IJCCJ
Indonesian Journal of Crime and Criminal Justice

Vol. 1 No. 3. November 2025. pp. 312-357 E-ISSN: 3108-9852 https://doi.org/10.62264/ijccj.v1i3.193

Reformulation of Wiretapping Regulations Based on Criminal Justice Reform: Lessons from US dan UK

Mohamad Mahdy [a,b*], Isharyanto Isharyanto [b], Hartiwiningsih Hartiwiningsih [b] Sobirov Bobur Baxtishodovich [c]
[a] Attorney General's Office of the Republic of Indonesia, Jakarta, Indonesia
[b] Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia
[c] Visiting Scholar, College of Business, University of Wyoming, United States
* corresponding author: mohamad.mahdy27@gmail.com

ARTICLE INFO

Article History:

Received: 21 August 2025
Revised: 25 September 2025
Revised: 19 October 2025
Accepted: 27 October 2025

Keywords:

Wiretapping;
Criminal Justice Reform;
Human Rights;
Law Enforcement.

ABSTRACT

This study aims to examine the extent to which wiretapping regulations in Indonesia prioritise the protection of privacy rights and how these regulations will be utilised to reform the criminal justice system in the future. This study is a normative legal analysis that employs a comparative approach, examining the laws of the United States and the United Kingdom. Based on the results of the study, it was concluded that wiretapping regulations in Indonesia do not yet provide protection of privacy rights and do not yet accommodate Constitutional Court Decision Number 006/PUU-I/2003 and Constitutional Court Decision Number/5/PUU-VIII/2010, which mandate that wiretapping regulations be regulated in a special law and uphold human rights. Based on a comparative study with the wiretapping legal systems in the United States and the United Kingdom, it was found that in order to achieve ideal wiretapping regulations, in addition to being regulated in a special law, there is also a need for checks and balances to prevent arbitrariness and rigid and biased rules, as well as stipulating that every wiretapping action must be proportional to the objectives to be achieved. There must also be a strict internal, external and independent monitoring system covering the application for authorisation, implementation and termination of wiretapping, with an emphasis on the protection of personal data and the privacy of citizens. In addition, the following aspects must also be reflected: a. Legality; b. Due process; c. Safeguards Against Illegitimate Access; and d. Legitimate Aims, Necessity and Proportionality.

1. Introduction

Law enforcement is the endeavour to ensure adherence to legal statutes in a modern

nation, executed by either the government or the judiciary, both of which possess the authority to implement the law through the aforementioned methods, in alignment with the established legal framework. In the Civil Law System, law enforcement employs a legal framework termed procedural law. However, in the Common Law System, it utilises an administrative framework referred to as the administration of justice.[1]

Law enforcement is often associated with criminal activity. The law consistently supports that which is governed. The evolution of criminal methodologies is highly dynamic and directly correlates with the progression of telecommunications technology, which is increasingly sophisticated, encompassing telephones, smartphones, computers, electronic mail, and other internet-based communication tools that facilitate and support criminal activities. Undoubtedly, it is evident that in the contemporary Internet age, global boundaries have become largely irrelevant, allowing criminals to exploit the Internet communication network with ease, often without the necessity for direct interaction (cyberspace).[2] This technical advancement will provide challenges for law enforcement in establishing evidence of crimes utilising communication devices. One method to employ communication technology in the pursuit of evidence is by monitoring the conversations and data of individuals suspected of criminal activity, as well as those utilising communication technology to perpetrate such offences. The American police initially employed wiretapping technology in the 1960s to combat organised crime and the rising incidence of street crimes. This technology is employed to identify illicit activities and acts that result in disclosure.[3]

Wiretapping technology advances in response to the need to address complex cases. According to conventional evidentiary laws, recorded conversations are inadmissible as evidence in court. Technological advancements have prompted the evolution of criminal legislation, leading to the development of means for substantiating challenging crimes. Consequently, wiretap results are now preserved as recorded conversation data, which can be utilised alongside electronic and other

---

[1] Selina Keesoony, 'International Anti-Money Laundering Laws: The Problems with Enforcement', *Journal of Money Laundering Control*, 19.2 (2016), pp. 130–47, doi:https://doi.org/10.1108/JMLC-06-2015-0025.
[2] Elstonsius Banjo, 'CYBERSPACE AND WIRETAPPING ON THE CRIMINAL LAW ENFORCEMENT OF CORRUPTION CASES IN INDONESIA', *Petita: Jurnal Kajian Ilmu Hukum Dan Syariah*, 9.2 (2024), pp. 561 – 578, doi:10.22373/petita.v9i2.405.
[3] Dadang Suhendi and Erwin Asmadi, 'Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia', *International Journal of Cyber Criminology*, 15.2 (2021), pp. 135–43, doi:10.5281/zenodo.4766552.

data kinds. The contemporary technological landscape reveals diverse classes of crimes, each with distinct wiretap regulations in common law and civil law jurisdictions.[4] Discussing wiretapping methods within criminal investigations that utilise communication technology in the criminal justice systems of the United Kingdom and the United States, both of which follow the standard law system, as well as Indonesia and France, which adhere to the civil law system, is quite intriguing. This comparison aims to identify the strengths and limitations of interception control mechanisms in both countries and to determine the authorities legally authorized to intercept information. The law in criminal justice serves to resolve conflicts, uphold truth and justice, and regulate societal behaviour.[5]

This study aims to promote equity among all parties by safeguarding privacy against unlawful tapping of communication devices. English law governs tapping through statutory provisions.[6] This situation contrasts with Indonesia's legislation, which has yet to provide comprehensive regulations on tapping. The state's practice of surveilling and intercepting communications has infringed upon the privacy rights of residents. In Indonesia, after the Constitutional Amendment, the right to privacy is acknowledged as a fundamental right of citizens that necessitates protection. Article 28, paragraph (1), letter G of the 1945 Constitution affirms that every individual is entitled to protection of their privacy, family, honour, dignity, and property, which encompasses personal data. Article 32 of Law No. 39 of 1999 on Human Rights underscores that the freedom and confidentiality of electronic communication shall only be infringed upon by a judicial order or an authority authorised by law.[7]

Wiretapping serves as a viable option in criminal investigations related to the evolution of crime categories. In this instance, wiretapping is among the most efficacious detection techniques for resolving criminal cases. Anti-wiretapping employs efficient technical methods to identify organised crimes, including corruption, drug trafficking, and other offences. This implies that those who

[4] Anthony Reyes and others, 'Chapter 6 - Legal Issues of Intercepting WiFi Transmissions', in *Cyber Crime Investigations*, ed. by Anthony Reyes and others (Syngress, 2007), pp. 111–31, doi:https://doi.org/10.1016/B978-159749133-4/50007-3.

[5] August Bequai, 'Monitoring Employee Communications in Cyberspace: The Pitfalls Facing Management', *Computers & Security*, 18.2 (1999), pp. 109–12, doi:https://doi.org/10.1016/S0167-4048(99)80028-5.

[6] Jia-Rong Sun, Mao-Lin Shih, and Min-Shiang Hwang, 'Cases Study and Analysis of the Court Judgement of Cybercrimes in Taiwan', *International Journal of Law, Crime and Justice*, 43.4 (2015), pp. 412–23, doi:https://doi.org/10.1016/j.ijlcj.2014.11.001.

