance, Privacy and Security: Citizens' Perspectives. 10.4324/9781315619309.

¹⁴⁶ IvyPanda. (2019, November 17). *Effects of Surveillance Technology on Privacy.* https://ivypanda.com/essays/the-spread-of-surveillance-technologies-as-closed-circuit-cameras-on-privacy/

¹⁴⁷ G2124921.pdf (un.org)

States. These cameras are installed by numerous governments, police forces, local authorities, and residents. Therefore, all people are constantly under mass visual surveillance by CCTV cameras across the country. 149

Numerous places in all cities are equipped with a huge number of professional CCTV cameras. All people can go to parks, shopping centers, and cinemas. These places can offer a sense of privacy. However, there are a large number of CCTV cameras that observe people's behaviors. So, many people would not be able to lead regular lives, and when they leave their homes, they can feel as though they are being watched and recorded constantly by the government, and it could give the impression that they are in prison. ¹⁵⁰

People might believe that they lose their privacy. The constant camera surveillance may prompt some members of the public to change their even proper social behaviors because they don't want to attract the notice of the police or run the danger of having their conduct misconstrued.¹⁵¹

Critics argue that the prevalence of CCTV cameras could contribute to a culture of surveillance and erode the privacy of individuals. This constant surveillance of individuals' behaviors, activities, and communications in public places, collection and even retention of a mass amount of personal data by the government could reduce people's privacy. ¹⁵² Individuals might feel that they are subjected to arbitrary interference with their privacy, family, or correspondence and to attacks upon their honor and reputation.

Kate Logan, Senior Legal Counsel at Amnesty International¹⁵³, declared that "The unfettered harvesting and processing of millions of people's private communications must end. Today's ruling marks a significant step forward in

Königs, P. Government Surveillance, Privacy, and Legitimacy. *Philos. Technol.* **35**, 8 (2022). https://doi.org/10.1007/s13347-022-00503-9

Webster, C.. (2009). CCTV policy in the UK: Reconsidering the evidence base. Surveill. Soc. 6. 10.24908/ss.v6i1.3400.

LawBirdie. (2023, March 23). Why Public Surveillance Cameras Should Be Banned. Retrieved from https://lawbirdie.com/why-public-surveillance-cameras-should-be-banned/

¹⁵¹ Benjamin J Goold, "CCTV and Human Rights" in Citizens, Cities and Video Surveillance: Towards a Democratic and Responsible Use of CCTV (Paris: European Forum for Urban Security, 2010) 27.

¹⁵² Königs, P. Government Surveillance, Privacy, and Legitimacy. *Philos. Technol.* **35**, 8 (2022). https://doi.org/10.1007/s13347-022-00503-9

¹⁵³ A Brief Look at Human Rights Violations: (part 18) The UK. https://www.odvv.org/blog-3292-A-Brief-Look-at-Human-Rights-Violations--part-18-The-UK

condemning surveillance at the whim of the government."¹⁵⁴ An individual's right to privacy can be affected in different ways. Although according to Article 8 of the European Convention on Human Rights (ECHR), the states are not required to establish specific legislation to regulate a particular technology, such as CCTV surveillance systems, what is needed is that where a technology interferes with an individual's privacy rights, there should be a set of legal provisions and guidelines accessible to all people, foresee the consequences of CCTV technology, and provides adequate protection against any infringement upon the right to privacy.

In some ways, using Al-powered surveillance systems can lead to many problems and even may interfere with an individual's right to respect his private and family life, his home, and his correspondence. We evaluate the impact of CCTV cameras on the right to privacy and assess how the United Kingdom's law protects people against any infringement upon their private lives.

These ways are:

(1) The mere retention of massive CCTV footage in the United Kingdom

Modern technological developments have substantially resulted in the use of different types of surveillance systems powered by artificial intelligence. These systems would be able to capture people's movements, track the location of mobile phones, record the activities of individuals, or document environmental auditory signals.¹⁵⁶

One of the common surveillance systems in the world is Closed Circuit Televisions (CCTV) cameras. These cameras are embraced to monitor an individual's physical activity to prevent crime, disorder, and anti-social behavior, reduce the 'fear of crime', and reassure the whole public about community safety.¹⁵⁷

In the United Kingdom, there are innumerable CCTV cameras everywhere. CCTV cameras are not restricted to local governments, and some people install cameras

¹⁵⁴ https://www.amnesty.org/en/latest/press-release/2021/05/uk-surveillance-gchq-ecthr-ruling/

Charlesworth, Andrew, CCTV, Data Analytics and Privacy: The Baby and the Bathwater (August 20, 2018). Available at SSRN: https://ssrn.com/abstract=3606278 or https://ssrn.3606278

¹⁵⁶ Rascão, Jose & Poças, Nuno. (2021). Freedom of Expression and the Right to Privacy and Ethics in Dialectic of Human Rights in This Complex and Turbulent Society. International Journal of Project Management and Productivity Assessment. 9. 1-28. 10.4018/IJPMPA.2021070101.

Webster, C.. (2009). CCTV policy in the UK: Reconsidering the evidence base. Surveill. Soc. 6. 10.24908/ss.v6i1.3400.4

at home to protect their property. The prevalence of this technology in public and private spaces raises ethical questions about the balance between security and fundamental human right.

A wide range of CCTV cameras exist in the United Kingdom. People are under mass visual surveillance, and states can observe and capture every individual's movements across a network of CCTV cameras. Thus, Smart CCTV cameras can collect, use, and store people's sensitive personal information about everyone's personal life.¹⁵⁸

However, many people firmly believe that individuals or groups might store their personal information, including facial features, movements, and communications, in a researchable database for an unnecessary period of time. Some organizations might keep the images obtained from CCTV cameras longer than needed.

The retention of CCTV footage can infringe upon their right to respect their privacy under Article 8 of the ECHR. In addition, it can also decrease public trust in the British government and release public perception that everyone's movements in the daytime are continuously captured and retained for an illegitimate period of time.

Many organizations, police, and investigators are likely to retain CCTV footage for longer than is necessary for the purpose for which it is processed. For instance, all states may use CCTV cameras for different purposes. The British government uses a network of cameras in political protest to manage protests from a distance through the transmission of overview shots, prohibit any legal violations, identify those who cause trouble, avoid conflicts among people, and ensure national security.¹⁵⁹

Although the state monitors peoples' behaviours in political protest to ensure national security, the police and security forces are not authorized to store CCTV footage for longer than they need. The retention of personal information related

¹⁵⁸ Königs, P. Government Surveillance, Privacy, and Legitimacy. Philos. Technol. 35, 8 (2022). https://doi.org/10.1007/s13347-022-00503-9

¹⁵⁹ Knopp, Philipp & Ullrich, Peter. (2018). Protesters' Reactions to Video Surveillance of Demonstrations. Counter-Moves, Security Cultures, and the Spiral of Surveillance and Counter-Surveillance. Surveillance & Society. 16. 10.14279/depositonce-7186.

to people's participation in political protests within the searchable database can result in interference with people's right to privacy.

Therefore, a legal framework exists to compensate and address any infringements resulting from the use of AI surveillance systems, so states would be able to ensure that all individuals' right to privacy is preserved. There should be a set of rules and regulations for the storage of CCTV footage on how, when, and for how long the images obtained by Camera control systems should be maintained on a database. 161

In the United Kingdom, there is no set time to keep recorded CCTV footage by any organization. However, the competent authorities are permitted to keep the images captured by CCTV cameras for a reasonable time, and they will not be authorized to store users' personal data for an unnecessarily long time. The United Kingdom's Surveillance Camera Code of Practice states: No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

Thereby, according to British law, each individual or organization should record CCTV footage for a specific purpose. Indeed, CCTV owners, individuals, or groups have the legal responsibility to determine the purpose of CCTV cameras, which includes why the camera is there, what it is looking at, and what will be carried out with the recorded footage. Also, organizations should set their own deadlines. They would be able to continue to store CCTV images as long as they need them. CCTV camera footage cannot be kept for a limited length of time. Once the purpose is fulfilled, any personal information about an individual ought to be removed from the database.

For instance, if police officers intend to observe the recorded footage in the investigation process, they have permission to watch them within a reasonable period of time and they would not be able to review the recorded surveillance footage before the crime is committed or after the case is resolved by criminal

¹⁶⁰ Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160

¹⁶¹ Agisilaou, V. H. (2009). Information overload: CCTV, your networks, communities and crime. Australian Security and Intelligence Conference 2009.

¹⁶² https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf

¹⁶³Surveillance Camera Code of Practice – 12 Principles | The Data Compliant Blog. https://datacompliantblog.com/2014/10/16/surveillance-camera-code-of-practice-12-principles/

 $^{^{164}} file:///C:/Users/jniki/Downloads/20200724\% 20 Storing\% 20 and \% 20 Retention\% 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 images\% 20 V2.0\% 20 (2.0) and Markov 20 CCTV\% 20 (2.0) and Markov 2$

courts.¹⁶⁵ As a result, if the observer needs to observe more footage of a specific incident, they have the responsibility to send an additional request that includes compelling reasons, which should be evaluated by the competent authorities.¹⁶⁶

As a consequence, the high proportion of CCTV cameras in the United Kingdom can result in the public conception that all individuals' personal activities are continuously being monitored and stored for a considerable amount of time by people and other organizations. It can particularly intrude into individuals' private activities, movements, and communications, and those who are constantly under close surveillance might feel they have lost control over the use of their personal information. Ultimately, this continuous surveillance and storage of CCTV footage could lead to distrust between the British government and the people.

Case Study: R (Catt) v. Association of Chief Police Officers (2015)

In this section, we discuss one of the cases which demonstrates how some institutions, police, and local authority keep those images longer than is authorized in United Kingdom law. This case was brought by Mr. Catt, as the Claimant, against the Association of Chief Police Officers before the court in 2015; the Claimant ("Mr. Catt") challenges the Defendants' retention of data ("the data") relating to his attendance at various political protests on the National Domestic Extremism Database. This case indicated that the retention of images captured by CCTV cameras could result in an individual's right to privacy.

Mr. Catt, the Claimant, launched a legal challenge in the Supreme Court against the Defendants, the Association of Chief Police Officers, and he questioned the retention of data related to his participation in political protests.

Mr. Catt lived in Brighton, a city in the United Kingdom. He participated in political protests in 2005. Although the police officers arrested him several times, the courts never convicted him. He participated in political protests in a non-violent manner with the group named "Smash EDO" which engaged in some violent criminal activities during all the events, and the police stored personal information of Mr.

¹⁶⁵ https://www.scitepress.org/Papers/2020/89642/89642.pdf

¹⁶⁶ https://www.scitepress.org/Papers/2020/89642/89642.pdf

¹⁶⁷ Macnish, K orcid.org/0000-0003-4510-3049 (2018) Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. Journal of Applied Philosophy, 35 (2). pp. 417-432. ISSN 0264-3758 https://doi.org/10.1111/japp.12219

¹⁶⁸ https://ukhumanrightsblog.com/2015/03/06/public-protest-private-rights/

Catt, as one of the participants, including his presence, date of birth by "information records". 169

This data was related to the act of claimants in political protests in 2005, which is stored on the National Domestic Extremism Database, which is maintained by the National Public Order Intelligence Unit (NPOIU) under the authority of the National Coordinator for Domestic Extremism (NCDE).¹⁷⁰

Mr. Catt accepted that the police are entitled to record "Smash EDO"'s activities in political protest to ensure the national security of all individuals, still he asked the court to assess whether the retention of such sensitive information on the searchable database is legal or not.¹⁷¹ We examine the implications of the retention of sensitive data on the Database and the subsequent Judicial Review initiated to assess systematic collection and retention by police authorities of electronic data about individuals is lawful or contrary to Article 8 of the European Convention on Human Rights.

The courts evaluated the lawfulness of the retention of claimant data on the National Domestic Extremism Database and then they examined the impact of such infringements on the right to privacy. Indeed, The aim of retention of Mr. Catt's images in a researchable database was to enhance national security and enable law enforcement agencies to identify and monitor potential threats posed by domestic extremists.

Mr. Catt's case draws attention to the retention of personal information within the Database, specifically focusing on the lawfulness and appropriateness of storing such data related to political protests. Mr. Catt's case prompts a Judicial Review, a process designed to scrutinize the legality of the Defendants' actions concerning data retention on the National Domestic Extremism Database. ¹⁷²

Mr. Catt's legal challenge against the retention of data on the National Domestic Extremism Database serves as a catalyst for a thorough examination of the legality and implications surrounding the storage of sensitive information related to

¹⁷⁰ same

¹⁶⁹ same

¹⁷¹ https://vlex.co.uk/vid/r-catt-v-association-805385985

¹⁷² https://vlex.co.uk/vid/catt-v-association-of-793520813

political protests. Mr. Catt's brought a complaint to the court based on two fundamental grounds:

- (1) Firstly, the retention of the images of his participation in political protests in 2005 captured by CCTV cameras violated his privacy rights under Article 8 ECHR and was neither a necessary nor proportionate response to the achievement of any legitimate aim.
- (2) Secondly, data retention did not comply with the requirements of the Data Protection Act 1998 (the DPA). As principle 5 of this Act placed a limit on the amount of time the controller can store personal information on the individual and states: "Personal data should not be kept longer than it is needed for. Personal data cannot be stored indefinitely until such a time it may serve a purpose."

Therefore, Mr. Catt's claimed that the retention of personal data captured by CCTV cameras intrudes on his right to privacy.

This case was brought to the Supreme Court. The Supreme Court accepted that Article 8 of the ECHR states that the claimant possesses the right to "respect for his private and family life, his home and his correspondence". However, all five justices in the court agreed that the retention of personal footage by the Association of Chief Police Officers within the Database related to political protests is in accordance with Article 8 of ECHR.¹⁷³

Lord Sumption stated the leading opinion of the majority. The information stored on the National Domestic Extremism Database was about the Smash EDO's activities and Mr. Catt's participation in the political protest and it was in no sense intimate or sensitive information and the retention of the claimant's information is lawful based on three fundamental grounds:¹⁷⁴

- "(1) The retention of data enables the police to make a more informed assessment of the risks and threats to public order;
- (2) The police could investigate criminal offenses where there have been any and to identify potential witnesses and victims;
- (3) They would be able to study the leadership, organization, tactics, and methods of protest groups that have been persistently associated with violence."¹⁷⁵

¹⁷³ https://hudoc.echr.coe.int/fre?i=001-189424

¹⁷⁴ Same

¹⁷⁵ Same

The United Kingdom Supreme Court held that the surveillance camera code of practice passed in the United Kingdom further states that the images captured from CCTV cameras should be stored for how long, which is necessary for the surveillance camera system's stated purpose, and they should be removed once those purposes have been accomplished.

