

INTERNATIONAL JOURNALOF LAW AND CONSTITUTION STUDY

Journal home page:https://jurnal.asrypersadaquality.com/index.php/ijlacos

DIGITAL SURVEILLANCE AND THE EXCLUSIONARY RULE IN CONTEMPORARY EVIDENCE LAW

Mirale Harahap, Mhd. Irsan Akbar, Dycky Alamsyah Pardede, Rizky Zaidan Ketaren

Islamic Criminal Law, Faculty of Sharia and Law, State Islamic University of North Sumatra

miraharahap205@gamil.com,irsannakbarr19@gmail.com,dickyalamsyahpardede17@gmail.com, rzaidanketaren@gmail.com

ABSTRACT

The massive digital transformation has brought significant changes to law enforcement practices and evidentiary systems in modern justice. The use of digital surveillance, such as electronic communication interception, social media monitoring, location tracking, metadata analysis, and other electronic data collection, is increasingly becoming a crucial tool in uncovering crimes. However, the use of this technology also raises complex legal issues, particularly regarding the protection of privacy rights, civil liberties, and the legitimacy of evidence obtained through digital surveillance mechanisms. In the context of contemporary evidentiary law, the exclusionary rule doctrine serves as a legal instrument that limits the use of evidence obtained unlawfully or through actions that violate an individual's constitutional rights. This study aims to analyze the urgency of applying the exclusionary rule to evidence generated through digital surveillance and examine the balance between law enforcement interests and human rights protection. The research method used is normative legal research with statutory, conceptual, and comparative approaches. The results of the study indicate that the development of digital technology demands clearer legal standards regarding the procedures for obtaining, managing, and using electronic evidence. The application of the exclusionary rule is an important mechanism to prevent abuse of authority in digital surveillance while maintaining the integrity of the judicial process. Therefore, strengthening regulations and effective supervision is needed to ensure that the use of technology in providing evidence remains in line with the principles of the rule of law, protection of privacy rights, and procedural justice in the digital era.

KEYWORDS

Digital Surveillance, Exclusionary Rule, Law of Evidence, Electronic Evidence, Right to Privacy, Human Rights, Procedural Justice.

Corresponding Author: Dycky Alamsyah Pardede

Article History	Submitted: March 16, 2026	Revision: March 18, 2026	Accepted: March 30, 2026	Published: July 30, 2026

https://doi.org/10.63736/ijlacos.v3i1

INTRODUCTION

The development of digital technology in recent decades has fundamentally changed the way society communicates, interacts, and stores information. Digitalization has not only impacted the economic, educational, and government sectors but has also had a significant impact on the criminal justice system and the law of evidence. The presence of the internet, smart devices, social media, artificial intelligence, cloud computing, and big data technology has generated enormous volumes of data that continue to increase daily. This digital data has ultimately become a valuable source of information in law enforcement processes, particularly in uncovering various forms of modern crime that are increasingly complex and technology-based (Mason & Seng, 2021).

In the context of law enforcement, the development of digital technology has encouraged the use of various forms of digital surveillance as a means of obtaining information and evidence. Digital surveillance encompasses various methods, such as electronic communication interception, location tracking via Global Positioning System (GPS), monitoring social media activity, collecting communication metadata, using facial recognition technology, and analyzing electronic data stored on digital devices and internet network systems (Solove, 2008). The use of this technology is considered capable of increasing the effectiveness of law enforcement officers in identifying perpetrators, collecting evidence, and uncovering criminal networks that are difficult to reach through conventional investigative methods.

The urgency of using digital surveillance is increasing with the development of various forms of transnational crime and cybercrime that exploit advances in information technology. Crimes such as computer system hacking, personal data theft, electronic fraud, drug trafficking through digital platforms, money laundering, and even acts of terrorism are now often carried out using electronic means that are difficult to track without the support of digital surveillance technology (Brenner, 2012). In such conditions, the state has a legitimate interest in utilizing surveillance technology as an instrument to maintain national security, public order, and the effectiveness of law enforcement.

However, the use of digital surveillance also raises various legal and ethical issues. Excessive surveillance or surveillance without a clear legal basis has the potential to violate an individual's right to privacy, which is a universally recognized human right. The right to privacy relates not only to the protection of one's private life but also to the protection of personal data, communications, and individual freedom from arbitrary interference by the state or other parties (Westin, 1967). In a democratic society, the right to privacy is seen as a crucial element in guaranteeing individual freedom and preventing the abuse of power.