[7] Hwian Christianto, 'From Crime Control Model to Due Process Model: A Critical Study of Wiretapping Arrangement by the Corruption Eradication Commission of Indonesia', *Padjadjaran Jurnal Ilmu Hukum*, 7.3 (2020), pp. 421–42, doi:10.22304/pjih.v7n3.a7.

perpetrate significant offences may be prosecuted based on the findings of eavesdropping. Wiretapping can be employed to identify criminal activity, eliminate significant criminal offences, address novel and highly sophisticated crimes, bolster national defence and security, and avert large-scale crimes that may disrupt public order or morals. The paper emphasises that while wiretapping may infringe upon human rights, it can also reveal criminal conduct. Law enforcement authorities may conduct wiretapping as a component of their investigative activities. This difficulty arises from the challenges law enforcement authorities face in detecting criminal activity. The outcomes of eavesdropping may subsequently serve as evidence in legal proceedings.[8]

The Big Indonesian Dictionary defines wiretapping as the intentional act of listening to and/or covertly recording information about others, encompassing the processes, methods, or acts of eavesdropping. This can also be construed as the intentional act of clandestinely eavesdropping on or recording the confidential information or conversations of others without their knowledge or consent. The wiretapping process can be elucidated in line with the relevant laws, regulations, and procedures as defined by the language employed in various nations. Wiretapping is commonly referred to as authorised interception or just interception. Wiretapping constitutes a subset of interception, which in turn encompasses wiretapping within a broader context. Conversely, electronic surveillance entails the covert observation of human actions and dialogues without the utilisation of wired or wireless communication networks. Consequently, electronic surveillance is fundamentally analogous to wiretapping; however, it does not utilise telecommunication networks for its execution and can visually document the actions of individuals.[9]

Wiretapping or interception undeniably constitutes a breach of human rights, especially the right to privacy in communication. Examination of the Indonesian Supreme Court Decision No. 1429 K/Pid/2010 dated 21 September 2010 in conjunction with Decision No. 117 PK/PID/2011 dated 13 February 2012. The KPK leadership was accused of breaching the Interception Law on Friday, 19 June 2009, as cited on 13 September 2009. Indonesia lacks a unified regulation governing

[8] L. Yes Esty Pratiwi and others, 'In-Depth Review : Legal Review on Human Rights Enforcement in the ASEAN and EU Context', *Journal of Law, Environmental and Justice*, 1.3 (2023), pp. 202–24, doi:10.62264/jlej.v1i3.16.

[9] Januar Rahadian Mahendra, Edwin Setiawan, and Arbend Ficasso Van Hellend, 'Corruption Eradication in Four Asian Countries : A Comparative Legal Analysis', *Journal of Law, Environmental and Justice*, 2.2 (2024), pp. 162–84, doi:10.62264/jlej.v2i2.98.

wiretapping procedures. This engenders susceptibility to the interception of citizens' private communications, encompassing online communications such as email and various social media platforms. As of now, Indonesia has a minimum of twelve statutes and regulations regarding wiretapping in various manners. The ambiguous and redundant regulations have jeopardised human rights, particularly the right to privacy.[10]

The campaign against corruption and terrorism has impacted wiretapping protocols and diminished the safeguarding of private rights. In practice, alongside the lack of wiretapping legislation, concerns about authority remain legally ambiguous. The ability to conduct wiretapping is a complex matter necessitating specific legislation, resulting in ambiguity regarding which entity possesses the right to perform such actions. This affects the issuance of wiretapping authority as outlined in various laws and institutional regulations, resulting in issues such as conflicting wiretapping regulations and disputes regarding the authority to conduct wiretapping. These disputes may lead to significant litigation and preliminary legal proceedings due to legal ambiguity.[11]

The principle of checks and balances, or the separation of powers, is more optimal. Furthermore, to enhance efficiency, it is imperative to institutionalise the integration of diverse operations within a singular unit into hybrid functions. Another aspect is the necessity to safeguard certain functions of power against political intervention and conflicts of interest. Judges, as bearers of judicial authority, are obligated to exercise caution in the enforcement of legal provisions deemed general norms. The presence of judges enhances legal regulations in their deliberations, as they address the deficiencies within the formal legal framework of the relevant legal system. The Constitutional Court's ruling encompasses a judicial review of wiretapping.[12]

Initially, Constitutional Court Decision Number 006/PUU-I/2003. The petitioner contended that the unqualified application of Article 12 paragraph (1) letter a of the KPK Law, which permits initiation against any individual without specified criteria or limitations, poses significant concerns regarding its relevance to the case.

---

[10] O L van Daalen, 'The Right to Encryption: Privacy as Preventing Unlawful Access', *Computer Law & Security Review*, 49 (2023), p. 105804, doi:https://doi.org/10.1016/j.clsr.2023.105804.

[11] Imran Eka Saputra and Muhammad Miftah Fauzan, 'The Authority of the Supervisory Board in the Supervision of the Corruption Eradication Commission in Indonesia', *Journal of Forensic Science and Medicine*, 11.3 (2025), pp. 186 – 194, doi:10.4103/jfsm.jfsm_100_21.

[12] Banjo, 'CYBERSPACE AND WIRETAPPING ON THE CRIMINAL LAW ENFORCEMENT OF CORRUPTION CASES IN INDONESIA'.

Furthermore, the Corruption Eradication Commission's assurance of confidentiality concerning wiretapping and recorded conversations severely undermines the privacy of all societal members, jeopardising their sense of security, individual protection, familial honour, and dignity, as these are perpetually at risk due to the commission's actions, which lack the necessary safeguards and restrictions outlined in the Law on Corruption Eradication (PTPK). No limits, protections, criteria, or qualifications exist concerning the timing of wiretapping and recording conversations, the parties involved in such talks, or the extent to which the repercussions of such wiretapping may be assured.[13]

This is profoundly unsettling as there is no assurance that the recordings will not be exploited for extortion or other detrimental purposes, thereby eroding the sense of security and privacy for all community members, particularly for executive and legislative officials, judicial state officials, and others in public administration.[14] Consequently, Article 12 paragraph (1) letter (i) directly conflicts with Article 28D of the 1945 Constitution, and Article 40 of the PTPK Law also contradicts Article 28D of the 1945 Constitution, which asserts that the stipulations of this article do not afford guarantees, protection, or legal recourse to any individual if the investigation conducted by the KPK fails to yield adequate evidence concerning the alleged corruption perpetrated by the suspect. The plaintiff additionally sought that the Constitutional Court deliver a verdict fully accepting the petition.[15]

Given that the provisions of Law No. 30 of 2002 concerning the Corruption Eradication Commission are inconsistent with the legislative draughting requirements established by the 1945 Constitution, Law No. 30 of 2002 lacks binding legal authority; specifically, Article 13(a), Article 69 paragraphs (1) and (2), Article 26 paragraph (3)(a), Article 71 paragraph (2), Article 12 paragraph (1)(a) and (i), and Article 40, as well as Article 13(a), 69(1) and (2), 26(3)(a), and 71(2) are not legally enforceable. Nevertheless, the judge determined that it cannot be established in court if the draft and provisions of Law Number 30 of 2002 contravene the 1945 Constitution of the Republic of

[13] Christianto, 'From Crime Control Model to Due Process Model: A Critical Study of Wiretapping Arrangement by the Corruption Eradication Commission of Indonesia'.
[14] Nanang Nurcahyo and others, 'Reform of the Criminal Law System in Indonesia Which Prioritizes Substantive Justice', *Journal of Law, Environmental and Justice*, 2.1 (2024), pp. 89–108, doi:10.62264/jlej.v2i1.91.
[15] Mohamad Mahdy, Hartiwiningsih, and Isharyanto, 'Wiretapping Law in Indonesia; Realising Due Process of Law', *Asian Journal of Human Services*, 28 (2025), pp. 242 – 272, doi:10.14391/ajhs.28.242.