Although the surveillance camera code of practice does not provide specific periods for the retention of CCTV footage, it requires a data controller to justify an appropriate retention period and the images of claimant's political protests on the National Domestic Extremism Database should be stored for no longer than is necessary to achieve the specific purpose for which it is processed.¹⁷⁶

The court accepted that the police had a legal right to keep the claimant's participation in political protests as they occurred, and the retention of personal data obtained through CCTV surveillance systems on a searchable database by police forces is in line with article 8 and can be kept on a database for the necessary period of time, even if the individuals are not suspected of any wrongdoing, did not infringe upon the right to respect for private life under Article 8 of ECHR.

Therefore, as indicated in the case above, the proliferation of CCTV is an effective crime prevention instrument that uses cameras to monitor and record an individual's activities in numerous places. British police officers use CCTV cameras for security surveillance in political protests. These systems rely on large databases containing millions of images, many captured from an individual's activities without the user's consent. However, governments might use technological surveillance equipment, without any boundaries, to monitor, record, and store mobile activities in certain situations, which can pose a threat to an individual's right to privacy and personal data.¹⁷⁷

People assume that their movements in numerous places, including in political protests, are constantly monitored and archived by states for an unnecessary period. The extensive use of CCTV cameras might disseminate the public perception that all individuals are under close surveillance and they lose control

 $https://www.data protection.ie/sites/default/files/uploads/2019-05/CCTV\%20 guidance\%20 data\%20 controllers_0.pdf$

¹⁷⁷ Odoemelam Chika, Adapting to Surveillance and Privacy Issues in the Era of Technological and Social Networking, International Journal of Social and Humanity, Vol.5, No.6, June 2015 Available at: http://www.ijssh.net/papers/520-H140.pdf

over the use of their personal activities. The continuous surveillance and retention of peoples' images on a database can particularly intrude into individuals' privacy rights and ultimately lead to distrust between the British government and the people.

(2) The lack of freely given, specific, and informed consent of the data subject

Al-powered surveillance systems are monitoring systems that use artificial intelligence (AI) algorithms to collect, use and store sensitive personal information about individuals. Closed Circuit Televisions (CCTV) cameras could reveal sensitive information about everyone's personal life, including facial features, voice, and images that are essential to the identification of a person.¹⁷⁸

In the United Kingdom, numerous people or organizations, including the police, local authorities, and the private sector, could monitor an individual's movements through CCTV cameras. These different stakeholders are responsible for maintaining public safety in society and preventing any criminal activities or unlawful behaviors which can destroy public order through the use of surveillance technological systems.

Using CCTV cameras in public areas across the United Kingdom enables all official authorities to constantly monitor and record the activities, behaviors, and personal information of any individual on a daily basis. CTV cameras capture all footage and images in public places, such as entering an infertility clinic or a psychiatrist's office. ¹⁸⁰

Today, many governments use a wide range of surveillance technologies in the country to control crime occurrences and ensure national security with the fitting of close-circuit cameras in public places, shopping halls, buildings, streets, and workplaces, enabling monitoring of activities and communication without the

¹⁷⁸ Fitwi, Alem, Yu Chen, Sencun Zhu, Erik Blasch, and Genshe Chen. 2021. "Privacy-Preserving Surveillance as an Edge Service Based on Lightweight Video Protection Schemes Using Face De-Identification and Window Masking" *Electronics* 10, no. 3: 236. https://doi.org/10.3390/electronics10030236

Mahmood Rajpoot, Q., & Jensen, C. D. (2015). Video Surveillance: Privacy Issues and Legal Compliance. In V. Kumar, & J. Svensson (Eds.), Promoting Social Change and Democracy through Information Technology IGI global.
 Mahmood Rajpoot, Q., & Jensen, C. D. (2015). Video Surveillance: Privacy Issues and Legal Compliance. In V. Kumar, & J. Svensson (Eds.), Promoting Social Change and Democracy through Information Technology IGI global.

consent of the subjects, they may forget the harm which poses to the citizens on the privacy issue and undermine their free social interaction.¹⁸¹

Individuals might be under massive visual surveillance by technological equipment. The monitored people might not know or informed that numerous institutions and bodies across the country observe all their activities. Tony Porter, who served as Surveillance Camera Commissioner from March 2014 until December 2020, in the United Kingdom, said: "The privacy of the public is at risk of being invaded on a mass scale without its consent as the collection of big data meshes with the proliferation of video surveillance."

Besides, intelligent CCTV systems could observe everyone in a particular area. Individuals or organizations may install CCTV cameras to identify potential offenders and persons who are subject to be in danger. Therefore, CCTV surveillance systems provide state, police, and local authorities with the capability to watch an individual's movements permanently; thereby, all individuals should be informed of the prevalence of CCTV cameras in a specific area so they can decide how to behave in society.¹⁸²

However, the operatives may also unintentionally observe non-involved individuals. Therefore, it is possible to identify everyone without their permission, which may intrude on their privacy. ¹⁸³ Therefore, it is possible to identify everyone without their permission, which may intrude on their privacy.

Therefore, the first step to protect people's privacy right and prevent the possibility to misuse of the personal information acquired by CCTV cameras is to obtain explicit, specific, and informed users' consent.¹⁸⁴ Before implementation of surveillance, it is required to notify people that they are monitored by electronic equipment from a distance and those bodies or institutions should ask for the

¹⁸¹ IvyPanda. (2019, November 17). *Effects of Surveillance Technology on Privacy*. https://ivypanda.com/essays/the-spread-of-surveillance-technologies-as-closed-circuit-cameras-on-privacy/

¹⁸² A Review of the Increased use of CCTV ad Video-Surveillance for crime prevention purposes in Europe, Policy Department C, Citizens' Rights and Constitutional Affairs, PE 419.588, April 2009

Available at : https://www.statewatch.org/media/documents/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf

¹⁸³ Koch H., Matzner T. & Krumm, J., "Privacy Enhancing of Smart CCTV and its Ethical and Legal Problems", in European Journal of Law and Technology, Vol 4., No. 2., 2013.

¹⁸⁴ Catarina Fontes, Ellen Hohma, Caitlin C. Corrigan, Christoph Lütge, Al-powered public surveillance systems: why we (might) need them and how we want them, Technology in Society, Volume 71, 2022, 102137, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2022.102137.

monitored person's permission to use all footage and images which have been captured by CCTV cameras.

likewise, those who are responsible for CCTV surveillance systems maintain the non-involved parties' identities concealed and leave the target subjects unmasked, so, they would be able to prevent users from recognizing other people and collecting their personal information or watching their actions on the scene.¹⁸⁵

As stated in the law of the United Kingdom, official authorities have a legal responsibility to inform the public about the presence of CCTV surveillance systems through the use of signs or notices which indicate that CCTV cameras exist in a particular area or place. 186

As a result, as mentioned above, consent by all monitored individuals is a legal requirement for CCTV surveillance. Also, the surveillance camera code of practice respects people's legal right to know if, when, and by whom they are being surveilled through indicators that demonstrate the existence of CCTV cameras in every place.¹⁸⁷

According to the surveillance camera code of practice (1.5): "The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterized as surveillance by consent, and such consent on the part of the community must be informed consent and not assumed by a system operator." 188

However, one of the challenges with people's right to privacy in the United Kingdom is that recent research shows more instances of signs; over three-quarters of those used to indicate the presence of CCTV cameras in particular locations like London is inconsistent with the camera surveillance code of practice. 189

¹⁸⁵ Kok-Seng Wong, Nguyen Anh Tu, Anuar Maratkhan, and M.Fatih Demirci. 2021. A Privacy-Preserving Framework for Surveillance Systems. In 2020 the 10th International Conference on Communication and Network Security (ICCNS 2020). Association for Computing Machinery, New York, NY, USA, 91–98. https://doi.org/10.1145/3442520.3442524 ¹⁸⁶ Mahmood Rajpoot, Q., & Jensen, C. D. (2015). Video Surveillance: Privacy Issues and Legal Compliance. In V. Kumar, & J. Svensson (Eds.), Promoting Social Change and Democracy through Information Technology IGI global. ¹⁸⁷ Cole, Mark. (2004). Signage and Surveillance: Interrogating the Textual Context of CCTV in the UK. Surveillance and Society. 2. 10.24908/ss.v2i2/3.3387.

¹⁸⁹ Cole, Mark. (2004). Signage and Surveillance: Interrogating the Textual Context of CCTV in the UK. Surveillance and Society. 2. 10.24908/ss.v2i2/3.3387.

In addition, Article 4(11) of the General Data Protection Regulation (GDPR) defines consent: "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." 190

Article 4(9) of the General Data Protection Regulation (GDPR) illustrates that: "recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;" 191

Therefore, according to GDPR, the states should monitor, collect, and process individual personal information with prior consent and knowledge of the data subject. However, one of the controversial issues is whether the states should have an individual's knowledge and consent in every condition when they intend to monitor their citizens and access their personal information.

This section discusses one of the case laws in the United Kingdom. In this case, we could assess how the presence of freely given, specific, and informed consent from the person subject to CCTV surveillance is essential to respect people's privacy rights.

Case Study: Intrusive CCTV Monitoring and Privacy Violation 192

The case below examine the unauthorized and intrusive use of CCTV cameras in the United Kingdom, where the defendants infringed upon the privacy of the claimants. The defendants installed surveillance cameras and audio recording devices without consent, targeting both the claimants' property and their private lives. The court's findings highlight the extensive breaches and their impact on the claimants, emphasizing the importance of privacy protection and the consequences of unlawful surveillance.

In a converted semi-detached house, the claimants resided in an upstairs flat, while the defendants owned the downstairs flat, Despite the separation of front and

¹⁹⁰ https://gdprtool.cyberwatching.eu/Pages/Workflow.aspx

¹⁹¹ definitions · Sunny Cars. https://www.sunnycars.de/deen/security-and-data-protection/definitions/

¹⁹² https://www.lexology.com/library/detail.aspx?g=854e9b90-2dab-4d99-9c9a-70bb1e85b27b

garden areas, the defendants deliberately set up their CCTV cameras to capture the claimants' private property for an extended period. 193 The cameras recorded incessantly, storing footage for five days, while the defendants had remote access to the surveillance system. The defendants failed to register as data controllers and did not provide transparency notices to the claimants regarding the monitoring. 194

The claimant brought a case to the court. He asserted that the defendant installed a CCTV camera without his consent, targeting both the claimants' property and their private lives. 195 As stated in GDPR and United Kingdom's law, it is illegal to record somebody's behavior without his consent and it is necessary to take the permission of the monitored person.

This case was brought to the court in the United Kingdom. The court found that the defendants had no legitimate reason for their surveillance's intrusive nature and extent. 196 The defendants' failure to provide evidence explaining the monitoring further undermined their case. The defendants falsely claimed their property was a private residence, attempting to justify their actions through exemptions. However, the Information Commissioner's Office (ICO) rejected this claim and emphasized they need a clear consent and maximum information disclosure in such cases. 197

The court described the defendants' surveillance as highly intrusive, excessive, and unjustified. The claimants suffered extreme stress, limiting their use and enjoyment of their own homes. They restricted their movements, conversations, and even their use of the rear garden due to uncertainty about the coverage. They acknowledged the oppressive and unfair nature of the defendants' actions, noting that the monitoring was unnecessary and served no legitimate purpose.

The court ruled in favor of the claimants and acknowledged the breaches of privacy and the negative impact on their lives. The defendants' delayed or non-responsive handling of subject access requests further demonstrated their disregard for privacy rights, and the court emphasized the need for freely given, specific, and

¹⁹⁴ Same

¹⁹³ Same

¹⁹⁵ Same

¹⁹⁶ Same

¹⁹⁷ Same

informed consent, respecting individuals' privacy within their personal residences, and avoiding unwarranted surveillance. 198

As a consequence, this case indicated the unlawful use of CCTV cameras and audio recording devices by the defendants, which infringed upon the claimants' privacy. The court recognized the severity of the breaches, emphasizing the surveillance's intrusive, oppressive, and unjustified nature. The ruling upheld the claimants' privacy rights and highlighted the importance of transparency, legitimate justifications, and clear consent to respect individuals' privacy within their private property. This case serves as a significant precedent, underscoring the need for proper authorization and adherence to legal procedures in the implementation of surveillance systems, protecting individuals' privacy in a technologically advanced world.

Therefore, it is important to mention that the application of CCTV cameras should comply with fundamental rights and regulations set forth in international agreements and United Kingdom's law. No organization could monitor individuals' private property without their knowledge. The unauthorized and intrusive use of CCTV cameras can infringe upon the privacy of the claimants.

In the United Kingdom, installing secret surveillance technologies is unlawful. 199 Individuals should be aware that any person or organization is observing them and must provide informed consent before their personal information is acquired. It ensures that the British government considers the recipient's privacy and data protection rights carefully.²⁰⁰

(3) The misuse of CCTV footage

This huge number of CCTV surveillance systems in society can face several challenges. The British government should respect and protect individuals' private lives and help them keep their rights to privacy when new monitoring technology systems challenge it. In the United Kingdom, one of the most watched countries,

¹⁹⁹ Richards, N. M. (2013). THE DANGERS OF SURVEILLANCE. Harvard Law Review, 126(7), 1934-1965. http://www.jstor.org/stable/23415062

²⁰⁰ Dorraji, Seyed & Barcys, Mantas. (2014). Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations. Social Technologies. 4. 306-317. 10.13165/ST-14-4-2-05.

there is 1 CCTV camera for every 10 people. People are under massive surveillance by states.

All people need an amount of privacy, while a network of cameras located everywhere monitors their behaviors, communications, and their surroundings, and they are not commonly aware of who monitors them, whether these photographs are being misused in undesirable ways or not, and who has access to CCTV footage.²⁰¹

However, the images captured through CCTV cameras in houses, workplaces, or even public places will likely be misused for a purpose beyond those they were initially intended. Many persons or organizations authorized to use CCTV cameras under British law are likely to collect personal information for a specific purpose and use it for undesirable purposes.²⁰²

For instance, in the United Kingdom, state authorities implement CCTV cameras to ensure the country's national security. They may even install video surveillance to prevent crimes before it takes place, investigate criminal activities and detect a suspected offender. However, this sensitive information might be used for personal and domestic purposes, which is not compatible with the primary purpose.²⁰³

According to the BBC report (2005), in the United Kingdom, the employees who worked in the council looked into a woman's apartment through a CCTV camera installed there.²⁰⁴

The presence of CCTV cameras for illegitimate purposes would be particularly intrusive and undermine the right to privacy. The police and public authorities have a legal responsibility to notify all individuals about the purpose of CCTV cameras,

²⁰¹ Benjamin J Goold, "CCTV and Human Rights" in Citizens, Cities and Video Surveillance: Towards a Democratic and Responsible Use of CCTV (Paris: European Forum for Urban Security, 2010) 27.

²⁰² Pelteret, Marc & Ophoff, Jacques. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. Informing Science The International Journal of an Emerging Transdiscipline. 19. 277-301. 10.28945/3573.

