Student First Name: Dawda

Student Last Name: Wally

Student ID: R2404D17931625

Date of Submission: November 10th, 2024

Assignment Name: CN7015_assignment-1.

Module Name: UEL-CN-7015-64412 IT and Internet Law

Module Code: CN7015

Table of Contents

1. Topic Description: Introduction

The coming of information and communication technology (ICT) has transformed the dynamics of society, notably impacting the legal landscape including data privacy and public surveillance. Digital advancement in the United Kingdom (UK) has facilitated the commission of traditional crimes like e.g. fraud, theft and other forms of cybercrimes, e.g. cyberattacks, hacking and malicious software distribution (Edwards and Savage 1986). With its continued evolution, ICT raises particular dilemmas for legislators in the balancing of rights of the individual (especially privacy) and public safety and national security (Rowland & Macdonald, 2000). This report looks at these challenges from the UK's legal perspective, by examining how legislation reacts to the wide-ranging issues of data privacy and public surveillance.

In recent years there have been substantial needs for robust data protection and privacy safeguards as more personal data is being collected, stored and analyzed by both private and public organizations. This helps to service the needs of researchers, because of ICTs' ability to collect such copious amounts of data. Such massive data collection, storage and analysis has been accompanied by a corresponding concern about individual privacy rights and the possibility of government overreach through widespread surveillance mechanisms. Legal responses in the UK to these issues have been formulated in the form of, amongst others, the Data Protection Act (DPA) 2018 and the Regulation of Investigatory Powers Act (RIPA) 2000 and certain case laws which attempt to interpret these legislative norms in practice (Lloyd, 2011).

This report takes a structured approach that starts with an overview of the major problems of data privacy and surveillance. Rules in the legal framework are discussed in light of the critical

analysis of how effective these rules are, and a comparison with similar rules in the European Union (EU). This structure will allow an in-depth exploration of how such data privacy protection and surveillance regulation laws are put in place in the UK, and how well these laws are protecting citizens' digital rights in terms of current and emerging threats.

The structural organization of the remainder of this report is as follows: Chapter 2 focuses on issue identification to lay the groundwork for the facts of the matters being addressed. Chapter 3 discusses relevant Acts and Directives. Chapter 4 focuses on analyses of different relevant case laws which is followed by a comprehensive conclusion in chapter 5.

1.1 Brief Overview of IT and Internet Law

Digital technology has increased and so too has the breadth of the legal frameworks designed to govern its use, policing for fair practice, and safeguarding the interests of companies and individuals (Edwards & Savage, 1986). Legally, in the UK, personal data should be treated following DPA 2018, to clarify when it is allowed to be surveilled under the RIPA 2000. The law in this area is ever-changing, with new technological advances posing problems to legislators who must adapt to get the right balance between technological advances and consideration of the ethics involved and maintaining public trust (Lloyd, 2011).

1.2 Key issues: Data Privacy and Surveillance

As data privacy and surveillance are important topics in IT and Internet law, they have a direct impact on individuals' freedom and society's trust in technology usage. Data privacy concerns

the rights that people have in personal information about them, such as what information is collected and shared. There has been an increase in the number of industries that depend on big data analytics, and thus, companies using online platforms and interconnected devices have raised concerns about data misuse, unauthorized access and poor consent mechanisms (Lloyd, 2011).

The monitoring of people's activities by government or private entities for purposes of public safety or crime deterrence is public surveillance (Rowland & Macdonald, 2000; Easton, 2007).

2. Issue Identification: Facts of the matter

This chapter examines the main issues concerning legal framework protection for data privacy and surveillance in the UK. Due to rapid growth in technology, the collection and processing of personal data are now an essential part of everyday private and public sector operations.