Indonesia.[16]

The Constitutional Court Decision Number: 5/PUU-VIII/2010, which annuls the wiretapping procedures outlined in the Decree during a plenary session, asserts that Article 31 paragraph (4) of Law Number 11 of 2008 regarding Electronic Information and Transactions is inconsistent with the 1945 Constitution and thus lacks binding legal authority. Article 31, paragraph 4 states: 'Additional regulations concerning the interception procedures mentioned in paragraph 3 shall be governed by Government Regulation.' The Constitutional Court asserts that the regulations concerning surveillance are governed by law. In announcing Decision No. 5/PUU-VIII/2010, the Constitutional Court outlined several key considerations. To rephrase: Initially, the acknowledgement that interception is an illegal conduct. Eavesdropping constitutes a breach of others' privacy and, hence, infringes upon human rights.[17] Historically, wiretapping has been frequently employed to facilitate specific legal processes, including the investigation of criminal cases related to terrorism, corruption, and narcotics offenses. This official interception is sometimes referred to as unlawful interception. The practice and jurisdiction of wiretapping are highly sensitive matters. This signifies a limitation of human rights, with concurrent legal ramifications. Consequently, legislation concerning the legality of wiretapping should be developed and articulated in alignment with the 1945 Constitution.

In light of the aforementioned decisions, the Constitutional Court of the Republic of Indonesia recommends the establishment of specific legislative regulations concerning wiretapping, taking into account all existing wiretapping laws within the criminal justice system. In this context, 'special' refers to a distinct statute that governs wiretapping activities exclusively. The proliferation of wiretapping techniques, driven by technological advancements, enhances the efficacy of crime detection amid growing complexity; thus, regulating wiretapping is crucial within legal frameworks. The Constitutional Court regards wiretapping as an infringement of privacy rights and a contravention of the 1945 Constitution.[18]

---

[16] Satria Unggul Wicaksana Prakasa and P E Noviandi Nur, 'Analysist of Cyber Espionage in International Law and Indonesian Law', *Humanities and Social Sciences Reviews*, 7.3 (2019), pp. 38 – 44, doi:10.18510/hssr.2019.736.

[17] Tutik Nurul Ramadhan, Bambang Sugiri, and Yuliati, 'Dinamika Regulasi Penyadapan Dalam Undang-Undang Dan Putusan Mahkamah Konstitusi', *Media Iuris*, 5.3 (2022), pp. 529 – 556, doi:10.20473/mi.v5i3.34204.

[18] Sinta Dewi, 'Privacy: An Overview of Indonesia Statutes Governing Lawful Interception', *Central European Journal of International and Security Studies*, 12.4 (2018), pp. 587 – 597

Consequently, wiretapping may fundamentally infringe upon human rights, especially the right to privacy; thus, its implementation must consistently be executed with vigilance to avert misuse and capriciousness by law enforcement authorities. Consequently, interception protocols and limitations on certain rights are important. These constraints and processes must be instituted and governed by legislation that ensures legal certainty and safeguards citizens' privacy. Any law enforcement action that lacks detailed regulation and evidently possesses the potential for power abuse. Consequently, the parameters of wiretapping authority must be established in a definitive, explicit, and quantifiable manner. He asserts that the jurisdiction of law enforcement officers to do eavesdropping should be confined to law enforcement parameters. Without constraints, there exists a potential for the misuse of authority under the pretext of law enforcement. This is due to the absence of explicit rules or regulations governing wiretapping. Concerns exist over the legal ambiguity surrounding the power to perform wiretapping and the admissibility of wiretapping results as evidence. The British legal system governs wiretapping through statutory provisions. This situation contrasts with Indonesian law, which lacks a comprehensive regulation of wiretapping within a singular statute.

2. Research Method

This study employs a normative legal framework,[19] utilising a legislative approach, an analysis of judicial decisions, and a comparative law methodology.[20] The legislative methodology involved a comprehensive inventory and analysis of all pertinent legislation concerning the legal issues presented. Given that the Indonesian legal framework encompasses various statutes related to wiretapping, a comprehensive examination of these regulations was conducted to identify discrepancies within the Indonesian wiretapping legal system. This study examines the judicial approach taken by the Constitutional Court of Indonesia, which has adjudicated multiple cases concerning wiretapping practices, notably including Constitutional Court Decision No. 5/PUU-VIII/2010 and Constitutional Court Decision No. 006/PUU-I/2003. A comparative legal analysis was conducted by examining the wiretapping legal frameworks in the UK and the US, aimed at providing insights for enhancing the wiretapping legal system in

<https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059703271&partnerID=40&md5=5e245cd4c7825b92670008c0042f95f5>.

[19] Ian Dobinson and Francis Johns, 'Qualitative Legal Research', 1 in *Research Methods for Law*, ed. by Mike McConville and Wing Hong Chui (Edinburgh University Press Ltd., 2007).

[20] Lina Kestemont, *Handbook on Legal Methodology* (Intersentia, 2018), doi:10.1017/9781839702389.

Indonesia as part of prospective reforms in the criminal justice system.[21]

3. Results and Discussion

Regulation and Implementation of Interception in the United Kingdom

The regulation of communication interception in the United Kingdom was influenced by two primary factors: the evolution of human rights in Europe and advancements in communication technology during the late 20th century. In the United Kingdom, the interception of communications has historically been employed to identify and avert criminal activity rather than for judicial prosecution. Communications interception was predominantly utilised as a means for law enforcement authorities to collect information rather than as courtroom evidence.[22]

In 1984, the case of Malone v. United Kingdom included a British citizen, James Malone, who expressed grievance over being subjected to wiretapping by the British Government, despite the absence of regulations governing wiretapping in the UK at that time. This prompted the British Parliament to pass the Interception of Communications Act 1985 (the 1985 Act). The 1985 Act was subsequently supplanted by the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA 2000 encompasses additional provisions than the 1985 Act, while nevertheless preserving the ideals of the latter. The United Kingdom possesses extensive legislation governing wiretapping. In July 2000, the United Kingdom implemented the Regulation of Investigatory Powers Act (RIPA), which governs the use of wiretapping.[23]

This regulation permits selected government agencies to conduct surveillance, monitoring, investigations, and interception of communications. This Act was enacted in reaction to the swift advancement of information technology, including the internet. Part I of the RIPA, including Sections 1 to 25, governs the interception of postal and telecommunications communications as well as the procurement of communication data. Part II governs surveillance and clandestine intelligence operations in Sections 26 to 48.

---

[21] Bert-Jaap Koops and Rudi Bekkers, 'Interceptability of Telecommunications: Is US and Dutch Law Prepared for the Future?', *Telecommunications Policy*, 31.1 (2007), pp. 45–67, doi:https://doi.org/10.1016/j.telpol.2006.11.006.

[22] Bill Hancock, 'Wiretaps in Europe — EU Debates a Resolution', *Computers & Security*, 18.5 (1999), pp. 388–89, doi:https://doi.org/10.1016/S0167-4048(99)90599-0.

[23] Tudurachi Elena, 'Wiretaps Interference of Public Authorities in the Right to Privacy and Correspondence', *Procedia - Social and Behavioral Sciences*, 116 (2014), pp. 4591–95, doi:https://doi.org/10.1016/j.sbspro.2014.01.991.