The debate over the boundaries between law enforcement and privacy protection has become increasingly prominent as technology's ability to collect and analyze massive amounts of data increases. Technological advances have enabled both governments and private entities to monitor individual activities on an unprecedented scale. This phenomenon has raised concerns about the emergence of a surveillance society, a situation where people's activities are constantly monitored, potentially threatening civil liberties and democratic principles (Lyon, 2018). Therefore, the use of digital surveillance technology requires clear legal regulations to prevent violations of citizens' fundamental rights.

From the perspective of evidentiary law, the issues that arise relate not only to the protection of privacy rights but also to the legality of evidence obtained through digital surveillance. Modern evidentiary systems require that evidence presented in judicial proceedings be not only relevant and have strong probative value, but also obtained through legally valid procedures. The principle of legality in obtaining evidence is a key pillar of a fair trial system, as it aims to prevent abuse of authority by law enforcement officials (LaFave et al., 2020).

In this regard, the exclusionary rule doctrine has developed in modern legal systems. This doctrine essentially stipulates that evidence obtained through unlawful means or in violation of a person's constitutional rights cannot be used in judicial proceedings. The application of the exclusionary rule first developed significantly in the

United States legal system through various court decisions that emphasized the importance of protecting citizens' constitutional rights, particularly regarding the prohibition of unreasonable searches and seizures (Dressler & Thomas, 2021).

The primary purpose of the exclusionary rule is not merely to protect the accused, but rather to maintain the integrity of the justice system and provide a deterrent effect against unlawful acts committed by law enforcement officers. Through this doctrine, the state is not permitted to profit from unlawful actions in the process of gathering evidence. Thus, the application of the exclusionary rule reflects the principle that law enforcement must be conducted based on the law and must not sacrifice the fundamental rights of individuals to achieve the goal of punishment (Kerr, 2018).

The development of digital technology presents new challenges in the application of the exclusionary rule. The ease of copying, transferring, modifying, and storing digital evidence in various virtual locations makes the process of assessing the legality of evidence acquisition increasingly complex. In many cases, digital evidence is obtained through surveillance mechanisms involving sophisticated technology and large amounts of data collection, making it difficult to draw a clear line between legitimate actions and those that violate privacy rights (Mason & Seng, 2021).

In many countries, courts face the challenge of adapting traditional evidentiary law principles to the realities of digital technology. Modern court decisions demonstrate a trend toward greater protection of personal data and electronic communications, while still considering the state's need to investigate serious crimes (Kerr, 2010). These developments demonstrate that the relationship between digital surveillance and the exclusionary rule is a central issue in contemporary evidentiary law.

In Indonesia, recognition of electronic evidence has strengthened following the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions, which was later amended by Law Number 1 of 2024. This regulation affirms that electronic information and electronic documents can be used as valid legal evidence in judicial proceedings. Furthermore, the enactment of Law Number 27 of 2022 concerning Personal Data Protection demonstrates the state's commitment to providing stronger protection for people's privacy rights in the digital era. However, regulations regarding the legal consequences of evidence obtained through unlawful

digital surveillance are still not comprehensively regulated in the Indonesian legal system.

This situation raises various issues in judicial practice, particularly when judges are confronted with digital evidence relevant to proving a crime but obtained through procedures of questionable legality. The debate over whether such evidence can still be used for law enforcement purposes or should be excluded to protect human rights demonstrates the importance of a more in-depth study of the relationship between digital surveillance and the exclusionary rule in the context of modern evidentiary law.

Based on this background, this study aims to analyze the application of digital surveillance in contemporary evidentiary processes, examine the relevance of the exclusionary rule doctrine to evidence obtained through digital surveillance, and formulate a legal regulatory concept that can balance the interests of law enforcement with the protection of privacy and human rights. This study is expected to provide academic contributions to the development of evidentiary law in the digital era and serve as a reference for policymakers in formulating regulations that are adaptive to developments in information technology.

RESEARCH METHODS

This research employs a normative legal research method, focusing on analyzing the legal norms governing the use of digital surveillance and the application of the exclusionary rule in contemporary evidentiary law. This method was chosen because it aims to examine the concepts, principles, doctrines, and legal provisions relating to the legality of collecting and using digital evidence in judicial proceedings. This approach allows researchers to analyze the alignment between developments in digital surveillance technology and the principles of human rights protection, privacy rights, and procedural justice in modern legal systems (Marzuki, 2021).