2.1 Data Privacy Concerns

2.1.1 Data privacy in the UK context.

In the UK, data privacy denotes the statutory leave and essential principles under which individual data are gathered, managed and disseminated. It aims to protect people's rights to their data and how organisations handle their information. UK data privacy law is based on DPA 2018 which is not too far away from the EU's General Data Protection Regulation (GDPR). According to this Act, it requires that data be processed in a lawful, fair and transparent manner and other

principles applicable to data minimization, accuracy, limitation to storage, and security (Lloyd, 2011). Data privacy does this via these guidelines; that is, empowering people to take control of their information and also setting the rules for organizations to deal with information in the right way.

2.1.2 Key concerns: data collection, consent, and individual rights.

The expansion of data-driven technologies has raised several key concerns regarding data privacy, particularly data collection, consent, and individual rights.

1. **Data Collection**: As data collection methods have become more modern, they are becoming invasive, too, and they capture information that we consider personal, from different sources, like social media, online transactions, Internet of Things (IoT) devices, etc. One worry is that a lot of data is being collected, often without people even knowing about it, let alone understanding how their data is used. To do this the DPA 2018 aims to limit unnecessary data collection and encourages best practice in anonymizing data to avoid over (un)intentional (mis)use (Edwards & Savage, 1986).

2. **Consent**: Under the DPA and GDPR, consent must be 'freely given, specific, informed, and unambiguous' meaning that people should always have a real choice whether their data is used or not. However getting real consent is always hard, especially when service providers pressure people to hand over their data to gain access to services they need. As a result, people have been pushing for more clarity and accountability in the mechanisms

through which people give consent to data use so that their autonomy over data is respected (ICO, 2006).

3. **Individual Rights**: The individual rights are: the right to access their data; the right to have incorrect personal data corrected; the right to erase their data; and the right to object to or restrict data processing. The idea is to give individuals the ability to steer the usage of their personal information and to provide recourse when their privacy has been breached. Yet these rights are not always realized in practice, notably when people are having trouble accessing or controlling data held by major organizations (Lloyd, 2011).

2.2 Public Surveillance and its Implications

This section defines what is meant by 'public surveillance' and explores the main modes of surveillance, with particular reference to surveillance by Closed Circuit Television (CCTV) and Automated Number Plate Recognition (ANPR) systems.

2.2.1 Definition and types of Surveillance (physical, data, psychological).

Public surveillance entails the surveillance of people's activities by government agencies, private firms and other bodies for enhancing physical safety, crime deterrence and information gathering. Surveillance can be categorized into three main types: physical, data, and psychological.

1. **Physical Surveillance**: It is directly observing or recording a person's physical activity (movement) in situ (essentially in the place), usually using CCTV cameras or security

personnel. Cameras and other monitoring equipment are often used for physical surveillance in urban spaces and transportation systems, which stops crime and records suspects' behaviours (Lloyd, 2011).

2. **Data Surveillance**: Data surveillance (digital or informational surveillance) is the act of tracking and analyzing people's online behaviour using transactional, behavioural, device, and personal data. Unlike physical surveillance, digital surveillance instead depends on digital footprints that interactions with online platforms, financial transactions and mobile devices leave as individuals go about their business. Private companies use data surveillance for targeted marketing and government agencies use them for national security purposes (Rowland & Macdonald, 2000).

3. **Psychological Surveillance**: Psychological surveillance is the analysis of an individual's behaviours or his/her psychological characteristics, to determine their mental state. Though not quite so common, this type of surveillance can have an impact on the behavior of people, creating a kind of 'lurking' effect where people might act differently, or make different decisions, because they feel as though they are being watched. On the other hand, considering one is being surveilled, will potentially influence behaviour such as opting to mirror public opinion to societal norms and expectations (Lloyd, 2011).

2.2.2 Concerns regarding CCTV, ANPR, and other surveillance mechanisms

Because CCTV is widely used in the UK, there is an estimated one camera for every 14 people making it one of the most surveilled nations (BBC News, 2006), it faces intense public scrutiny. CCTV, along with the related term 'CCTV surveillance', is used to monitor public space for the prevention of crime and criminal investigation. However, the widespread use does entail a whole host of privacy invasions since people cannot realize the extent to which their movements are being recorded and stalked.