These two components may permit concurrent or overlapping jurisdiction for wiretapping activities. The RIPA also governs the unauthorised interception of ongoing communications via public postal systems, public telecommunication systems, or private telecommunication systems. The outcomes of interception are not inherently admissible as evidence in judicial proceedings. The results may be utilised solely when the public prosecutor requires them to assess all pertinent material evidence for a balanced prosecution, or when the public prosecutor has conferred with a judge familiar with the case to reveal the interception results for the proceedings. This is governed by provisions 17 and 18 of the RIPA.[24]

It is governed by the Post Office Act and, more specifically, by the Home Office Guidelines. In 1984, the European Court of Human Rights ruled in the case of Malone v. the United Kingdom that the legislation in England and Wales was in contravention of the European Convention on Human Rights (ECHR). The Home Office Guidelines are generally acceptable; nonetheless, ambiguities exist that may lead to varying interpretations of the authorities authorized to conduct legally authorized incursions, as stipulated in Article 8 of the ECHR concerning the Protection of Privacy Rights.[25]

Following the verdict in the Malone v. United Kingdom case, the British Parliament enacted the Interception of Communications Act 1985 (hereafter referred to as the 1985 Act). This regulation was the inaugural instrument to govern the interception of communications in the United Kingdom explicitly. The power to issue warrants was retained by the departments associated with the Secretaries of State. The 1985 Act continues to employ wiretapping to prevent or detect serious crimes, thereafter discarding the acquired evidence when judged unneeded. The 1985 Act was subsequently updated due to many circumstances, including the assessment and dissemination of technology advancements and communication methods not addressed in the original legislation, including the internet and mobile phones. Secondly, the implementation of the Human Rights Act in 1988, which integrated the right to privacy as stipulated in the ECHR into the legal framework of England and Wales. In the ECHR, telecommunications interception is regarded as an infringement on the right to privacy. Any infringement of the privacy norms established by the ECHR, including the interception of

[24] Qiao Liu and others, 'Wiretap Resisting and Privacy Preserving Data Exchange with Physical Layer Security and Blockchain Based Authentication in Internet of Vehicles', *Microprocessors and Microsystems*, 104 (2024), p. 104965, doi:https://doi.org/10.1016/j.micpro.2023.104965.
[25] Uri Volovelsky, 'Civilian Uses of Unmanned Aerial Vehicles and the Threat to the Right to Privacy – An Israeli Case Study', *Computer Law & Security Review*, 30.3 (2014), pp. 306–20, doi:https://doi.org/10.1016/j.clsr.2014.03.008.

communications, will be deemed unlawful and may be deemed incompatible with the ECHR.[26]

Thirdly, the government's recent loss at the European Court of Human Rights in Strasbourg in the matter of Halford v. United Kingdom 1997. The plaintiff initiated the case, challenging his privacy rights as outlined in the ECHR concerning the utilisation of private telecommunications systems not governed by the 1985 Act. The court determined that the 1985 Act did not fully govern interception, indicating that the current surveillance framework applied just to public telecommunications systems, excluding private telecommunications. This private region rendered the legislation void since the agency failed to exercise its rights in accordance with the law, as specified in Article 8, paragraph (2) of the ECHR. The 1985 Act was superseded by the Regulation of Investigatory Powers Act (RIPA). RIPA encompasses more than the 1985 Act, while the latter is fundamentally preserved inside RIPA.

This debate will elucidate the regulation of interception in the UK by employing the principles articulated by Privacy International, which are as follows:

Initially, the legality outlined in the 1985 Act and the Regulation of Investigatory Powers Act 2000 governs communication interception as: 'a spectrum of investigative methodologies employed by security and law enforcement agencies for the prevention and detection of terrorism, in the interest of national security, for the identification of serious crime, and to protect the economic welfare of the UK (when directly associated with national security).' Part I of the RIPA (Regulation of Investigatory Powers Act) addresses the interception of postal and telecommunication communications as well as the procurement of communications data. Part II governs surveillance and intelligence collection, which may intersect in both instances. The RIPA governs the interception of real-time communications without legal authority, regardless of whether they occur via the public mail system, a public telecommunications system, or a commercial telecommunications system.[27]

In certain instances, a conversation overheard or a message perused by law enforcement officials constitutes merely 'surveillance.' Surveillance operations are

[26] Jawahitha Sarabdeen, 'Protection of the Rights of the Individual When Using Facial Recognition Technology', *Heliyon*, 8.3 (2022), p. e09086, doi:https://doi.org/10.1016/j.heliyon.2022.e09086.
[27] Cornelia Griebel and Franziska Hohl Zürcher, 'The Work of Intercept Interpreters in Lawful Communication Surveillance: A Daily Trade-off between Formal Requirements and Informal Needs', *International Journal of Law, Crime and Justice*, 74 (2023), p. 100609, doi:https://doi.org/10.1016/j.ijlcj.2023.100609.

governed by Part II of RIPA, which encompasses other activities beyond the interception of communications, including the deployment of recording equipment to monitor all actions within private dwellings or cars, referred to as intrusive surveillance. Simultaneously, a type of surveillance sanctioned or acknowledged by one of the communication entities is referred to as 'directed surveillance'. UK legislation governing interception or wiretapping has adhered to the idea of legality. This indicates that the oversight of such authority is dictated by legal regulations, which encompass both substantive and procedural legislation.[28]

Secondly, Legitimate Objectives, Necessity, and Proportionality. RIPA establishes a framework in which the executive issues warrants as a prerequisite for the legal interception of communications. Two categories of interception warrants exist. The initial category is termed a normal warrant, necessitating either the name or description of the individual to be intercepted or the specific location of the interception. The agency executing the interception often petitions for this form of warrant. Another category of warrant is referred to as a certificated warrant. It is designated as such because it necessitates a certificate from the Secretary of State and is exclusively applicable to external communications transmitted or received beyond the United Kingdom. This category of warrant is not subject to the stipulation of identifying a person or location, as is customary in standard warrants. Both categories of warrants are governed by Section 8 (1), (2), (3), (4), and (5) of the RIPA.[29]

The Secretary of State must grant both ordinary and certified warrants; typically, this is the Home Secretary, who oversees law and order in the UK.[30] In urgent situations requiring a warrant, the Secretary of State must evaluate the application and provide directives to the official before the warrant is endorsed. According to Section 6 of the RIPA, applications for both standard and certificate warrants may be submitted by or on behalf of specific senior persons, including:

a. the heads of security and intelligence agencies, namely the Director-General of the Security Service (MI5); the Chief of the Secret Intelligence Service (M16); the Director of

[28] Yantao Liu and Yasser Morgan, 'Security against Passive Attacks on Network Coding System – A Survey', *Computer Networks*, 138 (2018), pp. 57–76, doi:https://doi.org/10.1016/j.comnet.2018.03.013.
[29] Isabella Gollini, Alberto Caimo, and Paolo Campana, 'Modelling Interactions among Offenders: A Latent Space Approach for Interdependent Ego-Networks', *Social Networks*, 63 (2020), pp. 134–49, doi:https://doi.org/10.1016/j.socnet.2020.07.001.
[30] Nam-Phong Nguyen and others, 'Secure Communications in Cognitive Underlay Networks over Nakagami-m Channel', *Physical Communication*, 25 (2017), pp. 610–18, doi:https://doi.org/10.1016/j.phycom.2016.05.003.

Government Communications Headquarters (GCHQ); the Director-General of the National Criminal Intelligence Service (NCIS); and the Chief of Defence Intelligence Staff (DIS)2; dan

b. the heads of law enforcement agencies, namely the Commissioner of Police of the Metropolis21; the Chief Constable of the Police Service of Northern Ireland; the Chief Constable of any police force maintained under the Police (Scotland) Act 1967; and the Commissioners of Customs and Excise.