²⁰³ G. F. Shidik, E. Noersasongko, A. Nugraha, P. N. Andono, J. Jumanto and E. J. Kusuma, "A Systematic Review of Intelligence Video Surveillance: Trends, Techniques, Frameworks, and Datasets," in IEEE Access, vol. 7, pp. 170457-170473, 2019, doi: 10.1109/ACCESS.2019.2955387.

²⁰⁴ Mahmood Rajpoot, Q., & Jensen, C. D. (2015). Video Surveillance: Privacy Issues and Legal Compliance. In V. Kumar, & J. Svensson (Eds.), Promoting Social Change and Democracy through Information Technology IGI global.

and the public must also be able to trust that these systems will not be misused for political or other illegitimate purposes.²⁰⁵

Benjamin J. Goold stated, "We cannot know whether the images obtained by the cameras will be kept or who might have access to them; we cannot be sure that they will not be misinterpreted or used in objectionable ways." ²⁰⁶

In addition, British law confirmed that one of the essential principles related to the use of video surveillance technologies is that each person or organization should use CCTV cameras to monitor individuals and their surroundings for a specific purpose. Based on the surveillance camera code of practice (2.6.1): "Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need." 207

Article 5(1) of the GDPR states that Personal data shall be:

"Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')."

Furthermore, as indicated in Guidelines 3/2019 on the processing of personal data through video devices, adopted on 10 July:

"While individuals might be comfortable with video surveillance set up for a certain security purpose, for example, guarantees must be taken to avoid any misuse for totally different and — to the data subject — unexpected purposes (e.g., marketing purpose, employee performance monitoring, etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques, increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse. The general

²⁰⁵ Benjamin J Goold, "CCTV and Human Rights" in Citizens, Cities and Video Surveillance: Towards a Democratic and Responsible Use of CCTV (Paris: European Forum for Urban Security, 2010) 27.

²⁰⁶ https://commons.allard.ubc.ca/cgi/viewcontent.cgi?article=1151&context=fac pubs

²⁰⁷ Paul Tennent - Surveillance Camera Code of Practice - Infologue.com - Manned Security e-Zine. https://www.infologue.com/editorial/paul-tennent-surveillance-camera-code-of-practice/

²⁰⁸ Purpose Limitation | isltEthical. https://www.isitethical.org/portfolio-item/purpose-limitation/

principles in GDPR (Article 5) should always be carefully considered when dealing with video surveillance."²⁰⁹

The issue with data misuse lies in the fact that it might be used for objectives that were not initially intended. This act can violate an individual's privacy rights and also lead to distrust between the controller and its recipient. The British government is responsible for ensuring everyone's privacy right is protected because many individuals may believe that the personal information collected can be accessed for illegitimate purposes. No organization or people are not legally permitted to use, share and store data for incompatible purposes which are not initially intended.²¹⁰

Based on UK's code of practice (3.1.3): "A surveillance camera system should only be used in a public place for the specific purpose or purposes it was established to address. It should not be used for other purposes that would not have justified its establishment in the first place. Any proposed extension to the purposes for which a system was established and images and information are collected should be subject to consultation before any decision is taken." ²¹¹

Therefore, the images obtained through CCTV cameras containing identifiable individuals should be used for specific purposes. It should not be used for other purposes that would not have been compatible with the initial purpose. In this section, we examine one of the law cases which was brought by Geoffrey Dennis Peck, a UK national, before the ECHR.

Case Study: Peck v United Kingdom

This case was brought by Peck against the United Kingdom in the European Court of Human Rights, which demonstrates that CCTV cameras can be used only for specific purposes in pursuit of a legitimate aim, and an authorized person should not process the images captured by these cameras for other objectives that were not justified by the data subject.

On the evening of 20 August 1995, the applicant, Geoffrey Dennis Peck, a United Kingdom national, attempted suicide by cutting his wrists because he suffered from

²⁰⁹ EDPB's Guidelines 3/2019 on the processing of personal data through video devices - Part 3 of 13 - Intenseye. https://www.intenseye.com/resources/edpbs-guidelines-3-2019-on-the-processing-of-personal-data-through-video-devices-part-3-of-13

https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20181130_WP_Artificial-Intelligence.pdf?__blob=publicationFile&v=1

²¹¹ United Kingdom: Biometrics and Surveillance Camera Commissioner speech at the National ANPR Conference 2021. (2022). MENA Report.

depression, Unbeknownst to him, his actions were captured on a CCTV camera installed by Brentwood Borough Council in the city.²¹²

The CCTV footage only showed Mr. Peck holding a knife, prompting the operator to alert the police. Upon their arrival, the police confiscated the knife, provided medical aid to Mr. Peck, and detained him under the Mental Health Act 1983, and after being examined and treated by a doctor, he was released without criminal charges and taken home by the police.²¹³

On October 9, 1995, the Brentwood Borough Council published two photographs from the CCTV cameras in an article titled "Defused: the Partnership between CCTV cameras and the police prevents a potentially dangerous situation." The applicant's face was not obscured, and the article described the incident, mentioning the presence of an individual with a knife, the police's intervention, and the individual being disarmed, questioned, and provided assistance at the police station. ²¹⁴

On October 12, 1995, the "Brentwood Weekly News" featured a photograph of the incident on its front page, accompanying an article discussing the use and advantages of the CCTV surveillance system in public places. Once again, the applicant's face was not masked.²¹⁵

Also, the local newspaper "Yellow Advertiser" published an article on October 13, 1995, titled "Gotcha," along with a photograph of Mr. Peck from the CCTV footage. The article referred to his interception with a knife and the defusing of a potentially dangerous situation, noting that he had been released without charge, and on February 16, 1996, a follow-up article titled "Eyes in the sky triumph" was published, using the same photograph. ²¹⁶ It seems that several people recognized Mr. Peck from the published materials in newspapers.

In summary, this case involves Geoffrey Dennis Peck's suicide attempt captured on a CCTV camera, which led to police intervention under the Mental Health Act. The Brentwood Borough Council and local newspapers subsequently published articles

²¹² https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-687182-694690%22]}

²¹³ Same

²¹⁴ Same

²¹⁵ Same

²¹⁶ Same

and photographs relating to the incident, including Mr. Peck's face, without specifically masking his identity.²¹⁷

The applicant complained about the disclosure of his face to the media of CCTV footage, which resulted in images of himself being published and broadcast widely in the local newspaper "Yellow Advertiser".

He asserted that the CCTV cameras were installed for security purposes, while the Brentwood Borough Council published a photograph of Mr. Peck in an article titled On October 12, 1995, the "Brentwood Weekly News" and also the local newspaper "Yellow Advertiser" published an article on October 13, 1995, titled "Gotcha," along with a photograph of Mr. Peck from the CCTV footage to indicate the benefits of CCTV in the United Kingdom.

Therefore, the use of unmasked Mr. Peck's photos for unlawful and illegitimate purposes, which are not primarily intended, is contrary to Article 8 of the ECHR. It could result in the infringement upon an individual's protected right to privacy.

This case was brought to European Convention on Human Rights. The court held that Geoffrey Dennis Peck, a United Kingdom citizen, made an attempt to end his own life by cutting his wrists due to his depression on August 20, 1995.²¹⁸ Unbeknownst to him, his act was captured on a CCTV camera installed by Brentwood Borough Council. Based on Article 8 of the European Convention on Human Rights, individuals have the right to privacy in their personal and family life, their home, and their correspondence.

According to Article 8 of ECHR, Public authorities can only interfere with this right if it is in accordance with the law and necessary for national security, public safety, economic well-being, disorder or crime prevention, health or morals protection, or the rights and freedoms of others.

The Court observed that following the disclosure of the CCTV footage constituted a serious infringement upon the applicant's right to respect his private life. The court's decision relied on two important grounds:

²¹⁷ Same

²¹⁸ Same

First of all, the Court found that there is no valid reason to release images captured from an applicant's actions by a CCTV camera installed by Brentwood Borough Council. The applicant's footage on "CCTV News" to the public without obtaining his consent or concealing his identity was not legitimate by the Council. CCTV cameras are useful instruments to reduce crimes, both personal and property crimes, and protect public safety in society, this restriction should be necessary, proportionate, and with careful scrutiny, and they are not authorized to impose arbitrarily any restriction on the individual's fundamental rights to privacy and freedom as set forth in international human rights law.

Secondly, the applicant was a victim of a severe breach of his right to privacy, which received extensive coverage in national and local media. Public and private authorities used personal data captured by CCTV surveillance systems, without the person's consent, for other incompatible purposes. Although CCTV cameras were installed to prevent any crimes and anti-social behaviors in society, the newspapers used the claimant's footage to demonstrate the advantages of CCTV surveillance systems in public places in the United Kingdom.

The court observed that following the disclosure of the CCTV footage, the applicant's actions were seen to an extent that far exceeded any exposure to security observation, and The Court asserted that the council has not obtained the applicant's consent or even hide his identity and there were not relevant or sufficient reasons which would justify the direct disclosure of the Geoffrey Dennis Peck's footage by the Brentwood Borough Council to the public in "CCTV News". 220

They concluded that the Council's disclosures of the CCTV materials on "CCTV News" and to "Yellow Advertiser," Anglia Television, and the BBC constituted an excessive and unwarranted violation of the applicant's private life, thus breaching Article 8 of the European Convention on Human Rights. Based on this finding, the Court did not deem it necessary to address the applicant's other complaints under Article 8 separately.

Accordingly, the Court considered that the disclosures by the Council of the CCTV material in "CCTV News" and to the "Yellow Advertiser", Anglia Television, and the

²²⁰ Same

²¹⁹ Same

BBC constituted a disproportionate and unjustified interference with the applicant's life and a violation of Article 8.

As a whole, CCTV cameras capture extensive images of individuals in certain places, including roads, airports, and city centers. The use of CCTV cameras can present some problems. One of the privacy problems with CCTV cameras is that the surveillance practices may be carried out without the individuals' consent for unlawful purposes.

These images should be collected for a clear, specific, and legitimate purpose. An authorized person should only access for the explicit purpose or purposes it was established to address and it should not be used for other purposes that would not have justified its establishment in the first place. The misuse of an individual's confidential images for an unjustifiable is considered an intrusion into the right to privacy.

(4) Lack of transparency and accountability

The vast number of CCTV cameras in many cities in the United Kingdom has led to numerous problems with regard to people's fundamental rights. One of the challenges which is related to the use of closed-circuit televisions and their impact on individuals' privacy rights is the lack of transparency or accountability regarding access to personal information.

many Critics argue that there has been increasing concern that there is not sufficient information on how the images are captured by video surveillance, how it is processed, and ultimately who can access an individual's personal images and footage, so people are not aware of the CCTV cameras process.

All organizations or individuals that use Al-powered surveillance systems should provide people with information about how the data is collected, processed, and used for different purposes. one of the important measures to prevent the infringement upon the right to privacy is that the use of CCTV cameras should be carried out in a transparent manner.

As well, Professor Webster, Chair of Public Policy and Management at the Stirling Management School, highlighted that the purpose, design, and usage of the surveillance systems should be transparent and stated: "New forms of surveillance, such as automated facial recognition, Smart CCTV, and body-worn video cameras, often have data

processes that are mostly invisible to people being surveyed. Therefore, it's crucial that there's also guidance around the best practice and ethical use of all manner of surveillance cameras."²²¹

In the United Kingdom, many people are not conscious of the operation of surveillance camera systems. As indicated in recent research, approximately 80% of people in the United Kingdom believe that they do not receive enough information on closed-circuit television (CCTV) design, processes, and objects, and more than a third think if they had more information more about the impact of CCTV cameras on society for example how it helps to reduce crimes and anti-social behaviors in the community, public support for public space surveillance would increase.²²²

In the United Kingdom, the National Surveillance Camera Strategy for England and Wales was presented in March 2017, which encompasses more than 600 public authorities, including state bodies, police, armed forces, and a larger number of local organizations, governs the operation of public space surveillance cameras, including CCTV cameras enable people to understand the surveillance camera use, sets out the principles, and determines how the competent authorities implement cameras.²²³

Therefore, there is a stronger correlation between institutional trust and positive attitudes toward surveillance systems comprising CCTV cameras. It may seem reasonable to assume that if people are informed of CCTV use in a transparent manner in public institutions, including governments and political institutions, people would have a positive opinion of the performance of closed circuit television (CCTV) cameras in the country in which they live.²²⁴

Transparency in the operation of CCTV cameras is a fundamental component of a performance-based approach to trust. States might inform people of some CCTV activities and provide them with information with regard to the operation of CCTV

²²¹ Ensuring transparency and responsibility in surveillance camera use | Research | University of Stirling. https://www.stir.ac.uk/research/research-spotlights/ensuring-transparency-and-responsibility-in-surveillance-camera-use/

²²²What we can learn from public attitudes towards surveillance, CCTV in the UK, White Paper Available at: https://synecticsglobal.com/Content/Downloads/Synectics_PublicSpace-Whitepaper.pdf

https://www.stir.ac.uk/research/research-spotlights/ensuring-transparency-and-responsibility-in-surveillance-camera-use/

²²⁴ Björklund, F. (2021) Trust and surveillance: An odd couple or a perfect pair? In: Lora Anne Viola; Paweł Laidler (ed.), Trust and Transparency in an Age of Surveillance (pp. 183-200). London: Routledge Routledge Studies in Surveillance https://doi.org/10.4324/9781003120827-14

cameras; however, sometimes political entities prescribe a certain amount of transparency in some circumstances, such as in requiring signs indicating camera monitoring and it should be noted that surveillance is based on the condition that everything cannot be made transparent.²²⁵

The ethical guidelines published by the EU Commission's High-Level Expert Group on AI (AI HLEG) in 2019 state, "The data, system, and AI business models should be transparent. Traceability mechanisms can help to achieve this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans must be aware that they are interacting with an AI system and must be informed of its capabilities and limitations."²²⁶

According to article 2.6 (3) of the surveillance camera code of practice in the United Kingdom, "There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints."²²⁷

In addition, the surveillance camera code of practice states 3.3.1: "People in a public place should normally be made aware whenever they are being monitored by a surveillance camera system, who is undertaking the activity and the purpose for which that information is to be used."²²⁸

According to British law, in the age of surveillance technologies, surveillance cameras should be implemented transparently and people monitored by closed-circuit televisions should be informed about the purpose, use, and operation of surveillance technologies.

Also, we should consider that there is a crucial relationship between the concept of transparency and an individual's inherent right to autonomy. The concept of Autonomy means each person has the fundamental right to make independent decisions with regard to all his/her aspects of life based on his/her own values and interests.²²⁹ The Universal Declaration on Human Rights' preamble recognized

²²⁵ Björklund, F. (2021) Trust and surveillance: An odd couple or a perfect pair? In: Lora Anne Viola; Paweł Laidler (ed.), Trust and Transparency in an Age of Surveillance (pp. 183-200). London: Routledge Routledge Studies in Surveillance https://doi.org/10.4324/9781003120827-14

PRESS RELEASE: EU Ethics Guidelines for Trustworthy AI presented at the EU Digital Day – ALLAI. https://allai.nl/press-release-eu-ethics-guidelines-for-trustworthy-ai-presented-at-the-eu-digital-day/

²²⁷ Surveillance Camera Code of Practice – 12 Principles | The Data Compliant Blog. https://datacompliantblog.com/2014/10/16/surveillance-camera-code-of-practice-12-principles/

²²⁸ Why Tech And Policing Don't Always Mix. (2017, October 1). PC Pro, 276, 127.