The approaches used in this research include a statutory approach, a conceptual approach, and a comparative approach. The statutory approach is carried out by examining various regulations related to the law of evidence, electronic evidence, personal data protection, and digital surveillance. In the Indonesian context, the regulations that are the object of study include Law Number 1 of 2024 concerning the

Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, the Criminal Procedure Code (KUHAP), and various other relevant regulations. Meanwhile, the conceptual approach is used to analyze the concepts of digital surveillance, the right to privacy, electronic evidence, due process of law, and the doctrine of the exclusionary rule that have developed in legal theory and modern judicial practice. The comparative approach is carried out by comparing the regulations and implementation of the exclusionary rule in several countries, particularly the United States and countries that have developed regulations related to digital privacy protection and electronic evidence.

The legal sources used in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations, court decisions, and international legal instruments related to privacy rights and digital evidence. Secondary legal materials consist of law books, scientific journal articles, research results, and other academic works discussing digital surveillance, the law of evidence, and the exclusionary rule. Tertiary legal materials include legal dictionaries, legal encyclopedias, and other reference sources that support understanding of the concepts studied.

The legal material collection technique was conducted through library research, namely by identifying, inventorying, and reviewing various literature relevant to the research object. All collected legal materials were then analyzed using qualitative analysis methods with a descriptive-analytical approach. The analysis was carried out through a process of legal interpretation, systematization of norms, and evaluation of the application of legal principles related to the use of digital surveillance in the evidentiary process. The results of the analysis were then used to formulate legal arguments regarding the importance of implementing the exclusionary rule as an instrument for protecting privacy rights and guaranteeing justice in the contemporary evidentiary system.

Through this method, this research is expected to provide a comprehensive understanding of the relationship between digital surveillance and exclusionary rules,

while also offering relevant legal recommendations for the development of an evidence system that is adaptive to technological advances without ignoring the principles of the rule of law and the protection of human rights.

RESULTS AND DISCUSSION OF RESULTS

1. Digital Surveillance and the Exclusionary Rule in Contemporary Evidence Law

Based on a study of various regulations, legal doctrines, and developments in modern judicial practices, it was found that the use of digital surveillance has become an integral part of the contemporary evidentiary system. Advances in information technology enable law enforcement officials to obtain various forms of electronic evidence that were previously difficult to access through conventional investigative methods. Evidence obtained through digital surveillance includes electronic communication recordings, location data, social media activity, metadata, network-based CCTV recordings, and various other forms of digital data relevant to proving a crime.

Research shows that the use of digital surveillance significantly contributes to the effectiveness of law enforcement, particularly in handling crimes that utilize information technology, such as cybercrime, money laundering, corruption, human trafficking, and terrorism. Digital evidence obtained through electronic surveillance mechanisms is often the primary evidence in identifying perpetrators, reconstructing criminal events, and proving the link between the perpetrator and the crime.

However, this study also found that the use of digital surveillance raises complex legal issues related to the protection of privacy rights and the legality of obtaining evidence. The ability of technology to access, record, store, and analyze large amounts of personal data opens the opportunity for violations of citizens' constitutional rights if not accompanied by adequate oversight mechanisms. In some cases, electronic data collection is carried out without the consent of data subjects, without the permission of competent authorities, or without a clear legal basis, raising doubts about the validity of the evidence obtained.

This research found that the development of digital surveillance technology has not always been accompanied by regulatory developments that provide clear boundaries for procedures for obtaining electronic evidence. Consequently, debate has arisen over whether evidence obtained through methods that violate privacy rights can still be used in the evidentiary process for law enforcement purposes or should instead be excluded to protect individual rights.

In this regard, research results indicate that the exclusionary rule doctrine plays a crucial role in maintaining a balance between effective law enforcement and human rights protection. This doctrine asserts that evidence obtained through actions that violate the law or violate a person's constitutional rights should not be used in judicial proceedings. In the context of digital surveillance, the application of the exclusionary rule serves as a control instrument for law enforcement officers to ensure they remain within the law when collecting digital evidence.