Pursuant to Section 5 of the RIPA, before issuing either type of warrant, the Secretary of State must ensure that the application meets the following requirements:

a. the warrants are essential in the sense that they are in the interests of national security or for the purposes of preventing or detecting serious crime, protecting the UK economy from foreign threats or giving effect to provisions governing international legal assistance agreements;
b. the actions authorised by the warrants must be proportionate to the original purpose;
c. the information to be sought cannot be obtained by any other means..

All warrants, including ordinary and certificated warrants, are typically valid for a duration of three months. These warrants may be renewed if deemed necessary, depending on the same grounds. Warrant extensions predicated on major offences are also effective for a duration of three months. Extensions on national security or the national economy are authorised for a duration of six months. Warrants issued under exigent circumstances are valid for a maximum of five working days and may be extended by the Secretary of State. Warrants may be prematurely revoked if they are considered no longer proportionate and required, given the conditions that justified their initial issuance.[31] Section 3 of the RIPA delineates certain circumstances under which interception may be conducted legally without a warrant, including:

a. There are convincing grounds to believe that both the sender and recipient of the communication have consented to the interception.
b. Both the sender and recipient of the communication have consented to the interception, which is authorised more for surveillance than interception purposes. Surveillance may occur, for example, when a kidnapper is calling the sibling of the hostage and the police want to record the call in order to identify or track the kidnapper.

[31] Flavio G A de Meneses, Brian P Mulcahy, and Karolina Brook, 'Wiretap Laws and the Perioperative Physician – The Current State of Affairs', *Journal of Clinical Anesthesia*, 89 (2023), p. 111178, doi:https://doi.org/10.1016/j.jclinane.2023.111178.

c. The interception is carried out in connection with operational requirements or services. For example, the post office needs to open a post box to determine the sender's address because the recipient's address is unknown..

The Secretary of State is authorised to establish regulations allowing certain interception procedures during lawful business activities, within hospitals and prisons, and in foreign legal assistance agreements, as stipulated in Section 4 of the RIPA. Similar to the United States, Australia, and the Netherlands, the United Kingdom has enacted legislation permitting interception measures that infringe upon individual privacy rights for an explicit and legitimate purpose. Consequently, any limitation of privacy rights must align with the state's urgent necessities (necessity) and be accompanied by precise and judicious wiretapping measures (proportionality), as well as the advantages derived from such intrusive actions.[32]

Third, Safeguards Against Illegitimate Access. Sections 14 and 15 of the RIPA mandate that agencies doing interceptions implement internal safeguards for all outcomes of interception activities, regardless of whether they are conducted under standard or approved warrants. The opening, copying, and storage of materials obtained from interception activities must be restricted to essential interests for lawful reasons. The objectives encompass aiding the interception commissioner's functions concerning communications and ensuring equilibrium in the prosecution procedure. Additional protections are implemented for the outcomes of intercepting external communications in accordance with verified warrants. The Secretary of State shall guarantee that the outcomes of wiretapping are accessed by individuals solely for the purpose of validating the materials obtained from the wiretapping. Access to materials obtained from wiretapping or the whole report on the subject is restricted to individuals enumerated in the distribution list of each agency. All individuals concerned must adhere strictly to their legal obligations.[33]

Oversight is the cohesive force that maintains unity, ensuring that freedom does not exceed its bounds. Internal oversight can be achieved by establishing legal certainty and protection, as well as delineating oversight issues to ensure effective regulatory

[32] Liu and others, 'Wiretap Resisting and Privacy Preserving Data Exchange with Physical Layer Security and Blockchain Based Authentication in Internet of Vehicles'; de Meneses, Mulcahy, and Brook, 'Wiretap Laws and the Perioperative Physician – The Current State of Affairs'.
[33] Liu and others, 'Wiretap Resisting and Privacy Preserving Data Exchange with Physical Layer Security and Blockchain Based Authentication in Internet of Vehicles'; Elena, 'Wiretaps Interference of Public Authorities in the Right to Privacy and Correspondence'.

implementation. This law establishes exterior protection mechanisms through monitoring operations, in addition to internal protection.[34] The oversight procedures regarding the execution of interception in the UK can be delineated as follows:

a. Monitoring by the Court: the commissioner is responsible for reviewing the role of the Secretary of State in issuing warrants for interception measures, operations to obtain communications data, and regulatory balance to ensure that the products of interception are handled appropriately. The commissioner is required to submit an annual report to the prime minister. The report is presented to parliament and then made accessible to the public. The report includes or covers an evaluation of the interception process and a summary of the interception activities carried out. In addition, some successful interception activities that are not made public are also evaluated by the commissioner.
b. Monitoring by the Legislature: in terms of administrative financing and related policies, interception measures against M15, M16, and GCHQ communications are monitored by a parliamentary committee known as the Intelligence and Security Committee (ISC);
c. Monitoring by the Public: any member of the public who has been harmed by interception activities carried out by an interception agency can complain to the Investigatory Powers Tribunal (the Tribunal), which was established under Sections 65-69 of the RIPA.

The regulation of wiretapping has established measures with explicit and legitimate objectives. It infringes upon individual privacy rights, indicating that any limitation on these rights must correspond to the state's urgent requirements through precise and judicious interception measures (proportionality) and the advantages derived from such intrusive actions.[35]

Fourth, Due Process. The outcomes of interception measures cannot be regarded as admissible evidence in judicial proceedings unconditionally. The utilisation of these results is permissible solely when the public prosecutor requires them to assess all pertinent material evidence for a balanced prosecution process, or when the public prosecutor has conferred with the presiding judge familiar with the case to reveal the

[34] Hancock, 'Wiretaps in Europe — EU Debates a Resolution'; Elena, 'Wiretaps Interference of Public Authorities in the Right to Privacy and Correspondence'.
[35] Hancock, 'Wiretaps in Europe — EU Debates a Resolution'; Elena, 'Wiretaps Interference of Public Authorities in the Right to Privacy and Correspondence'; Jason Chan, Jin-Hyuk Kim, and Liad Wagman, 'State versus Federal Wiretap Orders: A Look at the Data', *International Review of Law and Economics*, 70 (2022), p. 106064, doi:https://doi.org/10.1016/j.irle.2022.106064.

results of the interception measures for the sake of justice. This is governed by Sections 17 and 18 of the RIPA. The UK system possesses a method for evaluating the legal procedures conducted by investigators.[36] Consequently, if the interception is executed unlawfully, the resultant evidence is deemed unlawful and inadmissible in judicial proceedings.