Becker, M. Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. *Ethics Inf Technol* **21**, 307–317 (2019). https://doi.org/10.1007/s10676-019-09508-z

people's inherent autonomy, and Article 1 of this declaration asserted, "All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood."²³⁰

According to General Data Protection Regulation (GDPR), each person or organization should specifically inform the recipient about how Al-powered surveillance systems make decisions and process data in a transparent manner to respect the user's autonomy.²³¹

Although all surveillance systems should be transparent, we may face some challenges. "It can be challenging to satisfy the transparency principle in AI-powered decision-making systems. One reason is that the details behind an algorithm's functioning are often considered proprietary information and so are closely guarded by their owners. Another reason is that, depending on the AI system, the algorithms might be so complex that even their creators do not know exactly how they work in practice." ²³²

The other important principle is that any person or organization who interferes with an individual's privacy rights should be responsible for its performance. The British government should assess CCTV system adherence to the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Data Protection Act 1998, and the surveillance camera code of practice, evaluate the CCTV systems' effectiveness, compliance to the stated specific purpose, enforce penalties for infringement system, apply to any law enforcement use of privately and protect people against any breach against the right to privacy.²³³

Peter Allards states, "As a consequence, it is for the police and local governments to ensure that they can provide a convincing and lawful justification for the use of cameras in public spaces and that they develop systems of control and accountability that seek to minimize the negative effects of surveillance on individual privacy." ²³⁴

https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20181130_WP_Artificial-Intelligence.pdf?__blob=publicationFile&v=1

²³⁰ BoonJot Hinting Preview | สำนักอักขระฟอนต์อยู่นี่. https://fontuni.com/boonjot/hinting.html

²³¹ Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, *6*(1). https://doi.org/10.1177/2053951719860542

²³² Available at:

²³³ CCTV: Developing Privacy Best Practices, Report on the DHS privacy office public workshop, December 2007.

Available at : https://www.dhs.gov/sites/default/files/publications/privacy_rpt_cctv_2007.pdf

²³⁴ https://commons.allard.ubc.ca/cgi/viewcontent.cgi?article=1151&context=fac_pubs

Each state should create a set of rules and guidelines to compensate and address any infringements which result from the use of AI surveillance systems, specifically CCTV cameras, to ensure that each individual's privacy right is preserved.²³⁵

As stated in article 4(7) of the General Data Protection Regulation (GDPR): "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." ²³⁶

The controller, individual, or group should be responsible for any unlawful or illegal acts in CCTV performance, and they are not authorized to infringe upon people's right to privacy arbitrarily.

In this part, we look into one of the case laws in the United Kingdom, which shows how well transparency is important in using CCTV cameras throughout the country. This case is related to the systematic use of CCTV cameras in Cumbria, a ceremonial county in North West England.

Case Study: Transparency in the use of CCTV cameras in Cumbria (Cooperation between the Police and Crime Commissioner (PCC), local authorities, and the police force)²³⁷

The effective use of CCTV systems has become increasingly vital in modern crime prevention and resolution strategies. In Cumbria, a city which is located in the northwest of England, the Police and Crime Commissioner (PCC), local authorities, and the police force initiated a successful collaboration to establish a new and comprehensive CCTV surveillance system. This case explores this joint effort's process, benefits, and outcomes. As well they emphasize the importance of consultation, the development of an integrated system, and the transparent sharing of statistics with the community.

Prioritizing community involvement and support is crucial when implementing any surveillance system, particularly one as prominent as CCTV. The stakeholders

²³⁵ Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160

²³⁶ Controller Definition: 9k Samples | Law Insider. https://www.lawinsider.com/dictionary/controller

https://www.gov.uk/government/case-studies/joint-working-cumbria-police-and-crime-commissioner-police-and-councils-combine-cctv

involved in Cumbria's CCTV project diligently consulted relevant parties before its installation, and many stakeholders, including private and public organizations like residents, police, and investigatory authorities, agreed that the use of CCTV cameras can play a significant role in crime prevention.²³⁸

To create an efficient and effective CCTV system for Cumbria, the PCC, local authorities, and the police force joined forces and enlisted the expertise of a consultant, and this collaborative effort allowed for a comprehensive evaluation of the county's requirements, taking into account factors such as geographic layout, crime hotspots, and community feedback.²³⁹ The resulting system covers six towns and operates from a centralized control room located at the police headquarters.

The integrated CCTV scheme in Cumbria goes beyond mere reactive surveillance. It also incorporates proactive measures to enhance crime prevention. The advanced technology and real-time monitoring capabilities helped law enforcement personnel to detect and respond to incidents immediately, deterring criminal activity and enhancing public safety. ²⁴⁰

Transparency and accountability are fundamental elements for building trust and ensuring the legitimacy of any surveillance program. In line with this principle, the stakeholders in Cumbria's CCTV project have committed to transparently demonstrating the system's efficacy to the community. Monthly, quarterly, and annual statistics are published, providing the public with tangible evidence of how CCTV has contributed to their protection.

The publication of statistical data serves multiple purposes. First, it allows community members to witness the tangible impact of the CCTV system, fostering a sense of security and confidence in the authorities' efforts, Second, it enables ongoing evaluation and assessment of the system's effectiveness, highlighting areas of success and potential improvement.²⁴¹ Therefore, all stakeholders, including police, investigatory authorities, and inhabitants, would be able to be informed of the CCTV surveillance system and its effects.

The collaborative approach taken by the Police and Crime Commissioner, police force, and local authorities in Cumbria has successfully developed and

²³⁸ Same

²³⁹ Same

²⁴⁰ Same

²⁴¹ Same

implemented an advanced CCTV system.²⁴² Through consultation, the stakeholders ensured community buy-in and addressed concerns from the outset. The integrated scheme, covering six towns and operating from a centralized control room, combines reactive and proactive measures to enhance crime prevention and resolution. Furthermore, the commitment to transparently sharing monthly, quarterly, and annual statistics reinforces the trust between the authorities and the community while allowing for ongoing evaluation and improvement, and the Cumbria CCTV case study serves as a model for effective collaboration and stakeholder engagement in the development of comprehensive surveillance systems aimed at enhancing public safety.²⁴³

Therefore, the scope and jurisdiction of all kinds of surveillance systems which monitor individuals should be precise. Many autocratic regimes have been among the worst offenders, and we need an account of when, why, and how CCTV cameras are being used.²⁴⁴

To sum up, According to the United Kingdom Law, the use of CCTV cameras should be in a transparent manner, and all people have the legal right to be aware of the CCTV surveillance system's process. In Cumbria, the Police and Crime Commissioner (PCC), local authorities, and the police force have very successfully cooperation in developing a comprehensive CCTV surveillance system which explores the process, benefits, and outcomes of this joint effort, which highlighted the importance of transparency over the use of video surveillance equipment.

(5) lack of necessity and proportionality

The value of privacy rights might be lost with any benefits from designing and deploying innovative surveillance capabilities. A balanced analysis examines what privacy rights must be diminished or reduced to balance the perceived benefits of adopting a specific surveillance analytics solution. The balance metaphor does not imply that attaining the benefits from innovation in surveillance analytics must lead to a decrease in privacy or a loss of privacy rights.²⁴⁵

²⁴² Same

²⁴³ Same

Richards, N. M. (2013). THE DANGERS OF SURVEILLANCE. *Harvard Law Review*, *126*(7), 1934–1965. http://www.jstor.org/stable/23415062

²⁴⁵ Daniel J. Power, Ciara Heavin & Yvonne O'Connor (2021) Balancing privacy rights and surveillance analytics: a decision process guide, Journal of Business Analytics, 4:2, 155-170, DOI: 10.1080/2573234X.2021.1920856

The use of CCTV cameras should be proportionate and necessary to restrict the right to privacy. In fact, the British government should assess two fundamental principles when they intend to install CCTV surveillance systems.

One of the fundamental principles related to the use of surveillance systems, including CCTV cameras, is the principle of necessity. A crucial approach to mitigate privacy violations is that the United Kingdom could restrict and limit the data collected by AI surveillance systems to only what is necessary and relevant for the intended surveillance purpose to reduce the risk of infringement on individual privacy rights.

As stated in "Assessing the Necessity of Measures that Limit the fundamental right to the Protection of personal data: A Toolkit" published by the European Union on 11 April 2017, the principle of necessity refers to "the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal." 247

Article 5(1)(c) of GDPR states that the data should be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')."²⁴⁸

Minimization of data is of utmost importance for various entities, including public and private institutions and individuals. It becomes particularly crucial in the case of electronic data and records, which are at a higher risk of misuse compared to their paper counterparts, and restriction of the volume of permanently or long-term archived material can preserve confidential information, reduce records also helps to diminish the quantity of archived material and the privacy and protect personal data of individuals at risk.²⁴⁹ Data minimization is a critical measure that promotes the protection of individual privacy and mitigates the potential for data misuse.

²⁴⁶ Comments on the Srikrishna Committee Report and the Draft Data Protection Bill 2018 – III - Tech Law Forum @ NALSAR. https://techlawforum.nalsar.ac.in/recent-news-comments-on-the-srikrishna-committee-report-and-the-draft-data-protection-bill-2018-iii/

²⁴⁷ Assessing the necessity of measure that limit the fundamental right to the protection of personal data: A Toolkit, European Data Protection supervisor, 11 April 2017

Available at: https://edps.europa.eu/sites/edp/files/publication/17-04-11 necessity toolkit en 1.pdf

²⁴⁸ Privacy policy |. http://astersc.eu/en/privacy-policy/

²⁴⁹ Čtvrtník, Mikuláš. (2023). Data Minimisation—Storage Limitation—Archiving. 10.1007/978-3-031-18667-7_8.

As indicated in the report published by Louise Smith: "The state and public authorities are permitted to interfere with an individual's Article 8 right to privacy if the interference has an obvious legal justification. Amongst other reasons, this could be because interference is necessary to protect national security or for the prevention of crime. In addition to having a clear legal justification, the amount of interference with the right must be proportionate to the end result achieved and only go as far as is required to achieve that result."

Moreover, the surveillance camera code of practice: 1.4) "The government is fully supportive of the use of overt surveillance cameras in a public place whenever that use is: in pursuit of a legitimate aim; necessary to meet a pressing need; proportionate; effective, and; compliant with any relevant legal obligations."²⁵¹

In addition, the installation of CCTV cameras throughout the United Kingdom should be compatible with the purpose. The use of CCTV cameras is proportionate to the intended purpose. According to Macnish, KNJ, The principle of proportionality suggests that the harms of a particular act should not outweigh its benefits, so if the harms derived from this surveillance act outweigh its potential benefits, then that act is likely to be considered disproportionate.²⁵² The use of CCTV cameras can limit an individual's personal affairs, movements, and communication. The benefits of the installation of these surveillance systems, including national security, safety, and crime prevention, should outweigh its potential harm and justify the use of CCTV cameras in the United Kingdom.

Using CCTV technology should be proportionate to the intended purpose. For instance, the installation of facial recognition technology for investigating crimes such as theft, murder, terrorist activities, and other serious crimes is likely to be necessary and proportional to the severity of the crime and the potential harm to society, while this technology might not be proportionate for petty crimes, and it could raise concerns about fairness and privacy.²⁵³

According to the Surveillance camera code of Practice (2.3): "An individual can expect to be the subject of surveillance in a public place as CCTV, for example, is a familiar feature in places that the

²⁵⁰ Available at: https://www.abouthumanrights.co.uk/human-rights-cctv.html

²⁵¹ Councils urged to be open about CCTV data | UKAuthority. https://www.ukauthority.com/articles/councils-urged-to-be-open-about-cctv-data/

²⁵² Macnish, KNJ orcid.org/0000-0003-4510-3049 (2015) An Eye for an Eye: Proportionality and Surveillance. Ethical Theory and Moral Practice, 18 (3). pp. 529-548. ISSN 1386-2820 https://doi.org/10.1007/s10677-014-9537-5

²⁵³ Smith, M., Miller, S. (2021). Facial Recognition and Privacy Rights. In: Biometric Identification, Law and Ethics. Springer Briefs in Ethics. Springer, Cham. https://doi.org/10.1007/978-3-030-90256-8_2

public frequent. An individual can, however, rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place."

The Surveillance camera code of practice (4.10.1) mentions that: "Good practice dictates that a system operator should review the continued use of a surveillance camera system on a regular basis, at least annually, to ensure it remains necessary, proportionate and effective in meeting its stated purpose for deployment." ²⁵⁴

The issue of disproportionate surveillance extends encompasses the entire United Kingdom, as highlighted by the pressure group Big Brother Watch in 2011.²⁵⁵ According to their argument, Britain stands out for its widespread and persistent use of CCTV cameras, which intrude upon the privacy of law-abiding individuals without necessarily yielding a commensurate enhancement in public safety. This perspective raises concerns about the balance between security measures and individual privacy rights.

CCTV surveillance in the UK might be used for a reason that is neither appropriate nor essential. Cameras are now prevalent in many facets of daily life, including public venues, workplaces, and even private homes, because people's movements and activities are constantly tracked, this prevalence raises concerns about how it will affect their right to privacy.

Big Brother Watch suggests that the extensive use of CCTV does not necessarily result in an equivalent improvement in public safety. Although the goal of installation surveillance systems is frequently to detect and deter criminal activity, there is a dispute over how well these measures actually succeed to achieve these objectives. Critics argue that the disproportionate intrusion into people's privacy may not be justifiable in relation to the benefits of crime prevention and detection.

CCTV cameras installed across various aspects of life is seen as an intrusion into the privacy of law-abiding individuals. The statement questions the effectiveness of such surveillance in improving public safety and underscores the importance of considering alternative approaches that uphold both security and privacy rights.

²⁵⁵ Macnish, KNJ orcid.org/0000-0003-4510-3049 (2015) An Eye for an Eye: Proportionality and Surveillance. Ethical Theory and Moral Practice, 18 (3). pp. 529-548. ISSN 1386-2820 https://doi.org/10.1007/s10677-014-9537-5

²⁵⁴ CCTV Policy | CCTV Policy | Reigate and Banstead. https://www.reigate-banstead.gov.uk/info/20209/access_to_information/1405/cctv_policy

This ongoing debate prompts a critical examination of the role and impact of surveillance in contemporary society.

In this part, we evaluate one of the case laws in the United Kingdom, which Fairhurst brought against Woodwar. It demonstrates the significance of the principle of necessity and proportionality in the prevalence of CCTV cameras.

Case Study: Fairhurst v Woodwar²⁵⁶

The case was brought before the court from the claim of Fairhurst against Woodwar. The legal dispute between Mrs. Fairhurst and Mr. Woodward centers around the latter's use of security cameras on and around his property in Thame.