Furthermore, research findings indicate that countries that have more thoroughly implemented the exclusionary rule tend to have stronger privacy protection mechanisms in the evidentiary process. Courts not only assess the relevance and probative value of evidence but also the legality of the method of obtaining it. Thus, privacy protection is positioned as an integral part of a fair trial system.

In the Indonesian context, research has found that electronic evidence has been legally recognized as valid evidence through the Electronic Information and Transactions Law and various other related regulations. However, there is no explicit and comprehensive regulation governing the application of the exclusionary rule to digital evidence obtained unlawfully. This situation has led to inconsistent judicial practice when dealing with electronic evidence obtained through supervisory mechanisms whose legality is questionable.

The research also shows that Indonesian evidence law still focuses more on the probative value of the evidence presented than on the legality of the process by which it was obtained. Consequently, there is the potential for the use of substantively

relevant evidence obtained through procedures that violate the principles of privacy and human rights protection. This situation has the potential to create legal uncertainty and diminish the guarantee of protection for citizens' constitutional rights in the digital age.

Based on these findings, this study concludes that the development of digital surveillance has significantly contributed to the effectiveness of contemporary evidentiary systems, but at the same time increases the risk of privacy violations. Therefore, a legal mechanism is needed to ensure that the use of digital surveillance technology is carried out proportionally, accountably, and in accordance with the principles of the rule of law. In this regard, the exclusionary rule is a relevant instrument for strengthening human rights protection while maintaining the integrity of the justice system in facing evidentiary challenges in the digital era.

DISCUSSION

1. Transformation of Evidence Law in the Digital Era

Advances in information technology have transformed the way the judicial system understands and uses evidence. In conventional evidentiary systems, evidence is generally physical and obtained through traditional investigative methods. However, the digital transformation has produced new forms of evidence derived from electronic activity, such as instant messages, emails, digital communication records, location data, electronic transactions, and social media activity. These changes demonstrate that evidentiary law must adapt to technological developments to remain relevant to the needs of modern law enforcement (Mason & Seng, 2021).

Digital evidence has distinct characteristics compared to conventional evidence. Digital data can be stored in large quantities, transferred rapidly, replicated without altering its original form, and stored in multiple locations without being limited by a specific geographic region. These characteristics provide advantages to the evidentiary process by enabling a more detailed and objective reconstruction of the facts. However, these characteristics also pose challenges related to authentication, data integrity, and the legality of the collection process (Kerr, 2018).

In this context, digital surveillance is becoming an increasingly important instrument in supporting the evidentiary process. Digital surveillance enables law

enforcement officials to obtain information unavailable through conventional investigative methods. Therefore, the development of digital surveillance is inseparable from the transformation of contemporary evidentiary law, which increasingly relies on digital data and technology.

2. Concept and Scope of Digital Surveillance

Conceptually, digital surveillance is the activity of monitoring, collecting, analyzing, and storing electronic data for specific purposes, including law enforcement and national security. Forms of digital surveillance can include electronic communication interception, social media monitoring, device location tracking, communication metadata analysis, the use of biometric technology, and the use of artificial intelligence to identify individual behavioral patterns (Lyon, 2018).

Technological advances have expanded the state's ability to monitor public activity. While previously surveillance was limited to specific individuals suspected of committing crimes, technology now allows for large-scale data collection on a much wider population. This phenomenon is known as mass surveillance, the practice of systematically gathering information on large numbers of individuals without necessarily being based on specific suspicions (Solove, 2008).

From a law enforcement perspective, this capability offers significant benefits by enabling early detection of various security threats and criminal acts. However, from a human rights perspective, overly broad surveillance has the potential to violate the rights to privacy, freedom of expression, and freedom of communication. Therefore, the use of digital surveillance must always be balanced with effective legal oversight mechanisms to prevent it from becoming an instrument of abuse of power.

3. The Right to Privacy as a Fundamental Right in the Digital Age

The right to privacy is a fundamental right recognized in various international and national human rights instruments. In modern developments, the concept of privacy is no longer limited to protecting one's personal space, but also encompasses the protection of personal data, electronic communications, digital identities, and various

information related to an individual's life (Westin, 1967).

The development of information technology has led to an increase in the amount of personal data generated by each individual. Activities such as using a mobile phone, accessing the internet, conducting electronic transactions, or interacting through social media automatically generate data that can be recorded and analyzed. This data not only describes a person's activities but can also be used to identify behavioral patterns, personal preferences, and even social relationships (Solove, 2008).