The second most frequently used surveillance tool is the ANPR system, which reads and records vehicle license plates at many points across road networks. Using ANPR data linked to databases (such as the Driver and Vehicle Licensing Agency (DVLA)) allows authorities to track vehicle movement and enforce laws including insurance, tax and traffic violations (ANPR, 2005). To some, ANPR is effective for detailing vehicles that took part in criminal activities (Lloyd, 2011); however, its critics argue that its contribution is the intrusion of mass surveillance that allows the state to build a substantial report of those individuals' travel patterns without adequate consent or proper auditing (Easton, 2007).

2.3 Legal Context and Case Studies

The main legislation that outlines how privacy and surveillance are managed in the UK are described in this section including the Computer Misuse Act, General Data Protection Regulation (GDPR) and other regulations.

2.3.1 Relevant laws and regulations, e.g., Computer Misuse Act, GDPR.

1. **Computer Misuse Act 1990**: The Computer Misuse Act 1990, enacted in response to the emerging threat of computer-related crime, renders 'unauthorised access' to computer systems and data criminal. First proposed to cover legal lacunae in the types of cases involving hacking and computer fraud, the Act created offences for unauthorized access (hacking), unauthorized access to commit further offences, and the unauthorized modification of computer material (Edwards & Savage, 1986). Over time, amendments have been made to the Act to strengthen it to keep pace with the evolved nature of cyber threats, which are becoming more and more commonplace, and the need to protect both the individual and the organisation from abuse of technology (Lloyd, 2011).

2. **Data Protection Act 2018 (DPA)** and **General Data Protection Regulation (GDPR)**: The DPA 2018 adopts the GDPR into UK law to become the principal data privacy legislation in the UK. In 2018 the GDPR, which applies throughout the European Union, set tight guidelines for the collection, storage and processing of personal information, forcing organizations to gain express consent for data use, setting forth data transparency, and ensuring data accuracy and security (ICO, 2018). GDPR protections are extended by the DPA which sets out UK-specific provisions for additional data susceptible protection and legal frameworks for data processing in the public interest (Lloyd, 2011).

3. **Protection of Freedoms Act 2012**: The purpose of this Act is to limit surveillance actions and where surveillance data is used and retained to protect individual freedoms. Among other things, its main provision requires that CCTV and other surveillance technologies should be subject to codes of practice and oversight. Biometric data collection is restricted by the Act, blocking fingerprinting and DNA storage to be retained only when justified and by judicial approval under particular situations (Lloyd, 2011).

3. Rule Identification: Relevant Acts, Directives, etc.

This section describes, identifies and analyses the UK legal framework under which the right not to be subjected to data surveillance and collection within the context of public life is regulated. Through key statutes and relevant case law, this section explains when, how, and by whom surveillance is protected and regulated.

3.1 UK Legal Framework

3.1.1 Overview of key UK statutes (Data Protection Act 2018, RIPA 2000).

1. **Data Protection Act 2018 (DPA)**:

   Data Privacy protection in the UK is principally enforced by the DPA 2018, which integrates the provisions of the EU's GDPR. It sets rules on how personal data is collected, processed, stored and shared. The DPA mandates lawful, fair and transparent processing, data minimization, accuracy, and accountability. The DPA protects the right of users to have access to, rectify or erase personal information (Lloyd, 2011). The DPA's

integration of GDPR principles, since the GDPR applies extraterritorially, means that UK data protection standards will remain aligned with EU regulation even in the post-Brexit world.