Regulation and Implementation of Interception in the United States

The government has a longstanding history of intercepting communications in the United States. Law enforcement agencies have engaged in wiretapping since the advent of telegraph telecommunications in 1844 and have utilised telephone wiretapping since the early 1990s. Legislation banning illegal eavesdropping was implemented in mid-1862; however, federal law was largely ineffective during that decade. In 1928, the Supreme Court, in Olmstead v. United States, ruled that the eavesdropping of telephone conversations by federal agents did not constitute a search or seizure as defined by the Fourth Amendment. The principal assertion of The Fourth Amendment is that protection against seizure pertains to tangible goods rather than to telephone conversations, which lack physical visibility.[37]

In 1934, the Federal Act of 1934 was the inaugural federal legislation that prohibited the eavesdropping of telephone calls without the caller's consent. This legislation also restricted the admissibility of wiretap evidence in judicial proceedings. Nonetheless, the efficacy of this legislation was compromised by executive authority. Three decades later, federal investigators continued to intercept communications in accordance with established protocols, particularly those of foreign agents alleged to have breached national security, pursuant to the president's constitutional authority.[38]

In 1960, the Supreme Court sought to protect individuals from illegal searches and seizures, including electronic surveillance of communications. In the 1967 case of Katz v. United States, the court established the concept of a reasonable expectation of privacy, ruling that wiretapping conducted without a judicial warrant violated the Fourth Amendment. This case overturned the 1928 Olmstead decision, ruling that eavesdropping on communications was permitted only if it conformed to constitutional standards. In 1968, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act,

---

[36] de Meneses, Mulcahy, and Brook, 'Wiretap Laws and the Perioperative Physician – The Current State of Affairs'; Elena, 'Wiretaps Interference of Public Authorities in the Right to Privacy and Correspondence'.
[37] 'FBI Outlines a Wiretapping Future', *Network Security*, 1995.11 (1995), pp. 2–3, doi:https://doi.org/10.1016/1353-4858(95)90144-2.
[38] Bill Hancock, 'US Government Fighting for Expanded Wiretap Laws', *Computers & Security*, 19.6 (2000), p. 477, doi:https://doi.org/10.1016/S0167-4048(00)06003-X.

establishing a distinct legal foundation for federal communication interception. Since that time, Congress has amended and updated the interception statute on multiple occasions. The Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA), and the Communications Assistance for Law Enforcement Act (CALEA) were established in 1978, 1986, and 1994, respectively. The most recent substantial amendment to the legislation regulating wiretapping was the implementation of the Patriot Act, enacted two weeks following the 9/11 attacks in 2001. These laws consolidate and fortify America by equipping the necessary instruments to detect and eliminate acts of terrorism.[39]

In United States law, wiretapping and recording are commonly referred to as wiretapping, electronic eavesdropping, and electronic surveillance. In the discourse on wiretapping in the United States, the author will employ the phrase electronic surveillance as a synonym for wiretapping. The author examines wiretapping in the United States to compare it with the wiretapping standard operating procedures in Indonesia. The wiretapping Standard Operating Procedure in Indonesia, as delineated in the preceding chapter, was established by law enforcement authorities, with the use of wiretapping authority requiring prior notification to the Director General of Post and Telecommunications. The licensing procedure in Indonesia is relatively straightforward when compared to the licensing process for wiretapping authorities in the United States.[40]

The utilisation of electronic surveillance authority by law enforcement personnel requires prior authorisation from a senior official within the United States Department of Justice, which includes the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, Assistant Deputy Attorney General, or Acting Assistant Deputy Attorney General of the Criminal Division, as designated by the Attorney General. Subsequently, law enforcement officials may petition the court for authorisation to do covert electronic surveillance. Section 216 of the Omnibus Crime Control and Safe Streets Act of 1968 permits a court to approve the tracking and surveillance of source or address information for computer communications, including email, in a manner analogous to the provisions for telephone conversations. The implementation of these tracking and interception techniques is permissible just within the jurisdiction of the court that granted the warrant. Per Article 216, a court with

[39] Alfonso Muñoz and others, 'Digital Wiretap Warrant: Improving the Security of ETSI Lawful Interception', *Digital Investigation*, 14 (2015), pp. 1–16, doi:https://doi.org/10.1016/j.diin.2015.04.005.
[40] Stephen Gleave, 'The Mechanics of Lawful Interception', *Network Security*, 2007.5 (2007), pp. 8–11, doi:https://doi.org/10.1016/S1353-4858(07)70034-X.

jurisdiction over a committed crime may issue a warrant that is enforceable throughout the United States. Title III of the Act requires the court to issue a comprehensive order detailing the duration and scope of permissible surveillance activities. This aims to reduce the impact of electronic spying on innocent talks. The court mandates that the parties impacted by this surveillance be informed at the expiration of the court's authorisation.[41]

First, legality. Various regulations govern interception efforts in the United States, notably Title III of the Omnibus Crime Control and Safe Streets Act of 1968. This statute is the paramount federal rule governing the real-time acquisition of actual content from wiretapped conversations for law enforcement purposes. The ECPA was updated in 1986 to encompass the wiretapping of electronic communications. Title III defines electronic communication as 'any transfer of signs, signals, letters, images, sounds, data, or intelligence of any sort sent wholly or partially by a wire, radio, electromagnetic, photoelectronic, or photooptical system.'[42]

Nearly all online communications, including email, are electronic in nature. Electronic communications exclude all wired or verbal communications, all communications transmitted via pager tones, all communications from tracking devices, and all electronic information transfers stored by a financial institution within a system utilised for the electronic storage and transfer of funds. The Foreign Intelligence Surveillance Act (FISA) authorises wiretapping of foreign powers or their agents within the United States to acquire foreign intelligence information. This information pertains to U.S. national security, encompassing real defense, potential threats, sabotage, international terrorism, and other covert intelligence operations. Section 1801(a) of FISA delineates the definition of 'foreign power', encompassing a foreign government or its subdivisions; a collective of foreign nationals excluding United States citizens; an entity governed by a foreign government; a group linked to international terrorism; and a foreign political organisation devoid of United States persons.[43]

Similar to Title III, FISA under Section 1801(n) governs the interception of the substantive content of communications. In contrast to Title III, FISA surveillance must focus on a foreign power or its agent situated in the United States, or a facility utilised or

---

[41] Susan Landau, 'Security, Wiretapping, and the Internet', *IEEE Security and Privacy*, 3.6 (2005), pp. 26 – 33, doi:10.1109/MSP.2005.158.
[42] Micah Sherr and others, 'Signaling Vulnerabilities in Wiretapping Systems', *IEEE Security and Privacy*, 3.6 (2005), pp. 13 – 25, doi:10.1109/MSP.2005.160.
[43] William P Bloss, 'Transforming US Police Surveillance in a New Privacy Paradigm', *Police Practice and Research*, 10.3 (2009), pp. 225 – 238, doi:10.1080/15614260802381083.

intended for use by a foreign power or its agent. The subject of the monitoring need not be linked to any criminal activity; however, the information obtained may yield evidence that could be used in a legal prosecution. The explicit objective of the surveillance must be to acquire foreign intelligence, rather than for law enforcement purposes. Electronic surveillance techniques in the United States are governed by federal legislation. United States federal law establishes a dual-purpose system designed to safeguard the confidentiality of telephone conversations, in-person discussions, and all computer-mediated communications, while concurrently permitting the identification and interception of communications for criminal investigations. In the United States, electronic monitoring tactics are employed differently than in Indonesia, where they are predominantly utilised in corruption investigations.[44]

In the United States, electronic surveillance techniques have been employed in numerous grave criminal cases as outlined in Title III of the Act, encompassing espionage, piracy, money laundering, homicide, terrorism, firearms offences, sexual exploitation of minors, and other serious crimes in accordance with U.S. law. Wiretapping in the United States is governed by three principal statutes: Title III of the Omnibus Safe Streets and Crime Control Act of 1968, referred to as Title III; the Foreign Intelligence Surveillance Act, abbreviated as FISA; and the Pen Registers and Trap and Trace Devices section of Title 18, known as the Pen/Trap Statute.[45]

Section 2510 (1) Title III defines "wire communication" as any communication, wholly or partially, transmitted via facilities utilising wire, cable, or similar connections between the origin and reception points, provided or operated by any individual engaged as a common carrier in the transmission of interstate or foreign communications. Section 2510 (2) Title III defines "oral communication" as any spoken communication expressed by an individual who has a reasonable expectation that such communication will not be intercepted under circumstances that warrant that expectation. Section 2510 (9) Title III defines "Judge of competent jurisdiction" as: '(a) a judge of a United States district court or a United States court of appeals;' (b) a judge of any court with general criminal jurisdiction in a State, who is empowered by State statute to issue orders permitting the interception of wire or oral communications. These provisions indicate that the court possesses the

[44] Zachary Crain, *Wiretapping*, in *The Encyclopedia of Civil Liberties in America: Volumes One-Three* (2015), III, doi:10.4324/9781315699868-738.