In this context, privacy violations do not always occur through direct disclosure of information, but can also occur through data collection processes conducted without consent or without a clear legal basis. Therefore, protecting privacy rights in the digital age must be understood as protecting the entire data management cycle, from data collection, storage, use, and even deletion.

The right to privacy is crucial in a democratic state governed by the rule of law because it serves as a constraint on state power. Without adequate protection, the state's ability to conduct digital surveillance could lead to practices that violate the principles of freedom and respect for human dignity.

4. Exclusionary Rule as an Instrument of Power Control

The exclusionary rule doctrine developed as a mechanism to prevent abuse of authority by law enforcement officials. The basic principle of this doctrine is that evidence obtained through unlawful means may not be used in judicial proceedings (LaFave et al., 2020).

Theoretically, this doctrine is based on the idea that the ends of law enforcement cannot justify the means. The state must respect the law even while attempting to enforce it. If evidence obtained through violations of the law can still be used, there is insufficient incentive for law enforcement officials to comply with established procedures (Dressler & Thomas, 2021).

In the context of digital surveillance, the exclusionary rule becomes increasingly important because technology provides a vast amount of access to individuals' personal information. Without clear restrictions, there is a risk that law enforcement will over-collect data for investigative purposes.

The application of the exclusionary rule conveys the message that human rights

protection is an integral part of the justice system. Therefore, the success of law enforcement is measured not only by the ability to identify perpetrators of crimes, but also by adherence to legal principles in the process of obtaining evidence.

5. The Relevance of the Exclusionary Rule to Evidence from Digital Surveillance Results

In the digital era, the relationship between digital surveillance and the exclusionary rule has become increasingly intimate. Digital surveillance often yields evidence of high probative value, but the process of obtaining it does not always comply with applicable legal standards. This situation raises questions about whether such evidence can still be used for law enforcement purposes or should be excluded to protect individual rights.

The application of the exclusionary rule in the context of digital evidence serves several important functions. First, it protects individuals' privacy rights from arbitrary surveillance. Second, it encourages law enforcement officials to comply with legal procedures in conducting investigations. Third, it maintains the legitimacy of the judicial system by ensuring that court decisions are not based on evidence obtained through unlawful means (Kerr, 2018).

Furthermore, this doctrine also plays a role in creating a balance between state interests and individual interests. The state remains authorized to conduct digital surveillance, but this authority must be exercised in accordance with the principles of legality and respect for human rights.

6. Challenges of Implementing the Exclusionary Rule in Indonesia

Indonesia has recognized electronic evidence as valid evidence through various regulations, particularly the Electronic Information and Transactions Law. However, no regulation explicitly adopts the exclusionary rule doctrine, as recognized in common law legal systems.

As a result, judicial practice still finds differing approaches to assessing evidence obtained through mechanisms whose legality is questionable. Some decisions emphasize the relevance and probative value of the evidence, while others also consider the legality of the acquisition process. This situation demonstrates the need to establish clearer legal standards regarding the relationship between the legality of evidence collection and its admissibility in the judicial process (Marzuki, 2021).

Another challenge is that technology advances much faster than regulatory development. New forms of digital surveillance often emerge before specific regulations govern them. Therefore, the legal system must have sufficient flexibility to adapt to technological developments without sacrificing legal certainty.

7. The Urgency of Reforming Evidence Law in the Digital Era

Based on research findings, reform of evidence law is an urgent need to address the development of digital technology. This reform not only relates to the recognition of electronic evidence as valid evidence but also encompasses regulations regarding the procedures for obtaining, managing, storing, and using digital evidence in judicial proceedings.

Implementing principles consistent with the exclusionary rule could be one solution to strengthen privacy protection and enhance the accountability of law enforcement officials. Clear regulations regarding digital surveillance procedures would provide legal certainty for law enforcement officials, judges, and the public.

Ultimately, contemporary evidentiary law must strike a balance between two equally important interests: effective law enforcement and the protection of human rights. Technological advancements should not be a justification for diminishing the protection of citizens' fundamental rights. Instead, technological developments must be accompanied by legal developments that ensure that technology's use remains within the bounds of justice, legal certainty, and respect for human dignity (LaFave et al., 2020).