2. **Regulation of Investigatory Powers Act 2000 (RIPA)**:

   The legal mechanisms under which public authorities can and are encouraged to intercept communications are established by the RIPA 2000. RIPA was enacted to respond to changes in the way that communication occurs, namely digitally, and set out the circumstances in which such surveillance can be sanctioned and kept within the realm of what is legally acceptable for investigative practice (The Scotsman, n.d.). RIPA contains provisions for both electronic and human intelligence gathering, and restricts how such authorisation is given, how activity is monitored, and how data are retained (Rowland & Macdonald, 2000). The Act has repeatedly been amended, for example, most recently with the Investigatory Powers Act 2016, which greatly increases the scope of surveillance and arouses fears of intrusion of privacy and the necessity of thrifty supervision (Easton, 2007).

3.1.2 Case law and precedents (e.g., R v Gold and Schifreen, R v Whitely).

1. **R v Gold and Schifreen** (1988):

   Unauthorised access to computer systems was tackled in the case of R v Gold and Schifreen, and it resulted in important developments in UK law concerning cybercrime.

In the 1980s two hackers by the name of Robert Schifreen and Stephen Gold exploited system vulnerabilities to gain unauthorized access to British Telecom's Prestel service. The defendants were charged with forgery under the Forgery and Counterfeiting Act but were later acquitted by the court as it believed the litigation to be insufficient for the prosecution of computer-related crimes (Edwards & Savage, 1986). This case illustrated the shortcomings of existing legislation in dealing with emerging cybercrimes and contributed directly to the promulgation of the Computer Misuse Act 1990 which criminalized unauthorized computer data access and modification (Lloyd, 2011).

2. **R v Whitely** (1991):

   The case of R v Whitely convicted the defendant under the Criminal Damage Act for changing computer files on a university's machine without permission. Whiteley's actions included the deletion of data and created functional disruptions but not hardware damage. This case was very important because it brought to light the problem of how to fit computer-related offences into damage laws, which generally dealt with tangible property (Rowland & Macdonald, 2000). The court ruling also underscored how laws specific to digital offences are critical and how this is why special laws, like the Computer Misuse Act, are needed to adequately cover offences related to cyber.

3.2 Comparative Overview with the EU Framework

The European Union's regulatory framework (and in particular GDPR)) has had a huge impact on the UK’s data protection laws. The UK's departure from the EU doesn't change that: GDPR principles are still having an influence on UK data protection standards in the form of the DPA 2018. This chapter digs into the differences & similarities between UK and EU data protection laws and considers the reverberations of Brexit upon compliance requirements.

3.2.1 Differences and similarities with EU data protection laws.

Similarities

The UK’s Data Protection Act 2018 is based on the GDPR and is very similar to the GDPR in its nature. Both the DPA and GDPR share common core principles that provide guarantees that personal data is processed in a lawful, fair, transparent and minimally intrusive way. About granting individuals the same rights such as the right to access, rectify, delete, and restrict the processing of data, both frameworks are the same (Lloyd, 2011). Also, they are subject to identical requirements for consent, data breach notifications and where appropriate appointment of data protection officers (DPOs).

Differences

Nevertheless, UK and EU data protection frameworks have several similarities but also some differences. Specific exemptions for UK interests, including greater flexibility in processing personal data for immigration and national security reasons (Rowland & Macdonald, 2000), are

introduced to the DPA. This also means the Information Commissioner's Office (ICO) in the UK — the national regulator — has more powers than its counterparts in other EU member states and will be able to pursue data breaches more aggressively in the territories of which it (UK) is responsible.

3.2.2 Impact of Brexit on data protection compliance.

The uncertainty surrounding data protection compliance between the UK and the EU was brought in by Brexit. While the UK still holds principles set by GDPR through their DPA, they have left the EU, and as such there is a new regulatory environment in the UK. As a result of the post-Brexit, the UK is now an 'EU third country' and thus, data transfers from the EU to the UK must meet the EU's adequacy requirements. This was granted by the European Commission to the UK in June 2021 and allows UK – EU data transfers to flow freely provided certain conditions are met (European Commission, 2021).