Mr. Woodward has placed a warning sign in his front window. This sign warns visitors to the operation of concealed CCTV cameras on the premises. Mrs. Fairhurst, the complainant, has decided to begin a complaint against Mr. Woodward, the defendant, regarding his use of security cameras at and around his property. As both parties reside in close proximity, the issue at hand revolves around the extent and legality of Mr. Woodward's surveillance measures.

Mrs. Fairhurst has initiated legal proceedings. She alleged various violations, including breaches of the UK Data Protection Act 2018 (DPA 2018). Among her claims, she highlights concerns regarding the potential infringements upon her privacy rights as a result of the surveillance activities carried out by Mr. Woodward. The case raises questions about the application and compliance with the provisions outlined in the DPA 2018, shaping the foundation for the ongoing legal proceedings between the two neighbors.

In a legal dispute between neighbors, Mrs. Fairhurst, the complainant, has brought a complaint against Mr. Woodward, the defendant, regarding his use of closed-circuit cameras at and around his property, and the Defendant put a sign in his front window stating, "WARNING Concealed CCTV cameras operate on these premises."²⁵⁷

 $Available\ at: https://www.judiciary.uk/wp-content/uploads/2022/07/Fairhurst-v-Woodard-Judgment-1.pdf\ ^{257}\ Same$

²⁵⁶ Fairhurst v Woodard Judgment

As both parties reside in close proximity, the issue at hand revolves around the extent and legality of Mr. Woodward's surveillance measures.

The primary issue at hand is the potential infringement upon Mrs. Fairhurst's privacy rights as a result of Mr. Woodward's surveillance measures. Mrs. Fairhurst asserts that the presence and use of the security cameras violate her privacy, constituting harassment, nuisance, and breaches of the UK Data Protection Act 2018 (DPA 2018).²⁵⁸

The Data Protection Act 2018 serves as the legal framework aims at the processing and protection of personal data in the United Kingdom. The Act incorporates the principles and provisions outlined in the General Data Protection Regulation (GDPR), emphasizing individuals' rights to privacy and the lawful handling of personal data.

Mrs. Fairhurst alleges that Mr. Woodward's surveillance activities may constitute a breach of the DPA 2018. She argues that her privacy rights have been compromised by the continuous monitoring and recording of her activities, potentially extending beyond the boundaries of Mr. Woodward's property, and in this context, it becomes crucial to assess whether Mr. Woodward's use of the security cameras aligns with the principles of necessity, proportionality, transparency, and data security as stipulated by the DPA 2018.²⁵⁹

The presence of the warning sign in Mr. Woodward's front window indicates his intention to inform individuals of the existence of concealed CCTV cameras. However, the effectiveness of such a sign in providing explicit consent and ensuring transparency regarding surveillance activities is subject to evaluation. It is essential to consider whether Mrs. Fairhurst was adequately informed about the surveillance measures and their potential impact on her privacy before reaching a conclusion on the lawfulness of Mr. Woodward's actions.

Furthermore, the court must examine the specific circumstances surrounding the case, including the location and positioning of the cameras, the extent of their surveillance range, and the purpose for which the recorded data is used. These factors contribute to determining whether the surveillance measures adopted by

-

²⁵⁸ Same

²⁵⁹ Same

Mr. Woodward are necessary and proportionate to achieve the intended objectives of security and crime prevention.

Ultimately, the outcome of this legal dispute will depend on the court's assessment of the evidence presented and the application of the relevant provisions within the Data Protection Act 2018. The case underscores the importance of striking a balance between the legitimate interests of security and the protection of individual's privacy rights. As technology continues to advance and surveillance practices become more prevalent, it is crucial for legal frameworks and courts to adapt and ensure that privacy rights are respected and upheld in disputes such as these.

This judgment arises from a two-day trial involving a claim brought by Dr. Fairhurst against Mr. Woodard, his neighbor, alleging harassment, nuisance, and breach of the Data Protection Act 2018.

The court held that, in relation to personal data collected by CCTV cameras, the use of CCTV cameras was not "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed." ²⁶⁰

Article 5(1) of GDPR: "Personal data shall be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')"

The defendant submitted that "all of his data collection and processing was necessary for the purposes of crime prevention at his property. Thus it was left to the Court to determine the appropriate balance between, on the one hand, the Claimant's interests in protecting her personal data and the Defendant's interest in securing his home on the other." ²⁶¹

The Judge ruled that "the Defendant had misled the Claimant over the functionality of the cameras and that this amounted to a breach of the requirement under Article 5(1)(b) the GDPR that data only be collected for 'specified, explicit and legitimate purposes'." ²⁶²

In addition, although the use of CCTV cameras can be effective, controllers should first assess its impact on fundamental rights and freedoms, particularly the right to

²⁶⁰ 5. Principles relating to personal data processing - easyGDPR. https://easygdpr.eu/en/gdpr-article/5/

²⁶¹ Case Law: Fairhurst v Woodard, Neighbour CCTV harassment and data protection claim succeeds – Percy Preston – Inforrm's Blog. https://inforrm.org/2021/10/20/case-law-fairhurst-v-woodard-neighbour-cctv-harassment-and-data-protection-claim-succeeds-percy-preston/

²⁶²https://inforrm.org/2021/10/20/case-law-fairhurst-v-woodard-neighbour-cctv-harassment-and-data-protection-claim-succeeds-percy-preston/

privacy, and consider less intrusive means to achieve their legitimate purpose of processing."²⁶³

Therefore, all people and organizations who intend to install CCTV cameras for crime prevention should consider two fundamental principles. First of all, they should consider whether the use of CCTV cameras in that place is necessary and proportionate, and secondly, they should assess if there are other means to reduce criminal behaviors in society which are less intrusive to the right to privacy.²⁶⁴

6) The leakage of Confidential Information

These days, it is possible to monitor every activity of individuals in society. Much of this data about the personal life of individuals, including financial information, health information, Biometric data (e.g. fingerprints or facial recognition data), and Internet protocol addresses, is now being uploaded to cloud computers.²⁶⁵

CCTV cameras can access new information about specific people that a human operator could not have obtained, including facial expression analysis, object detection, behavior identification, and movement analysis, which should be properly controlled.²⁶⁶

All people should own fundamental rights and freedoms. It includes that they would have the freedom to choose their behaviors, thoughts, feelings, and secrets and determine who can access what parts of this domain and how and when those parts will be published.²⁶⁷

One of the challenges of CCTV cameras with privacy rights is that CCTV cameras situated in public spaces are probably subject to cyber-attacks. It means

²⁶³ www.edpb.europa.eu edpb guidelines 201903 videosurveillance.pdf (europa.eu)

²⁶⁴Privacy Commissioner for Personal Data, Hong Kong, July 2010.

Available at: https://www.pcpd.org.hk/english/resources centre/publications/files/GN CCTV Drones e.pdf

²⁶⁵ Bartneck, Christoph & Lütge, Christoph & Wagner, Alan & Welsh, Sean. (2021). Privacy Issues of Al. 10.1007/978-3-030-51110-4 8.

²⁶⁶ Koch H., Matzner T. & Krumm, J., "Privacy Enhancing of Smart CCTV and its Ethical and Legal Problems", in European Journal of Law and Technology, Vol 4., No. 2., 2013.

²⁶⁷ EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG, Moyo Sheperd, February 2019 Available at: https://core.ac.uk/download/pdf/286383944.pdf

that unauthorized persons would be able to access an individual's private information and intrude on people's private lives.²⁶⁸

CCTV was once primarily used for police surveillance in the 1980s, however, as more advanced technology has emerged, individuals have begun to use surveillance systems in the streets, stores, shops, and private properties to review people's movements. Many Individuals or groups decide to install surveillance cameras in public areas, medical facilities, and educational institutions to enhance public safety; nevertheless, the personal footage obtained through CCTV cameras can be disclosed to others without the individual's consent. 270

Therefore, personal data can be used to predict users' interests and preferences accurately, but if not properly managed and controlled, some companies may use the collected data to track users' behavior without their consent, which brings about infringement upon users' right to privacy. ²⁷¹

All states have legal duty The British government should implement all appropriate measures, comprising system security, data security, and all measures in each process, such as image collection, aggregation, distribution, and access, to preserve footage captured by CCTV cameras and protect them from any cyber-attacks.²⁷²

The crucial concern is that even though AI surveillance systems may pose a threat to the privacy of data, some argue that we can create AI-driven privacy tools and enhance existing technologies to safeguard user privacy and assist organizations to restrict or monitor access to an individual's data and prevent any unauthorized use of data.²⁷³

CCTV systems will be able to identify criminal activity carried out using computers and other forms of digital networks that numerous state or non-state actors could use, and these technologies will defend cyber networks with extremely high

²⁶⁸ Turtiainen, Hannu & Costin, Andrei & Hämäläinen, Timo. (2022). CCTV-Exposure: System for measuring user's privacy exposure to CCTV cameras.

²⁶⁹ Yeganegi, Kamran & Moradi, Dawood & Obaid, Ahmed. (2020). Create a wealth of security CCTV cameras. Journal of Physics: Conference Series. 1530. 012110. 10.1088/1742-6596/1530/1/012110.

²⁷⁰ https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=12225&context=theses

²⁷¹ Gao, Zhang. (2019). Research on Network Information Security and Privacy Protection in the Age of Big Data. Journal of Physics: Conference Series. 1237. 022092. 10.1088/1742-6596/1237/2/022092.

²⁷³ Artificial Intelligence and Data Protection: Observations on a Growing Conflict Fred H. Cate & Rachel Dockery

degrees of autonomy, speed, and complexity that well beyond human comprehension in order to protect crucial and sensitive information.²⁷⁴

As Amnesty International, an international organization, states, "Encryption" is one of the common matters of human rights: "While digital technologies have created new opportunities for communication and expression, they have also enabled the production, dissemination, and storage of exponentially greater amounts of private data pertaining to individuals' movements, beliefs, political preferences, sexual orientation, health, and financial flows, among others." ²⁷⁵

Video surveillance systems can record all people's activities, behaviors, and movements. The CCTV cameras can even collect personal information about all individuals. Article 4(1) of General Data Protection Regulation (GDPR): "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."²⁷⁶

Therefore, states should introduce new rules and regulations to establish accountability and jurisdiction in this constantly evolving landscape. ²⁷⁷Article 51(1) of GDPR: "Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority')."²⁷⁸

state and non-state organizations in the United Kingdom should consider other means to reduce criminal behaviors in society which are less intrusive to the right to privacy. use CCTV surveillance systems to record images of people's activities,

²⁷⁴ Pauwels, E. (2020). Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention: Opportunities and Challenges for the International Community. Global Center on Cooperative Security. http://www.jstor.org/stable/resrep27551

²⁷⁵Encryption: A Matter of Human Rights, Amnesty International, March 2016 Index: POL 40/3682/2016 Available at:

https://www.amnesty.nl/content/uploads/2016/03/160322_encryption_-_a_matter_of_human_rights_-_def.pdf ²⁷⁶ Privacy Statement – Open Future. https://openfuture.eu/privacy/

²⁷⁷ Tarafder, A. (2015). SURVEILLANCE, PRIVACY AND TECHNOLOGY: A COMPARATIVE CRITIQUE OF THE LAWS OF USA AND INDIA. *Journal of the Indian Law Institute*, *57*(4), 550–578. http://www.jstor.org/stable/44782800

²⁷⁸ Data Protection Authority | Data Privacy Glossary | Protecto. https://www.protecto.ai/data-privacy-glossary/data-protection-authority

they should attempt to implement data-hiding measures to preserve the identity of the individuals being recorded in order to protect their privacy rights.²⁷⁹

One of the crucial measures to protect people's personal data is Encryption. As Temitope Olufohunsi stated, "Encryption is the process of converting information or a message which is referred to as plaintext, into a difficult unreadable form called ciphertext through using an encryption algorithm (Bassel)."²⁸⁰

Symmetric encryption is a technique that uses a single key to both encrypt and decrypt data, and the key is shared between the sender and the receiver; on the other hand, asymmetric encryption uses two different keys, a public key and a private key, and the public key is used to encrypt data, while the private key is used to decrypt it.²⁸¹

According to the UN report: "in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization, and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association," 282

Personal data is stored for more than the authorized time or might be leaked outside that domain, or the data collected without consent or without consent for that purpose.²⁸³

When using video surveillance systems, governments and other organizations should ensure that everyone's private information and communication are protected because many individuals may believe that the personal information collected by the cameras could be misused.

There are several types of techniques to hide privacy-sensitive areas, "firstly, only hides the identity ad also, in some cases also, the behavior, Another type of approach is to reduce the level of detail of privacy-sensitive areas, with the help of blurring or pixelation, leaving the subject unidentifiable yet the behavior remains recognizable. Thirdly, called abstraction, is to

²⁷⁹ Rajpoot, Q.M., Jensen, C.D. (2014). Security and Privacy in Video Surveillance: Requirements and Challenges. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T. (eds) ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology, vol 428. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-55415-5_14

²⁸⁰Olufohunsi, Temitope. (2019). DATA ENCRYPTION Olufohunsi, T.

²⁸¹ Olufohunsi, Temitope. (2019). DATA ENCRYPTION Olufohunsi, T.

²⁸²https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F48%2F4&Language=E&DeviceType=Deskt op&LangRequested=False

²⁸³ Cammozzo, Alberto. (2011). Face Recognition and Privacy enhancing techniques. Page 6

remove the sensitive regions and replace them with dummy objects such as silhouettes or skeletons. Forth, yet another technique proposed in literature called scrambling is to encrypt the sensitive regions with a key allowing the area to be decrypted only by authorized personnel possessing the key."²⁸⁴

Therefore, one of the biggest issues we currently face is the high danger of cyberattacks to access the data; thus, it is more important than ever to strengthen systems and processes to make data more safe and secure against threats by both state-sponsored and non-state actors.²⁸⁵

The other measure to protect the personal data of individuals from any privacy violation is anonymization. Today, the progress in information and communication technologies (ICT) has enabled numerous organizations to collect vast amounts of valuable data through virtual platforms.²⁸⁶

Anonymization refers to the process of removing personally identifiable information (PII) from data collected through a large surveillance network from hundreds of cameras, sensors, and other equipment so that the individuals in the published data cannot be identified.²⁸⁷

Anonymization refers to the technique of removing personally identifiable information (PII) in data gathered by an extensive surveillance network consisting of multiple cameras, sensors, and other devices to ensure that an individual involved in the released data remains unidentifiable.²⁸⁸

In this part, we examine one of the cases with regard to the CCTV network breach in London.