CONCLUSION

The development of information and communication technology has brought significant changes to the evidentiary system in criminal procedure law. The presence of digital surveillance as an instrument for gathering information and evidence has expanded the ability of law enforcement officials to uncover various forms of modern

crime, particularly cybercrime, terrorism, money laundering, corruption, and other transnational crimes. Electronic evidence generated through digital surveillance mechanisms has high evidentiary value because it can record facts more objectively, accurately, and measurably than some forms of conventional evidence. The recognition of electronic evidence in the Indonesian legal system demonstrates that evidentiary law has adapted to technological developments and the needs of contemporary law enforcement.

However, this study found that the use of digital surveillance not only provides benefits for law enforcement but also poses serious challenges to the protection of privacy and human rights. The technology's ability to access, collect, store, and analyze personal data on a large scale has the potential to violate citizens' constitutional rights if not accompanied by a clear legal basis, effective oversight mechanisms, and proportionate restrictions. Therefore, the use of digital surveillance technology must always be implemented based on the principles of legality, necessity, proportionality, accountability, and respect for human rights.

This research also shows that the exclusionary rule doctrine has crucial relevance in contemporary evidentiary law. This doctrine serves as a mechanism to prevent the use of evidence obtained through actions that violate the law or an individual's constitutional rights. In the context of digital surveillance, the application of the exclusionary rule aims not only to protect privacy rights but also to maintain the integrity of the judicial system, promote the professionalism of law enforcement officers, and ensure that the law enforcement process continues to run according to the principle of due process of law. Digital evidence obtained through illegal wiretapping, unauthorized data access, or other unlawful methods essentially has the potential to lose its evidentiary value because it violates the principle of procedural fairness.

In the Indonesian context, although electronic evidence has received legal recognition through the Electronic Information and Transactions Law and various other regulations, the application of the exclusionary rule has not been explicitly and

comprehensively regulated in criminal procedure law. Consequently, legal uncertainty remains in determining whether digital evidence obtained through unlawful procedures is admissible or should be excluded in the judicial process. This situation demonstrates the need for reform of evidence law that is more responsive to developments in digital technology and places greater emphasis on the legality of the evidence acquisition process.

Based on the overall research results, it can be concluded that the relationship between digital surveillance and the exclusionary rule reflects the need to balance two equally important interests: the effectiveness of law enforcement and the protection of human rights. The ideal contemporary evidentiary system is not only one capable of discovering material truth through the use of digital technology, but also one that ensures that all evidence is obtained legally, respects the right to privacy, and complies with the principles of the rule of law and justice. Therefore, strengthening regulations regarding digital surveillance, personal data protection, and the application of the exclusionary rule principle are important steps in realizing a modern, just criminal justice system oriented toward protecting citizens' constitutional rights in the digital era.

REFERENCE

Brenner, S. W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. Northeastern University Press. https://www.upne.com/9781555538332/cybercrime-and-the-law/

Dressler, J., & Thomas, G. C. (2021). *Criminal procedure: Principles, policies and perspectives* (7th ed.). West Academic Publishing. https://subscription.westacademic.com/

Indonesia. (2008). *Law Number 11 of 2008 concerning Electronic Information and Transactions*. https://peraturan.bpk.go.id/Home/Details/37589/uu-no-11-tahun-2008

Indonesia. (2022). *Law Number 27 of 2022 concerning Personal Data Protection*. https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022

Indonesia. (2024). *Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions*.

https://peraturan.bpk.go.id/Home/Details/287162/uu-no-1-tahun-2024

Kerr, O. S. (2010). Applying the Fourth Amendment to the Internet: A general approach. *Stanford Law Review, 62*(4), 1005–1046. https://www.stanfordlawreview.org/print/article/applying-the-fourth-amendment-to-the-internet-a-general-approach/

Kerr, O. S. (2018). *Computer crime law* (4th ed.). West Academic Publishing.

LaFave, W. R., Israel, J. H., King, N. J., & Kerr, O. S. (2020). *Criminal procedure* (7th ed.). West Academic Publishing.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Marzuki, P. M. (2021). *Legal research* (Revised ed.). Kencana.

Mason, S., & Seng, D. (2021). *Electronic evidence and electronic signatures* (6th ed.). Institute of Advanced Legal Studies. https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-evidence-and-electronic-signatures-6th-edition

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.