[45] Deven R Desai, 'Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding', *Notre Dame Law Review*, 90.2 (2015), pp. 579 – 632 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84922426795&partnerID=40&md5=6f205f1d1149dd6f7d3895c6ddb07a22>.

jurisdiction to issue authorisation for interception, with the relevant court being a judge of a United States District Court or a United States Court of Appeals.[46]

Section 2515 Title III stipulates that if any wire or oral communication has been intercepted, its contents and any evidence derived from it cannot be admitted as evidence in any trial, hearing, or proceeding before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or its political subdivisions if such disclosure contravenes this chapter. Section 2518 (9) Title III mandates that the contents of any intercepted wire or oral communication or evidence derived therefrom shall not be admitted as evidence or disclosed in any trial, hearing, or proceeding in Federal or State court unless each party has received a copy of the court order and accompanying application authorising or approving the interception at least ten days prior to the trial, hearing, or proceeding. The judge may waive this ten-day limit if he determines that it was impracticable to provide the party with the aforementioned material ten days before the trial, hearing, or proceeding, and that the party will not suffer prejudice due to the delay in receiving such information.[47]

Sections 2515 and 2518 (9) of Title III stipulate that copies of warrants issued by a judge must be submitted to the court when wiretapping results are intended to be utilized as evidence. In the absence of attachment, the evidence will be deemed inadmissible in court. In contrast to Title III, the wiretapping provisions in FISA are explicitly designated for foreign powers or their agents situated in the United States, as well as for facilities utilised or intended for use by such entities. Wiretapping involving United States citizens requires a court order. This is specified in Section 1804 (a) of FISA.[48]

The third statute regulating wiretapping is the Pen/Trap Statute. This legislation governs the real-time monitoring and acquisition of records and other non-content data from cable and electronic connections, including outbound dialled telephone numbers and incoming calls. Section 3121(c) of the Pen/Trap Statute, Limitation. A government agency permitted to install and utilise a pen register or trap and trace device under this chapter or State law shall employ technology that is reasonably accessible, which limits the recording or decoding of electronic or other impulses to the dialling, routing,

---

[46] Julie Brill, *The Intersection of Privacy and Consumer Protection*, in *The Cambridge Handbook of Consumer Privacy* (2018), doi:10.1017/9781316831960.020.

[47] David H Price, *The American Surveillance State: How the U.S. Spies on Dissent*, in *The American Surveillance State: How the U.S. Spies on Dissent* (2022) <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85209977301&partnerID=40&md5=641c5519f8626ad9fb3b622fc718cf7a>.

[48] Glyn Elwyn and others, 'Individuals Recording Clinical Encounters: A Review of Applicable Law in Multiple Countries', *Communication and Medicine*, 19.1 (2024), pp. 58 – 76, doi:10.1558/cam.20257.

addressing, and signalling information used in the processing and transmission of wire or electronic communications, thereby excluding the contents of any wire or electronic communications.[49]

In contrast to Title III and FISA, the Pen/Trap Statute imposes limitations on the utilisation of Pen/Trap technology by agencies possessing wiretapping authority. The recording and decoding of electronic frequencies should be limited. The Pen Register and Trap and Trace Devices Act governs the real-time monitoring and gathering of records and non-content information from wired and electronic communications, including outbound dialled telephone numbers and incoming calls.[50]

This law defines 'pen register' as a device or process that records or decodes calls, routing, addressing, or signalling information transmitted by an electronic or wire communication instrument or facility, excluding the content of any communication. This phrase excludes apparatus or methodologies employed for billing or cost accounting. A 'trap and trace device' refers to a mechanism or procedure that captures incoming electronic signals or tones to reveal the originating number or connection information, including routing, records, and signals, thereby ascertaining the source of electronic and cable communications, excluding the content of those communications. Legislation in the United States has instituted the principle of legality regarding interception or wiretapping. This indicates that the oversight of such authority is dictated by legal regulations, which encompass both substantive and procedural legislation.[51]

Secondly, Legitimate Aims, Necessity, and Proportionality. The diverse rules regulating wiretapping in the United States affect the various warrant court systems, which the author will elucidate in the subsequent section:

The Warrant Court System was established under Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Wiretapping pursuant to Title III of the Omnibus Safe Streets and Crime Control Act of 1968 necessitates a judicial order for execution. Section 2510 (9) of Title III designates that the appropriate jurisdiction for this action is a judge of the US District Court or the US Court of Appeals. A request for wiretapping must have authorisation from one of the following senior authorities in the Department of Justice

[49] Elwyn and others, 'Individuals Recording Clinical Encounters: A Review of Applicable Law in Multiple Countries'.
[50] David Bright, Russell Brewer, and Carlo Morselli, 'Reprint of: Using Social Network Analysis to Study Crime: Navigating the Challenges of Criminal Justice Records', *Social Networks*, 69 (2022), pp. 235–50, doi:https://doi.org/10.1016/j.socnet.2022.01.008.
[51] Bequai, 'Monitoring Employee Communications in Cyberspace: The Pitfalls Facing Management'.

prior to judicial approval: a. The Attorney General; b. Deputy Attorney General; c. Associate Attorney General; d. Any Assistant Attorney General, Acting Assistant Attorney General, or Acting Deputy Assistant Attorney General.[52]

All requests must be submitted in writing and under oath to the judge. Furthermore, pursuant to Section 2518 of Title III, the request must include details concerning: Firstly, the identity of the investigator or law enforcement officer presenting the request, as well as the authority that authorizes it; Secondly, the facts and case circumstances provided by the applicant to substantiate the judge's conviction that a court order is necessary. This information encompasses specifics of the purported offence that has occurred or is anticipated; an initial description and location of the facility or site where the communication will be intercepted, as well as the nature of the communication to be intercepted; and the identity of the individual, if known, who perpetrated the offence and with whom the communication to be intercepted was conducted; Third, the consideration of whether alternative investigative techniques have been used and proven ineffective, or the rationale for their belief that wiretapping or interception will provide success or pose a risk to their safety; Fourth, the duration for which the wiretapping or interception is required; and Fifth, the details of the prior application.[53]

Wiretapping applications are not universally permissible; however, pursuant to Section 2516 (1) (a) to (r), Title III, such requests may solely be made for offences including murder, kidnapping, robbery, torture, bribery, child abuse, narcotics violations, crimes against national security, and offences punishable by death or imprisonment exceeding one year. Nonetheless, the wiretapping petition must establish 'probable cause' for the court to ascertain that: a. An individual is engaging in, has engaged in, or is likely to engage in a crime enumerated in Title III; b. Relevant communications about the offence will be acquired through the wiretapping; and c. The facilities or locations from which the electronic, oral, or wire communications are intercepted are utilised, will be utilised, or are typically utilised by that individual.[54]

---

[52] Cristina Blasi Casagran, *Surveillance in the European Union*, in *The Cambridge Handbook of Surveillance Law* (2017), doi:10.1017/9781316481127.028.