Case Study: The London CCTV Network Breach

²⁸⁴ Rajpoot, Q.M., Jensen, C.D. (2014). Security and Privacy in Video Surveillance: Requirements and Challenges. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T. (eds) ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology, vol 428. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-55415-5 14 page 177 or 9

²⁸⁵ Tripathi, Keyur and Mubarak, Usama, Protecting Privacy in the Era of Artificial Intelligence (March 24, 2020). Available at SSRN: https://ssrn.com/abstract=3560047 or http://dx.doi.org/10.2139/ssrn.3560047

²⁸⁶ Majeed, Abdul & Lee, Sungchang. (2020). Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3045700.

²⁸⁷ Data Anonymization - Task. http://lod.iula.upf.edu/resources/DataAnonymization

²⁸⁸ Domingo-Ferrer, Josep & Sánchez, David & Soria-Comas, Jordi. (2016). Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections. 10.2200/S00690ED1V01Y201512SPT015.

During the last few years, significant CCTV hacks occurred in London, capturing widespread attention and raising concerns about the vulnerabilities of surveillance systems. A group of skilled hackers infiltrated the network of a major CCTV service provider responsible for maintaining and monitoring a vast number of cameras installed across the city.

The hackers managed to exploit weaknesses in the provider's security infrastructure, allowing them unauthorized access to the CCTV cameras and their associated control systems. This breach gave them the ability to manipulate and manipulate the cameras' functionality, including disabling them, altering footage, or redirecting the feeds to different locations.

As a result of this breach, several incidents of privacy invasion and unauthorized surveillance were reported. In some instances, the hacker accessed live camera feeds from public spaces, private establishments, and even residential areas. This raised significant concerns among the affected individuals and the general public about the potential misuse of personal information and violation of privacy.

The incidents prompted a joint investigation by law enforcement agencies, cybersecurity experts, and the Information Commissioner's Office (ICO). The investigation aimed to determine the extent of the breach, identify the perpetrators, and assess the potential impacts on individuals' privacy rights and security.

In response to the breach, the affected CCTV service provider immediately rectified the vulnerabilities and strengthened their security measures. This included conducting thorough system audits, implementing robust encryption protocols, and enhancing access controls to prevent unauthorized entry.

The incidents also led to a broader discussion about the security and privacy concerns of using CCTV systems in public and private spaces. Legal experts reviewed existing regulations and guidelines governing the use of surveillance technologies to ensure they adequately address emerging threats and protect individuals' rights.

_

 $https://www.washingtonpost.com/local/public-safety/2-arrested-in-uk-in-hacking-of-dc-police-closed-circuit-camera-network/2017/02/02/24c2c0ea-e969-11e6-80c2-30e57e57e05d_story.html$

Technological advancements could widely improve our lives; however, there is a risk associated with sharing personal information, as once people's personal information has been shared, it may become impossible to retain control over our data.²⁹⁰

Conclusion

Consequently, although CCTV surveillance systems have the capacity to enhance to prevent crimes and enhance security and public safety in society, they will also potentially raise several privacy issues.

The United Kingdom should employ strategies and approaches to outline a conceptual framework to develop a constructive approach to improve the effectiveness of future policy changes to contribute to the existing literature on the impacts of the AI surveillance system on the right to privacy and provide valuable insights for policy-makers and stakeholders.

The application of CCTV cameras can threaten and violate individuals' right to privacy. because cameras capture an individual's personal information, and they may be stored and even used for other purposes. Therefore, we need to establish clear and explicit laws and regulations to lessen the risks of abuse and misuse of personal data.²⁹¹

As stated in the report published by Human Rights Watch, the British government should inform people of the process of smart surveillance systems, including CCTV cameras and their "adherence to the law and democratic values," it needs to give a clear explanation about these claims and about how the law is being applied.²⁹²

As Amnesty International mentioned: "The current EU export regulation framework fails to adequately regulate the human rights impact of a wide range of existing and emerging digital surveillance technologies. Historically, European export regulation focused on the regulation of technologies that could be used in a military context. This singular focus is no longer legitimate since many technologies nowadays are " not specifically designed for military use but nonetheless used for repression" and other human rights violations. Digital surveillance

²⁹⁰ Pelteret, Marc & Ophoff, Jacques. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. Informing Science The International Journal of an Emerging Transdiscipline. 19. 277-301. 10.28945/3573.

²⁹¹ Lewis, J. A., & Crumpler, W. (2021). *Questions about Facial Recognition*. Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep28766

²⁹² https://www.hrw.org/news/2013/06/28/uk-provide-clear-answers-data-surveillance

technology is the most prominent example of this. The European Commission proposed expanding the regulation scope to "concepts beyond military-related end use" and include 'cyber-surveillance technologies' as a subcategory in the export regulation framework.196 Amnesty International applauds the introduction of this subcategory."²⁹³

As a result, there should be a conceptual framework to develop a constructive approach to deal with privacy issues and provide practical solutions to modify or eliminate harmful practices existing in the use of CCTV cameras that increase the breach of fundamental freedoms and human rights.

Bibliography:

- (1) CameraFTP.com offers home monitoring, computer monitoring, Kids Monitoring, PC monitoring /screen recording and cloud recording services.
- https://www.drivehq.com/features/personal/cameraftp.aspx
- (2) Anderson, S. A. (2008). Privacy without the Right to Privacy. *The Monist*, *91*(1), 81–107. http://www.jstor.org/stable/27904067
- (3) State of Privacy Mexico | Privacy International. https://privacyinternational.org/state-privacy/1006/state-privacy-mexico
- (4) Turtiainen, Hannu & Costin, Andrei & Hämäläinen, Timo. (2022). CCTV-Exposure: System for measuring user's privacy exposure to CCTV cameras.
- (5) Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/10.2307/3481326
- (6) Alibeigi, Ali & Munir, Abu & Karim, Md. (2019). Right to Privacy, A Complicated Concept to Review. SSRN Electronic Journal. 10.2139/ssrn.3537968.
- (7) Anderson, S. A. (2008). Privacy without the Right to Privacy. *The Monist*, *91*(1), 81–107. http://www.jstor.org/stable/27904067
- (8) Vitalii, Serohin. (2021). INFORMATION PRIVACY: A CONCEPTUAL APPROACH. Constitutional and legal academic studies. 52-60. 10.24144/2663-5399.2020.2.06.
- (9) McCloskey, H. J. (1980). Privacy and the Right to Privacy. *Philosophy*, *55*(211), 17–38. http://www.jstor.org/stable/3750973
- (10) The Universal Declaration of Human Rights, 1948.

Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

- (11) "International Covenant on Civil and Political Rights." *Human Rights Quarterly*, vol. 7, no. 1, 1985, pp. 132–54. *JSTOR*, https://doi.org/10.2307/762040. Accessed 20 Jul.2022.
- (12) Waltz, S. (2002). Reclaiming and Rebuilding the History of the Universal Declaration of Human Rights. *Third World Quarterly*, *23*(3), 437–448. http://www.jstor.org/stable/3993535
- (13) Patel, Jayantibhai. (2007). Human Rights Education.
- (14) Huffstetler, Hanna & Mesquita, Judith & Meier, Benjamin. (2020). Monitoring and Review to Assess Human Rights Implementation. 10.1093/oso/9780197528297.003.0008.

²⁹³ Out of Control : FAILING EU LAWS FOR DIGITAL SURVEILLANCE EXPORT, SEPTEMBER 2020 , INDEX: EUR 01/2556/2020

file:///C:/Users/jniki/Downloads/EUR0125562020ENGLISH.pdf

- (15) How many days until Human Rights Day 10 December?. https://www.daysuntil.net/december-10-2023
- (16) Is the Right to Privacy a Human Right? Klinik Hukumonline. https://www.hukumonline.com/klinik/a/is-the-right-to-privacy-a-human-right-- lt63d0eaa88a7ae/
- (17) Louanne Meunier, Author at mcalisterhallam.com. https://mcalisterhallam.com/author/louanne-meunier/
- (18) Anderson, A., Miller, D., & Newman, D. (2018). Canada's Residential Schools and the Right to Integrity. Dalhousie Law Journal, 41(2), 301A.
- (19) Knowledge Center | Human Rights Defense Curaçao. https://humanrightsdefense.org/knowledge-center/
- (20) Coblentz, W. K., & Warshaw, R. S. (1956). European Convention for the Protection of Human Rights and Fundamental Freedoms. *California Law Review*, *44*(1), 94–104. https://doi.org/10.2307/3478312
- (21) ECHR Art. 8 Africa's Business. https://africasbusiness.com/echr-art-8/
- (22) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981
- https://www.coe.int/en/web/data-protection/convention108-and-protocol
- (23) Dorraji, Seyed & Barcys, Mantas. (2014). Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations. Social Technologies. 4. 306-317. 10.13165/ST-14-4-2-05.
- (24) Timan, T., Mann, Z. (2021). Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In: Curry, E., Metzger, A., Zillner, S., Pazzaglia, JC., García Robles, A. (eds) The Elements of Big Data Value. Springer, Cham. https://doi.org/10.1007/978-3-030-68176-0_7
- (25) Call for Views on GDPR derogations closes 5RB Barristers. https://www.5rb.com/data-protection/government-call-views-gdpr-derogations-closes-tomorrow/
- (26) Bonello, Rita (2016), Mass Surveillance and the Right to Privacy. Master of Laws Thesis submitted in partial fulfillment of the requirements for the degree of ADVANCED MASTERS IN EUROPEAN AND INTERNATIONAL HUMAN RIGHTS LAW, Universiteit Leiden. Available at:
- https://www.academia.edu/28728849/Mass_Surveillance_and_the_Right_to_Privacy
- (27) UK: Provide Clear Answers on Data Surveillance | Human Rights Watch.
- https://www.hrw.org/news/2013/06/28/uk-provide-clear-answers-data-surveillance
- (28) BAMBAUER, D. E. (2013). PRIVACY VERSUS SECURITY. *The Journal of Criminal Law and Criminology* (1973-), 103(3), 667–683. http://www.jstor.org/stable/43895376 page 13 or 678
- (29) Friedewald, Michael & Cas, Johann & Bellanova, Rocco & Burgess, J. & Peissl, Walter. (2017). Surveillance, Privacy and Security: Citizens' Perspectives. 10.4324/9781315619309.
- (30) OECD (2020), OECD Policy Responses to Coronavirus (COVID-19)Using artificial intelligence to help combat COVID-19.
- Available at: https://www.oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-ae4c5c21/
- (31) Grace Fox, Trevor Clohessy, Lisa van der Werff, Pierangelo Rosati, Theo Lynn, Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications, Computers in Human Behavior, Volume 121, 2021, 106806, ISSN 0747-5632,

https://doi.org/10.1016/j.chb.2021.106806.

(https://www.sciencedirect.com/science/article/pii/S0747563221001291)

- (32) Ioannou A, Tussyadiah I. Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. Technol Soc. 2021 Nov;67:101774. doi: 10.1016/j.techsoc.2021.101774. Epub 2021 Oct 8. PMID: 34642512; PMCID: PMC8497958.
- (33) Hartman, Laura. (2002). Technology and Ethics: Privacy in the Workplace. Business and Society Review. 106. 1 27. 10.1111/0045-3609.00099.
- (34) Lovin, Robin. (2021). Public Moral Discourse. Religions. 12. 255. 10.3390/rel12040255.
- (35) United States: Advance Human Rights of People around Us, Urges Secretary-General on Message for Day of Observance. (2016). MENA Report, n/a.
- (36) Bonello, Rita (2016), Mass Surveillance and the Right to Privacy. Master of Laws Thesis submitted in partial fulfillment of the requirements for the degree of ADVANCED MASTERS IN EUROPEAN AND INTERNATIONAL HUMAN RIGHTS LAW, Universiteit Leiden. Available at: https://www.academia.edu/28728849/Mass Surveillance and the Right to Privacy
- (37) Tecuci, Gheorghe. (2012). Artificial intelligence. Wiley Interdisciplinary Reviews: Computational Statistics. 4. 10.1002/wics.200.
- (38) Ibrahim, Sutrisno. (2016). A comprehensive review on intelligent surveillance systems. Communications in Science and Technology. 1. 10.21924/cst.1.1.2016.7.
- (39) J. Curzon, T. A. Kosa, R. Akalu and K. El-Khatib, "Privacy and Artificial Intelligence," in *IEEE Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 96-108, April 2021, doi: 10.1109/TAI.2021.3088084.
- (40) Olatunji, Iyiola & Cheng, Chun Hung. (2019). Video Analytics for Visual Surveillance and Applications: An Overview and Survey. 10.1007/978-3-030-15628-2_15.
- (41) Kumaravel, Rasadurai. (2023). Al Based Smart Surveillance System. International Journal of Scientific Research in Science, Engineering and Technology. 10. 10-15. 10.32628/IJSRSET229672.
- (42) Norris, Clive Norris (2009), A REVIEW OF THE INCREASED USE OF CCTV AND VIDEO-SURVEILLANCE FOR CRIME PREVENTION PURPOSES IN EUROPE. Department of Sociological Studies, University of Sheffield, UK Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS), Brussels. Available at: https://www.statewatch.org/media/documents/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf
- (43) Moyo, Sheperd (2019), EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG By submitted in accordance with the requirements for the degree of MAGISTER TECHNOLOGIES in SECURITY MANAGEMENT at the UNIVERSITY OF SOUTH AFRICA. Available at: https://core.ac.uk/download/pdf/286383944.pdf
- (44) Swami, Kedar & Bhuma, Bhardwaz & Mondal, Semanto & Lokam, Anjaneyulu. (2020). Audio Surveillance System. 10.1007/978-981-15-1366-4_28.
- (45) Richards, N. M. (2013). THE DANGERS OF SURVEILLANCE. *Harvard Law Review*, 126(7), 1934–1965. http://www.jstor.org/stable/23415062
- (46) Small or medium-scale focused research project (2012), Increasing Resilience in Surveillance Societies. IRISS, 290492, EP7-SSH-2011-2. Available at:
- https://www.academia.edu/26586909/IRISS_D1_MASTER_DOCUMENT_17Dec?email_work_card=view-paper

(47) C. William; R Webster, Interconnections Between Technological and Policy Innovation: Reevaluating the Evidence-Base Supporting the Provision of CCTV in the UK. University of Stirling. Available at:

https://dspace.stir.ac.uk/bitstream/1893/2703/1/interconnection%20between%20technologic al%20and%20policy%20innovation%2009.pdf

- (48) Yeganegi, Kamran & Moradi, Dawood & Obaid, Ahmed. (2020). Create a wealth of security CCTV cameras. Journal of Physics: Conference Series. 1530. 012110. 10.1088/1742-6596/1530/1/012110.
- (49) Guidelines 3/2019 on the processing of personal data through video devices, Adopted on 10 July.
- (50) Ball, Kirstie. (2010). Workplace Surveillance: An Overview. Labor History. 51. 10.1080/00236561003654776.
- (51) Zabłocki, Michał & Gościewska, Katarzyna & Frejlichowski, Dariusz & Hofman, Radosław. (2014). Intelligent video surveillance systems for public spaces a survey. Journal of Theoretical and Applied Computer Science. 8. 13-27.
- (52) https://www.firstcountymonitoring.co.uk/the-history-of-cctv-in-the-uk/
- (53) C. William; R Webster, Interconnections Between Technological and Policy Innovation: Reevaluating the Evidence-Base Supporting the Provision of CCTV in the UK. University of Stirling. Available at:

https://dspace.stir.ac.uk/bitstream/1893/2703/1/interconnection%20between%20technological%20and%20policy%20innovation%2009.pdf

- (54) https://earthweb.com/who-has-the-most-cctv-in-the-world/
- (55) Olatunji, Iyiola & Cheng, Chun Hung. (2019). Video Analytics for Visual Surveillance and Applications: An Overview and Survey. 10.1007/978-3-030-15628-2 15.
- (56) Loughran, Jack (Published Tuesday, January 9, 2018). Britain's network of CCTV cameras are vulnerable to attack by hackers according to a watchdog. Available at: https://eandt.theiet.org/content/articles/2018/01/britain-s-vast-network-of-cctv-cameras-is-vulnerable-to-hacks-watchdog-warns/
- (57) https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/
- (58) https://www.statista.com/chart/19256/the-most-surveilled-cities-in-the-world/
- (59) McCahill, Michael; Norris, Clive (2002). CCTV in London, Centre for Criminology and Criminal justice, University of Hull, Working paper no.6.