However, this adequacy decision is conditional and therefore UK based organisations need to keep track to remain compliant, especially where cross-border data is involved. If adequacy status was later revoked, organizations would be required to transfer EU personal data lawfully using an alternative mechanism, such as SCCs or BCRs (Lloyd, 2011).

The UK has expressed an interest in moving towards a data protection regime 'made in the UK' which may differ increasingly from EU standards over time. This could bring with it compliance risks for businesses, as a significant divergence from GDPR could have a 'domino effect' on

future adequacy decisions, meaning companies doing business between the EU and UK could be hit with tougher data processing requirements.

4. Analysis: Analysis of Relevant Case Laws

In this section, the effectiveness of the present UK data privacy agency is critically examined to find how well current law and enforcement mechanisms deal with data protection issues.

4.1 Data Privacy Legislation Effectiveness

4.1.1 Evaluation of existing laws and their enforcement

The overarching data privacy legislation in the UK is the DPA 2018, which is in compliance with the GDPR and lays high standards to keep personal data safe. The DPA sets out specific rules for how data must be processed by organizations which must also be aware of individuals' rights as well as their responsibilities. As a result of these standards having to be enforced by the Information Commissioner's Office (ICO), there has been a greater awareness and responsibility over how people handle data, resulting in huge fines to organizations that fail to comply (ICO, 2018).

Several recent instances where large corporations have been fined communications watchdog the ICO for data breaches, which show the body can strongly enforce these new powers. For example, British Airways was fined £20 million for not protecting their customer's personal and financial data from over 400,000 customers (ICO, 2020), which proves that the ICO is dedicated

to maintaining data security. Greatly proactive this has been with organizations' care for improving data treatment and refocusing their cybersecurity measures so as not to face penalties.

4.1.2 Gaps in data protection, and challenges in regulatory compliance

Although the DPA is organized well, it still contains gaps protecting data. There is one significant gap; for example, in emerging data processing technologies, such as artificial intelligence (AI) and machine learning, which operate by processing and analyzing enormous datasets which often include sensitive personal information. These developments fall into areas that have not been fully accounted for by the current legislation, resulting in ambiguities concerning compliance requirements as well as difficulty for organizations seeking to understand how these technologies may be legally used (2000, Rowland & Macdonald).

The provisions for the DPA allow for law enforcement and national security reasons, however, this is narrowly drawn and can lead to inconsistencies in how data protection applies across different sectors (Lloyd, 2011).

A particular problem for many Small and medium-sized enterprises (SMEs) is that it can prove difficult to allocate the required funds and expertise to adequately meet the demands of complicated data protection requirements creating a disparity in levels of compliance between industries. In addition, Brexit has created additional uncertainty for companies processing the EU Citizens' data, which should meet the GDPR standards, thus creating another level of regulatory complexity (European Commission, 2021).

4.2 Public Surveillance and Privacy Trade-offs

This section explores the conflict between competing interests in this field and examines key case law that sets out how UK courts have read and applied surveillance laws in that context.

4.2.1 Balancing state security needs vs. individual privacy rights

Surveillance technology in UK public spaces is at a high level. CCTV cameras monitor crowded places while ANPR and digital tracking tools detect criminal activities. These powerhouses are critical enablers to national security operations, furnishing law enforcement agencies with real-time information that helps prevent, as well as investigate crimes. Conversely, such widespread exposure may increase the incidence of monitoring which can diminish a person's privacy and have a ‘chilling effect’ in which the existence of excessive surveillance discourages persons from acting freely due to fear of the constant eye (Rowland & Macdonald, 2000).

The laws governing lawful surveillance were set out in the RIPA 2000 and the Investigatory Powers Act 2016 (IPA) but their wide government powers have been a cause for concern over how far is too far into civil rights. Some proponents argue that surveillance is a vital instrument in national security, hindering crime as well as securing the public's safety in the existing context of security threats (Lloyd, 2011).