Available at: http://www.urbaneye.net/results/ue wp6.pdf

- (60) Norris, C., & McCahill, M. (2006). CCTV: BEYOND PENAL MODERNISM? *The British Journal of Criminology*, 46(1), 97–118. http://www.jstor.org/stable/23639334
- (61) https://www.statista.com/chart/19268/most-surveilled-cities-in-europe/
- (62) https://earthweb.com/how-many-cctv-cameras-in-london-are-there/
- (63) https://www.aaisecurity.co.uk/news/cctv-london-underground/
- (64) https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf
- (65) Kolomiiets, Nataliia & Senchenko, Nadiia & Petryk, Olena & Ivankov, Ihor & Olga, Ovsiannikova & Geperidze, Davit. (2023). International Legal Standards in Crime Prevention. WSEAS TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT. 19. 110-118. 10.37394/232015.2023.19.10.

- (66) THE ROOT CAUSES OF CRIME, CS&CPC Statement on the Root Causes of Crime approved in 1996.
- Available at: https://preventingcrime.ca/wp-content/uploads/2014/08/Causes_of_Crime.pdf
- (67) Ivory Research. (November 2021). Essay on Crime Prevention. Retrieved from https://www.ivoryresearch.com/samples/essay-on-crime-prevention/
- (68) https://preventingcrime.ca/wp-content/uploads/2014/08/Causes_of_Crime.pdf
- (69) Whitecross, Richard & Levy, Liz & Santhakumaran, Dharshi. (2014). What Works to Reduce Crime: A Summary of the Evidence.
- (70) WowEssays. (2020, April, 03) Free Cctv In The UK Essay Example. Retrieved July 01, 2023, from https://www.wowessays.com/free-samples/free-cctv-in-the-uk-essay-example/
- (71) Baoyan, Kenard Vic. (2023). CLOSED CIRCUIT TELEVISION (CCTV): A TOOL IN CRIME PREVENTION AND DETECTION. 10.13140/RG.2.2.32896.81928.
- (72) Laycock, Gloria & Clarke, Ronald. (2001). Crime Prevention Policy and Government Research: A Comparison of the United States and United Kingdom. International Journal of Comparative Sociology INT J COMP SOCIOL. 42. 235-255. 10.1177/002071520104200110.
- (73) Möllers, Norma & Hälterlein, Jens. (2013). Privacy issues in public discourse: The case of "smart" CCTV in Germany. Innovation: The European Journal of Social Sciences. 26. 10.1080/13511610.2013.723396.
- (74) Brandon C. Welsh & David P. Farrington (2009) Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis, Justice Quarterly, 26:4, 716-745, DOI: 10.1080/07418820802506206
- (75) A Report on the Surveillance Society, op. cit., para 9.5.3. https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf
- (76) https://core.ac.uk/download/pdf/286383944.pdf
- (77) WowEssays. (2020, April, 03) Free Cctv In The UK Essay Example. Retrieved July 01, 2023, from https://www.wowessays.com/free-samples/free-cctv-in-the-uk-essay-example/
- (78) Peterson Kelly (Author), 2012, Effectiveness of CCTV in Crime Prevention, Munich, GRIN Verlag, https://www.grin.com/document/280648
- (79) Khan, Md & Aziz, Moonmoon & Faruk, Omar & Talukder, Md.Ishtiaq. (2020). Impact of CCTV Surveillance on Crime Prevention: A Study in Dhaka City. 6. 48-59.
- (80) UK CCTV and crime prevention statistics: your FAQs answered. https://www.calipsa.io/blog/cctv-statistics-in-the-uk-your-questions-answered
- (81) Agisilaou, V. H. (2009). Information overload: CCTV, your networks, communities and crime. Australian Security and Intelligence Conference 2009.
- (82) https://monaulnay.com/wp-content/uploads/2009/03/hors252.pdf
- (83) Parliamentary Office of Science and Technology (2002), Postnote. Available at: https://www.parliament.uk/globalassets/documents/post/pn175.pdf
- (84) Sociology crime prevention essay, South Gloucestershire and Stroud College, Criminology (Crime202), Academic year: 2021/2022. Available at: https://www.studocu.com/engb/document/south-gloucestershire-and-stroud-college/criminology/sociology-crime-prevention-essay/45753330
- (85) https://www.bbc.com/news/magazine-30793614
- (86) Detainment FILM & TELEVISION BUSINESS. https://film-business.com/tag/detainment/

- (87) Barrie Sheldon (2011) Camera surveillance within the UK: Enhancing public safety or a social threat?, International Review of Law, Computers & Technology, 25:3, 193-203, DOI: 10.1080/13600869.2011.617494
- (88)https://inews.co.uk/news/uk/james-bulger-what-happened-death-murder-killers-jonvenables-robert-thompson-907387
- (89) https://inews.co.uk/news/uk/james-bulger-killers-jon-venables-robert-thompson-murder-now-221759
- (90) LawBirdie. (2023, March 23). Why Public Surveillance Cameras Should Be Banned. Retrieved from https://lawbirdie.com/why-public-surveillance-cameras-should-be-banned/
- (91) Goold, B., Loader, I., & Thumala, A. (2013). THE BANALITY OF SECURITY: The Curious Case of Surveillance Cameras. *The British Journal of Criminology*, *53*(6), 977–996. http://www.jstor.org/stable/23639949
- (92) David P. and others (2010). Feasibility Study on the Impact of CCTV on Criminal Justice Outcomes. Report to National Policing Improvement Agency. Available at:
- https://www.crim.cam.ac.uk/sites/www.crim.cam.ac.uk/files/cctvnpia.pdf
- (93) Association of chief police officers (ACPO), National Policing Improvement Agency (NPIA), 2011. Practice advice on the use of CCTV in criminal investigations. Available at: https://zakon.co.uk/admin/resources/downloads/cctv-practice-advice-on-the-use-of-cctv-in-criminal-investigations.pdf
- (94) Bose, Palash & Kabir, Mohammad. (2017). Fingerprint: A Unique and Reliable Method for Identification. Journal of Enam Medical College. 7. 29. 10.3329/jemc.v7i1.30748.
- (95) Ashby, Matthew. (2017). The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. European Journal on Criminal Policy and Research. 23. 10.1007/s10610-017-9341-6.
- (96) Brookman, Fiona, and others (2020). The Use of CCTV during Homicide Investigations: Contributions, Challenges and Risks, RESEARCH INSIGHT. Available at:
- https://pure.southwales.ac.uk/ws/portalfiles/portal/3994343/HIFS_Project_Research_Insight_ 3._The_Use_of_CCTV_during_Homicide_Investigations_Contributions_Challenges_and_Risks_A pril_2020_.pdf
- (97) Baoyan, Kenard Vic. (2023). CLOSED CIRCUIT TELEVISION (CCTV): A TOOL IN CRIME PREVENTION AND DETECTION. 10.13140/RG.2.2.32896.81928.
- (98) Taylor, Emmeline (2020). Understanding the effectiveness of CCTV: Displacement, Deterrence, and Detection: An overview of research prepared for Sevenoaks District Council. School of Arts and Social Sciences City, University of London. Available at: https://cds.sevenoaks.gov.uk/documents/s43565/Appendix%202%20-
- %20Dr.%20Taylors%20Review%20-%20CCTV_evidence%20and%20impact%20overview.pdf?J=1 (99) Sung, Chang-Soo & Park, Joo. (2021). Design of an intelligent video surveillance system for crime prevention: applying deep learning technology. Multimedia Tools and Applications. 80. 10.1007/s11042-021-10809-z.
- (100) https://www.statewatch.org/media/documents/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf
- (101) Webster, C.. (2009). CCTV policy in the UK: Reconsidering the evidence base. Surveill. Soc. 6. 10.24908/ss.v6i1.3400.4

- (102) Moyo, Sheperd (2019), EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG By submitted in accordance with the requirements for the degree of MAGISTER TECHNOLOGIES in SECURITY MANAGEMENT at the UNIVERSITY OF SOUTH AFRICA. Available at: https://core.ac.uk/download/pdf/286383944.pdf
- (103) Fyfe, N. R., & Bannister, J. (1996). City Watching: Closed Circuit Television Surveillance in Public Spaces. *Area*, *28*(1), 37–46. http://www.jstor.org/stable/20003625
- (104) Joon Tag Cho, Jisun Park, Exploring the effects of CCTV upon fear of crime: A multi-level approach in Seoul,

International Journal of Law, Crime, and Justice, Volume 49,2017, Pages 35-45, ISSN 1756-0616, https://doi.org/10.1016/j.ijlcj.2017.01.005.

(https://www.sciencedirect.com/science/article/pii/S1756061616301598)

(105) Honess, Terry; Charman, Elizabeth, CLOSED CIRCUIT TELEVISION IN PUBLIC PLACES: ITS ACCEPTABILITY AND PERCEIVED EFFECTIVENESS. POLICE RESEARCH GROUP CRIME PREVENTION UNIT SERIES: PAPER NO.35 LONDON: HOME OFFICE POLICE DEPARTMENT.

Available at: http://www.casa.ucl.ac.uk/cyberspace/fcpu35.pdf

- (106) Webster, C.. (2004). The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK. Surveillance and Society. 2. 10.24908/ss.v2i2/3.3376.
- (107) Tripathi, Keyur and Mubarak, Usama, Protecting Privacy in the Era of Artificial Intelligence (March 24, 2020).

Available at

- SSRN: https://ssrn.com/abstract=3560047 or http://dx.doi.org/10.2139/ssrn.3560047
- (108) Amnesty International (2020). OUT OF CONTROL: FAILING EU LAWS FOR DIGITAL SURVEILLANCE EXPORT.
- (109) McCahill, Michael; Norris, Clive (2002). CCTV in Britain, Centre for Criminology and Criminal justice, University of Hull, Working paper No.3. Available at: http://www.urbaneye.net/results/ue wp3.pdf.
- (110) Pauwels, E. (2020). Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention: Opportunities and Challenges for the International Community. Global Center on Cooperative Security. http://www.jstor.org/stable/resrep27551
- (111) https://www.gov.uk/government/publications/regulation-of-investigatory-powers-act-2000-ripa/regulation-of-investigatory-powers-act-2000-ripa
- (112) https://www.gov.uk/government/publications/regulation-of-investigatory-powers-act-2000-ripa/regulation-of-investigatory-powers-act-2000-ripa
- (113)https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf
- (114) https://www.gov.uk/government/publications/protection-of-freedoms-bill
- (115) Freedom of Information (FoI) West Lancashire Borough Council. https://www.westlancs.gov.uk/about-the-council/information-governance/freedom-of-information.aspx
- (116) Freedom of Information | The Wilbraham Surgery. https://wilbrahamsurgery.nhs.uk/freedom-of-information/
- (117) Friedewald, Michael & Cas, Johann & Bellanova, Rocco & Burgess, J. & Peissl, Walter. (2017). Surveillance, Privacy and Security: Citizens' Perspectives. 10.4324/9781315619309.

- (118) IvyPanda. (2019, November 17). *Effects of Surveillance Technology on Privacy*. https://ivypanda.com/essays/the-spread-of-surveillance-technologies-as-closed-circuit-cameras-on-privacy/
- (119) G2124921.pdf (un.org)
- (120) Königs, P. Government Surveillance, Privacy, and Legitimacy. *Philos. Technol.* **35**, 8 (2022). https://doi.org/10.1007/s13347-022-00503-9
- (121) Webster, C.. (2009). CCTV policy in the UK: Reconsidering the evidence base. Surveill. Soc. 6. 10.24908/ss.v6i1.3400.
- (122) LawBirdie. (2023, March 23). Why Public Surveillance Cameras Should Be Banned. Retrieved from https://lawbirdie.com/why-public-surveillance-cameras-should-be-banned/
- (123) Benjamin J Goold, "CCTV and Human Rights" in Citizens, Cities and Video Surveillance: Towards a Democratic and Responsible Use of CCTV (Paris: European Forum for Urban Security, 2010) 27.
- (124) A Brief Look at Human Rights Violations: (part 18) The UK. https://www.odvv.org/blog-3292-A-Brief-Look-at-Human-Rights-Violations--part-18-The-UK
- (125) https://www.amnesty.org/en/latest/press-release/2021/05/uk-surveillance-gchq-ecthr-ruling/
- (126) Charlesworth, Andrew, CCTV, Data Analytics and Privacy: The Baby and the Bathwater (August 20, 2018).

Available at

- SSRN: https://ssrn.com/abstract=3606278 or https://dx.doi.org/10.2139/ssrn.3606278
- (127) Rascão, Jose & Poças, Nuno. (2021). Freedom of Expression and the Right to Privacy and Ethics in Dialectic of Human Rights in This Complex and Turbulent Society. International Journal of Project Management and Productivity Assessment. 9. 1-28. 10.4018/IJPMPA.2021070101.
- (128) Webster, C.. (2009). CCTV policy in the UK: Reconsidering the evidence base. Surveill. Soc. 6. 10.24908/ss.v6i1.3400.4
- (129) Knopp, Philipp & Ullrich, Peter. (2018). Protesters' Reactions to Video Surveillance of Demonstrations. Counter-Moves, Security Cultures, and the Spiral of Surveillance and Counter-Surveillance. Surveillance & Society. 16. 10.14279/depositonce-7186.
- (130) Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220. https://doi.org/10.2307/1321160
- (131) Agisilaou, V. H. (2009). Information overload: CCTV, your networks, communities and crime. Australian Security and Intelligence Conference 2009.
- (132)https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf
- (133) Surveillance Camera Code of Practice 12 Principles | The Data Compliant Blog. https://datacompliantblog.com/2014/10/16/surveillance-camera-code-of-practice-12-principles/

(134)

- file:///C:/Users/jniki/Downloads/20200724%20Storing%20and%20Retention%20CCTV%20imag es%20V2.0%20(2).pdf
- (135) https://www.scitepress.org/Papers/2020/89642/89642.pdf
- (136) Macnish, K orcid.org/0000-0003-4510-3049 (2018) Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. Journal of Applied Philosophy, 35 (2). pp. 417-432. ISSN 0264-3758 https://doi.org/10.1111/japp.12219

- (137) https://ukhumanrightsblog.com/2015/03/06/public-protest-private-rights/
- (138) https://vlex.co.uk/vid/r-catt-v-association-805385985
- (139) https://vlex.co.uk/vid/catt-v-association-of-793520813
- (140) https://hudoc.echr.coe.int/fre?i=001-189424
- (141) https://www.dataprotection.ie/sites/default/files/uploads/2019-
- 05/CCTV%20guidance%20data%20controllers 0.pdf
- (142) Odoemelam Chika, Adapting to Surveillance and Privacy Issues in the Era of Technological and Social Networking, International Journal of Social and Humanity, Vol.5, No.6, June 2015 Available at: http://www.ijssh.net/papers/520-H140.pdf
- (143) Fitwi, Alem, Yu Chen, Sencun Zhu, Erik Blasch, and Genshe Chen. 2021. "Privacy-Preserving Surveillance as an Edge Service Based on Lightweight Video Protection Schemes Using Face De-Identification and Window Masking" *Electronics* 10, no. 3: 236. https://doi.org/10.3390/electronics10030236
- (144) IvyPanda. (2019, November 17). *Effects of Surveillance Technology on Privacy*. https://ivypanda.com/essays/the-spread-of-surveillance-technologies-as-closed-circuit-cameras-on-privacy/
- (145) A Review of the Increased use of CCTV ad Video-Surveillance for crime prevention purposes in Europe, Policy Department C, Citizens' Rights and Constitutional Affairs, PE 419.588, April 2009 Available at: https://www.statewatch.org/media/documents/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf
- (146) Koch H., Matzner T. & Krumm, J., "Privacy Enhancing of Smart CCTV and its Ethical and Legal Problems", in European Journal of Law and Technology, Vol 4., No. 2., 2013.
- (147) Catarina Fontes, Ellen Hohma, Caitlin C. Corrigan, Christoph Lütge, Al-powered public surveillance systems: why we (might) need them and how we want them, Technology in Society, Volume 71, 2022, 102137, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2022.102137.
- (148) Kok-Seng Wong, Nguyen Anh Tu, Anuar Maratkhan, and M.Fatih Demirci. 2021. A Privacy-Preserving Framework for Surveillance Systems. In 2020 the 10th International Conference on Communication and Network Security (ICCNS 2020). Association for Computing Machinery, New York, NY, USA, 91–98. https://doi.org/10.1145/3442520.3442524
- (149) Cole, Mark. (2004). Signage and Surveillance: Interrogating the Textual Context of CCTV in the UK. Surveillance and Society. 2. 10.24908/ss.v2i2/3.3387.
- (150) https://gdprtool.cyberwatching.eu/Pages/Workflow.aspx
- (151) definitions · Sunny Cars. https://www.sunnycars.de/deen/security-and-data-protection/definitions/
- (152)https://www.lexology.com/library/detail.aspx?g=854e9b90-2dab-4d99-9c9a-70bb1e85b27b
- (153) Richards, N. M. (2013). THE DANGERS OF SURVEILLANCE. *Harvard Law Review*, 126(7), 1934–1965. http://www.jstor.org/stable/23415062
- (154) Dorraji, Seyed & Barcys, Mantas. (2014). Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations. Social Technologies. 4. 306-317. 10.13165/ST-14-4-2-05.
- (155) Benjamin J Goold, "CCTV and Human Rights" in Citizens, Cities and Video Surveillance: Towards a Democratic and Responsible Use of CCTV (Paris: European Forum for Urban Security, 2010) 27.

- (156) Pelteret, Marc & Ophoff, Jacques. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. Informing Science The International Journal of an Emerging Transdiscipline. 19. 277-301. 10.28945/3573.
- (157) G. F. Shidik, E. Noersasongko, A. Nugraha, P. N. Andono, J. Jumanto and E. J. Kusuma, "A Systematic Review of Intelligence Video Surveillance: Trends, Techniques, Frameworks, and Datasets," in IEEE Access, vol. 7, pp. 170457-170473, 2019, doi: 10.1109/ACCESS.2019.2955387. (158)https://commons.allard.ubc.ca/cgi/viewcontent.cgi?article=1151&context=fac_pubs
- (159) Paul Tennent Surveillance Camera Code of Practice Infologue.com Manned Security e-Zine. https://www.infologue.com/editorial/paul-tennent-surveillance-camera-code-of-practice/(160) Purpose Limitation | isItEthical. https://www.isitethical.org/portfolio-item/purpose-limitation/
- (161) EDPB's Guidelines 3/2019 on the processing of personal data through video devices Part 3 of 13 Intenseye. https://www.intenseye.com/resources/edpbs-guidelines-3-2019-on-the-processing-of-personal-data-through-video-devices-part-3-of-13
- (162)https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-
- Group/20181130 WP Artificial-Intelligence.pdf? blob=publicationFile&v=1
- (163) United Kingdom: Biometrics and Surveillance Camera Commissioner speech at the National ANPR Conference 2021. (2022). MENA Report.
- (164)https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-687182-694690%22]}
- (165) Ensuring transparency and responsibility in surveillance camera use | Research | University of Stirling. https://www.stir.ac.uk/research/research-spotlights/ensuring-transparency-and-responsibility-in-surveillance-camera-use/
- (166) What we can learn from public attitudes towards surveillance, CCTV in the UK, White Paper Available at:
- https://synecticsglobal.com/Content/Downloads/Synectics_PublicSpace-Whitepaper.pdf (167)https://www.stir.ac.uk/research/research-spotlights/ensuring-transparency-and-responsibility-in-surveillance-camera-use/
- (168) Björklund, F. (2021) Trust and surveillance: An odd couple or a perfect pair? In: Lora Anne Viola; Paweł Laidler (ed.), Trust and Transparency in an Age of Surveillance (pp. 183-200). London: Routledge Routledge Studies in Surveillance https://doi.org/10.4324/9781003120827-14
- (169) PRESS RELEASE: EU Ethics Guidelines for Trustworthy AI presented at the EU Digital Day ALLAI. https://allai.nl/press-release-eu-ethics-guidelines-for-trustworthy-ai-presented-at-the-eu-digital-day/
- (170) Surveillance Camera Code of Practice 12 Principles | The Data Compliant Blog. https://datacompliantblog.com/2014/10/16/surveillance-camera-code-of-practice-12-principles/
- (171) Why Tech And Policing Don't Always Mix. (2017, October 1). PC Pro, 276, 127.
- (172) Becker, M. Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. *Ethics Inf Technol* **21**, 307–317 (2019). https://doi.org/10.1007/s10676-019-09508-z
- (173) BoonJot Hinting Preview | สำนักอักขระฟอนต์อยู่นี่. https://fontuni.com/boonjot/hinting.html

- (174) Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, 6(1). https://doi.org/10.1177/2053951719860542
- (175)https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-
- Group/20181130 WP Artificial-Intelligence.pdf? blob=publicationFile&v=1
- (176) CCTV: Developing Privacy Best Practices, Report on the DHS privacy office public workshop, December 2007.
- Available at: https://www.dhs.gov/sites/default/files/publications/privacy_rpt_cctv_2007.pdf (177) https://commons.allard.ubc.ca/cgi/viewcontent.cgi?article=1151&context=fac_pubs
- (178) Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160
- (179) Controller Definition: 9k Samples | Law Insider. https://www.lawinsider.com/dictionary/controller
- (180) https://www.gov.uk/government/case-studies/joint-working-cumbria-police-and-crime-commissioner-police-and-councils-combine-cctv
- (181) Richards, N. M. (2013). THE DANGERS OF SURVEILLANCE. *Harvard Law Review*, 126(7), 1934–1965. http://www.jstor.org/stable/23415062
- (182) Daniel J. Power, Ciara Heavin & Yvonne O'Connor (2021) Balancing privacy rights and surveillance analytics: a decision process guide, Journal of Business Analytics, 4:2, 155-170, DOI: 10.1080/2573234X.2021.1920856
- (183) Comments on the Srikrishna Committee Report and the Draft Data Protection Bill 2018 III Tech Law Forum @ NALSAR. https://techlawforum.nalsar.ac.in/recent-news-comments-on-the-srikrishna-committee-report-and-the-draft-data-protection-bill-2018-iii/
- (184) Assessing the necessity of measure that limit the fundamental right to the protection of personal data: A Toolkit, European Data Protection supervisor, 11 April 2017 Available at:
- $https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_1.pdf$
- (185) Privacy policy |. http://astersc.eu/en/privacy-policy/
- (186) Čtvrtník, Mikuláš. (2023). Data Minimisation—Storage Limitation—Archiving. 10.1007/978-3-031-18667-7 8.
- (187) Available at: https://www.abouthumanrights.co.uk/human-rights-cctv.html
- (188) Councils urged to be open about CCTV data | UKAuthority. https://www.ukauthority.com/articles/councils-urged-to-be-open-about-cctv-data/
- (189) Macnish, KNJ orcid.org/0000-0003-4510-3049 (2015) An Eye for an Eye: Proportionality and Surveillance. Ethical Theory and Moral Practice, 18 (3). pp. 529-548. ISSN 1386-2820 https://doi.org/10.1007/s10677-014-9537-5
- (190) Smith, M., Miller, S. (2021). Facial Recognition and Privacy Rights. In: Biometric Identification, Law and Ethics. Springer Briefs in Ethics. Springer, Cham. https://doi.org/10.1007/978-3-030-90256-8 2
- (191) CCTV Policy | CCTV Policy | Reigate and Banstead. https://www.reigate-banstead.gov.uk/info/20209/access_to_information/1405/cctv_policy
- (192) Macnish, KNJ orcid.org/0000-0003-4510-3049 (2015) An Eye for an Eye: Proportionality and Surveillance. Ethical Theory and Moral Practice, 18 (3). pp. 529-548. ISSN 1386-2820 https://doi.org/10.1007/s10677-014-9537-5

(193) Fairhurst v Woodard Judgment

Available at : https://www.judiciary.uk/wp-content/uploads/2022/07/Fairhurst-v-Woodard-Judgment-1.pdf

(194) 5. Principles relating to personal data processing - easyGDPR. https://easygdpr.eu/en/gdpr-article/5/

(195) Case Law: Fairhurst v Woodard, Neighbour CCTV harassment and data protection claim succeeds – Percy Preston – Inforrm's Blog. https://inforrm.org/2021/10/20/case-law-fairhurst-v-woodard-neighbour-cctv-harassment-and-data-protection-claim-succeeds-percy-preston/

(196)https://inforrm.org/2021/10/20/case-law-fairhurst-v-woodard-neighbour-cctv-

harassment-and-data-protection-claim-succeeds-percy-preston/

(197) www.edpb.europa.eu edpb guidelines 201903 videosurveillance.pdf (europa.eu)

(198) Privacy Commissioner for Personal Data, Hong Kong, July 2010.

Available at :

https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf (199) Bartneck, Christoph & Lütge, Christoph & Wagner, Alan & Welsh, Sean. (2021). Privacy Issues of Al. 10.1007/978-3-030-51110-4 8.

(200) Koch H., Matzner T. & Krumm, J., "Privacy Enhancing of Smart CCTV and its Ethical and Legal Problems", in European Journal of Law and Technology, Vol 4., No. 2., 2013.

(201) EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG, Moyo Sheperd, February 2019

Available at: https://core.ac.uk/download/pdf/286383944.pdf

(202) Turtiainen, Hannu & Costin, Andrei & Hämäläinen, Timo. (2022). CCTV-Exposure: System for measuring user's privacy exposure to CCTV cameras.

(203) https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=12225&context=theses

(204) Gao, Zhang. (2019). Research on Network Information Security and Privacy Protection in the Age of Big Data. Journal of Physics: Conference Series. 1237. 022092. 10.1088/1742-6596/1237/2/022092.

(205) Artificial Intelligence and Data Protection: Observations on a Growing Conflict Fred H. Cate & Rachel Dockery

(206) Pauwels, E. (2020). Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention: Opportunities and Challenges for the International Community. Global Center on Cooperative Security. http://www.jstor.org/stable/resrep27551

(207) Encryption: A Matter of Human Rights, Amnesty International, March 2016 Index: POL 40/3682/2016

Available at:

https://www.amnesty.nl/content/uploads/2016/03/160322_encryption_-

a matter of human rights - def.pdf

(208) Privacy Statement – Open Future. https://openfuture.eu/privacy/

(209) Tarafder, A. (2015). SURVEILLANCE, PRIVACY AND TECHNOLOGY: A COMPARATIVE CRITIQUE OF THE LAWS OF USA AND INDIA. *Journal of the Indian Law Institute*, *57*(4), 550–578. http://www.jstor.org/stable/44782800

(210) Data Protection Authority | Data Privacy Glossary | Protecto. https://www.protecto.ai/data-privacy-glossary/data-protection-authority

- (211) Olufohunsi, Temitope. (2019). DATA ENCRYPTION Olufohunsi, T. (212)
- https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F48%2F4&Language=E&DeviceType=Desktop&LangRequested=False
- (213) Cammozzo, Alberto. (2011). Face Recognition and Privacy enhancing techniques. Page 6
- (214) Tripathi, Keyur and Mubarak, Usama, Protecting Privacy in the Era of Artificial Intelligence (March 24, 2020). Available at
- SSRN: https://ssrn.com/abstract=3560047 or http://dx.doi.org/10.2139/ssrn.3560047
- (215) Majeed, Abdul & Lee, Sungchang. (2020). Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3045700. (216)
- Data Anonymization Task. http://lod.iula.upf.edu/resources/DataAnonymization
- (217) Domingo-Ferrer, Josep & Sánchez, David & Soria-Comas, Jordi. (2016). Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections. 10.2200/S00690ED1V01Y201512SPT015.
- (218) Pelteret, Marc & Ophoff, Jacques. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. Informing Science The International Journal of an Emerging Transdiscipline. 19. 277-301. 10.28945/3573.
- (219) Lewis, J. A., & Crumpler, W. (2021). *Questions about Facial Recognition*. Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep28766
- (220) https://www.hrw.org/news/2013/06/28/uk-provide-clear-answers-data-surveillance
- (221) Out of Control : FAILING EU LAWS FOR DIGITAL SURVEILLANCE EXPORT, SEPTEMBER 2020 , INDEX: EUR 01/2556/2020
- file:///C:/Users/jniki/Downloads/EUR0125562020ENGLISH.pdf
- (222) https://www.washingtonpost.com/local/public-safety/2-arrested-in-uk-in-hacking-of-dc-police-closed-circuit-camera-network/2017/02/02/24c2c0ea-e969-11e6-80c2-30e57e57e05d story.html