4.2.2 Case law examples and analysis

1. **R v A and B** (2008):

   In R v A and B two individuals brought a challenge to their conviction under RIPA because their Convention rights under Article 8 European Commission of Human Rights (ECHR) had been infringed. Covert surveillance without clear authorisation was at the heart of the case. Surveillance is permitted under RIPA but the use of it must be proportionate to the end in view and conform with human rights standards, the court ruled. The principle of proportionality is reinforced in this case, since surveillance should only be adopted in measures that are necessitated by the security requirements but without that by which the privacy rights of individuals are unduly affected (Easton, 2007).

2. **Big Brother Watch and Others v United Kingdom** (2018)

   The practices authorized by the IPA were the subject of a landmark case brought to the European Court of Human Rights, Big Brother Watch and Others v United Kingdom. But the applicants said the law allowed a blanket authorisation for indiscriminate interception of communications in breach of the right to privacy, freedom of expression and the right to access information. The Court said insufficient safeguards against arbitrary interference existed in some provisions of the IPA, notably on bulk data collection and weak oversight measures. This decision showed that privacy rights needed to be protected by the comprehensive safeguards contained in the law on surveillance,

particularly where extensive surveillance techniques (European Court of Human Rights, 2018).

3. **R (on the application of Bridges) v Chief Constable of South Wales Police** (2020) South Wales Police used facial recognition technology to identify individuals in public spaces and this case addressed that. Mr. Public member, Bridges, challenged that this technology was legal under data protection and human rights laws. The police had not assessed the proportionality and necessity of using facial recognition in a way to caused privacy violations, so the court ruled in favour of Bridges. The fact that this case recognized the need for conducting in-depth impact assessments before deploying surveillance technology is an important facet; the principle that state security efforts should not unnecessarily impinge upon the individual's right to privacy except where justified and protected by effective safeguards (Lloyd, 2011).

4.3 Global Perspectives and Influence on UK Law

European Union regulations have been a factor and so have the broader international developments in the UK's approach to data protection and surveillance. This includes a discussion on the effect key international regulations, in particular the GDPR, have had on UK law and the impact of global surveillance practices on privacy and security policies in the UK.

4.3.1 Influence of international regulations (e.g., GDPR) on UK law

In 2018, the GDPR passed into effect for the entire European Union, largely affecting the UK's data protection laws. The GDPR was initially created as an EU regulation and is now in the UK as part of the DPA 2018. The strict requirement of the handling of data, consent, and individual rights of the GDPR led to another benchmark that the UK adopted a similarly rigorous regulatory framework to protect personal data (Lloyd, 2011).

Despite Brexit, the UK still upholds GDPR principles because the EU (European Commission, 2021), through the adequacy decision in June 2021 (GDPR, 2021) allows free passage of data between the EU and the UK on condition that the UK maintains the same data protection standards. It gives UK businesses access to EU data markets whilst creating an environment for international data transfers to be compatible. Yet the future divergence between the UK and GDPR could mean the adequacy status would no longer hold, and it was up to the UK to stay on the right side of the global data protection jurisprudential scale.

Beyond the EU, the impact of GDPR has also been felt throughout Japan, Brazil, and South Korea when they recently passed data protection laws themselves. In turn, this global move toward GDPR-like standards has reiterated the need for high data protection standards in the UK, meaning UK-based organisations can continue to follow industry standards and streamline global data flows unhindered (ICO, 2018).

4.3.2 Implications of global surveillance practices on UK policies

Global surveillance practices have immensely influenced and altered UK policies on privacy and security. The United States and China have created complex surveillance systems, which they justify in terms of domestic national security, and which are frowned upon as violations of individual privacy. It has emerged that international trends of robust monitoring capabilities in response to global security threats shape the surveillance framework in the UK including the IPA 2016 (Easton, 2007).

Former National Security Agency contractor Edward Snowden's 2013 revelations about government data collection programs (including the USA's PRISM) made the extent of government surveillance the source of a huge amount of attention. In response to perceived gaps in existing legislation the IPA 2016, often referred to as the 'Snooper's Charter,' was introduced to expand government powers, so that revelations such as these brought on changes in the UK's surveillance law. Under the Act bulk data collection and extensive surveillance are authorized which parallels global trends in state monitoring but causes privacy advocates concern (Lloyd, 2011).

The implication of these practices continues to feature in the array of UK policy interests in international forums where the UK is frequently questioned over how its surveillance policies conform to human rights standards. Calls for stronger oversight and accountability mechanisms which would maintain UK security while limiting surveillance to comply with privacy standards, however, have been made in the UK, informed by this international perspective.

5. Conclusion

The Data Protection Act 2018 and the Regulation of Investigatory Powers Act 2000 provide the legal basis on which data privacy and public surveillance in the UK are governed – juggling the competing demands of upholding individual rights and protecting national security. Influenced by the GDPR considerably, the DPA has set a high bar for data protection and provides a wide range of rights for individuals concerning their personal information and strong obligations for organizations using that information. Laws that govern public surveillance, like RIPA and Investigatory Powers Act, are also state's behaviour demonstrating the use of surveillance in service of public safety and crime prevention.

The analysis, however, emphasizes the gaps and difficulties of the applicability of this framework. The DPA provides wide guidelines on data protection but new technologies such as AI and machine learning raise complexities not currently covered by prevailing laws. However, it is also the case that the UK's regulatory environment experiences difficulties in ensuring consistency across sectors with data protection enforcement, with smaller organisations being less resourced to comply with compliance. Furthermore, the influence of Brexit has added yet more compliance uncertainties because the UK is still awaiting an adequacy status determination from the EU.

The case law analysis reveals that the judiciary takes a clear position in the surveillance stream when it comes to controlling proportionality and oversight, to prevent surveillance practices from violating privacy rights without proportional justification. But, while these laws remain, there is still a worry about the wide-ranging powers that the Investigatory Powers Act and others grant to the government and a pressing need for strict accountability safeguards and guarantees.

However, changing these requirements may require the UK to adapt its legal framework to meet these altering challenges, including how data privacy and surveillance are applicable in an ever-changing digital setting. Some of the work required could involve updating current legislation, more detailed guidelines on new technologies being introduced and taking on a balanced approach to international regulatory alignment. With technology transforming society, having a legal system that evolves with the times and can protect the rights of individuals and foster public trust in the digital age will be imperative.

6. References

ANPR. (2005). *Strategy for the Police Service 2005–8*. Association of Chief Police Officers.

BBC News. (2006). *Britain is 'Surveillance Society'*. http://news.bbc.co.uk/1/hi/uk/6108496.stm

Easton, M. (2007). *Whitehall Plan for Huge Database*. BBC News.

Edwards, C., & Savage, N. (1986). *Information Technology & the Law*. MacMillan Publishers.

European Commission. (2021). *Commission Implementing Decision on the adequate protection of personal data by the United Kingdom*. https://ec.europa.eu

European Court of Human Rights. (2018). *Big Brother Watch and Others v United Kingdom*. https://www.echr.coe.int

ICO. (2006). *A Surveillance Society*. https://www.ico.gov.uk

ICO. (2018). *Guide to the General Data Protection Regulation (GDPR)*. https://ico.org.uk

ICO. (2020). *ICO issues fine to British Airways*. https://ico.org.uk

Lloyd, I. (2011). *Information Technology Law* (6th ed.). Oxford University Press.

Rowland, D., & Macdonald, E. (2000). *Information Technology Law*. Cavendish Publishing Limited, UK.

The Scotsman. (n.d.). *The Intelligence and Security Committee's report on the 2005 bombings*. http://thescotsman.scotsman.com/londonbombings/MI5-spied-on-only-one.5282797.jp