[53] Kanathip Thongraweewong, 'State Telecommunication Surveillance: A Comparative Study of the US and Thai Telecommunication Privacy Laws', *2014 4th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2014*, 2014, pp. 347 – 352, doi:10.1109/DICTAP.2014.6821709.

[54] Han-Bit Moon, Young-Kwang Jung, and Won-Sang Ra, 'Terminal Acceleration Stabilizing Guidance Law for Impact Angle Constrained Interception of a Non-Maneuvering Target', *International Journal of Control, Automation and Systems*, 13.6 (2015), pp. 1410 – 1422, doi:10.1007/s12555-014-0196-z.

According to Section 2518(5), Title III, the application must demonstrate that the wiretapping will be executed in a manner that minimizes inadvertent wiretapping, such as communications that are extraneous, irrelevant, and not pertinent to the crime or subject matter addressed in the application. Section 2518 (11) (b), Title III, permits agencies engaged in wiretapping to request 'Roving Taps,' enabling them to seek a court order that does not designate a specific line or email account, thereby authorising the recording of any telephone line, mobile phone, or internet account utilised by the suspect. Roving taps are authorized if there are reasonable grounds to suspect that the individual being intercepted is attempting to evade wiretapping from a particular location, for example, by redirecting calls to circumvent surveillance. Nonetheless, Roving Taps are hardly utilised. Annually, only six roaming taps are authorised in criminal cases governed by Title III. Roving taps are not universally employed in wiretapping; their use is limited to specific circumstances and instances.[55]

According to Section 2518 (5) of Title III, court orders must limit wiretapping of communications, indicating that such surveillance should not extend beyond 30 days. A court order extension may be granted, but it cannot exceed 30 days and must conclude after the permitted purpose is fulfilled. Section 2518 (7) (a), Title III mandates that prior to securing a court order, law enforcement officials designated by the Attorney General, Deputy Attorney General, or Associate Attorney General may commence wiretapping of communications under exigent circumstances, including: a. Critical situations that jeopardise life or inflict severe harm on any individual; b. Conspiratorial actions that pose a threat to national security; c. Conspiratorial activities are typical of criminal organisations. According to Section 2518 (7) (b) Title III, a petition for a court order must be filed within 48 hours of the initiation or execution of wiretapping. If the request is not submitted or is denied, the wiretapping must cease immediately and will be deemed unlawful.[56]

The subsequent topic is the Court Warrant System established under the Foreign Intelligence Surveillance Act (FISA) of 1978. Under FISA, the monitoring target must be a foreign power or an agent of a foreign power situated in the United States, and the monitored facility must be utilised or intended for use by a foreign power or its agents.

---

[55] Tihomir Katulic and Goran Vojkovic, 'From Safe Harbour to European Data Protection Reform', *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings*, 2016, pp. 1447 – 1451, doi:10.1109/MIPRO.2016.7522367.

[56] Silja Vöeneky, *Espionage, Security Interests, and Human Rights in the Second Machine Age: NSA Mass Surveillance and the Framework of Public International Law*, in *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (2017), doi:10.1017/CBO9781316658888.019.

Wiretapping that entails the collection of communications from any United States individual situated within the United States requires a court warrant. The necessity to secure a court order is less rigorous than the stipulations outlined in Title III.[57]

FISA warrants are required to be issued by a specialised tribunal referred to as the FISA Court. The court has 11 district court justices selected by the Chief Justice of the Supreme Court. The FISA Court possesses the jurisdiction to accept applications and authorise electronic surveillance/interception across the United States. A judge on the FISA Court is prohibited from accepting an application that another judge has previously denied. According to Section 1803 of FISA, if a court rejects a warrant request, it must provide a written explanation for its decision. This statement is submitted to the court for examination. The evaluation is conducted by three adjudicators designated by the chief judge of the District Court or the Court of Appeals. The court possesses the authority to assess the denial of applications for warrant issuance. If the court determines that the denial of the application is warranted, it must furnish a written account of the rationale for its decision, which the Supreme Court may review. In 2003, despite the FISA Court's historical record of never rejecting a warrant application, it denied four petitions, and the US government chose not to challenge the decisions.[58]

According to Section 1804 (a) of FISA, every application must be submitted in writing and under oath by a federal officer. It must receive authorisation from the Attorney General before being presented before a judge. Section 1804 (a)(7)(B) of FISA mandates that the applicant must include a list of information akin to that required in a Title III application. FISA mandates that the application contain a declaration that 'a significant objective of the surveillance is to acquire foreign intelligence information'. The declaration must be issued by the Assistant to the President for National Security Affairs or an executive officer appointed by the President, based on the Senate's recommendation and counsel.[59]

According to Section 1805(a), a court shall issue a warrant if: The President has

---

[57] Peter N Grabosky and Russell G Smith, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, in *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities* (2018), doi:10.4324/9780203794401.

[58] Daniella Lock, 'Form Over Substance: Human Rights Law's Search for Effective Protections Against the Abuse of Surveillance Powers', *European Human Rights Law Review*, 2022.3 (2022), pp. 299 – 309 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85135443824&partnerID=40&md5=4c64619bbe5af57c9c8694828bf1cb7a>.

[59] Stephen Gleave, 'The Mechanics of Lawful Interception', *Network Security*, 2007.5 (2007), pp. 8 – 11, doi:10.1016/S1353-4858(07)70034-X.

permitted the Attorney General to endorse the application; b. The application has been submitted by a federal officer and sanctioned by the Attorney General. Suppose there exists reasonable cause to suspect that a United States citizen is being monitored electronically by a foreign power or its agent. In that case, this applies to each facility or site where such surveillance is conducted or will be conducted by the foreign power or its agent. An agent of a foreign power encompasses individuals who are aware of or aid others engaged in covert intelligence operations, sabotage, or international terrorism.[60]

The agency overseeing the surveillance has said that it will adopt minimal protocols for acquiring and distributing information derived from the surveillance results. FISA warrants are typically valid for a duration of 90 days. If the subject of the monitoring is a foreign entity, the warrant remains valid for up to one year. If the interception target is a foreign power agent, the warrant remains valid for 120 days. An extension of the warrant may be issued under the same conditions as the prior warrant, contingent upon the extension request including new information as mandated for the previous request.[61]

Under FISA, the President, via the Attorney General, may authorise warrantless electronic monitoring for the acquisition of foreign intelligence information for a duration of one year, contingent upon the Attorney General's declaration of the following: The surveillance is strictly intended to acquire the content of communications transferred primarily between foreign powers or to gain technical intelligence from properties or sites controlled by foreign powers. The surveillance excludes communications involving United States citizens. The agency performing the surveillance has indicated it will adopt minimal procedures, and the Attorney General will report these procedures to both the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least 30 days prior to the application's effective date.[62]

The subsequent topic is the Court Warrant System, derived from the Pen Registers and Trap and Trace Devices section of Title 18. According to Sections 3122 and 3127 (2) of the Pen/Statute, a court order for a Pen/Trap must be issued by a US District Court (including a magistrate judge) or the US Court of Appeals. The court issuing the warrant must possess jurisdiction over the criminal offence under investigation. Any Attorney

---

[60] Ian Leigh, 'Changing the Rules of the Game: Some Necessary Legal Reforms to United Kingdom Intelligence', *Review of International Studies*, 35.4 (2009), pp. 943 – 955, doi:10.1017/S0260210509990374.
[61] Gleave, 'The Mechanics of Lawful Interception', 2007; Leigh, 'Changing the Rules of the Game: Some Necessary Legal Reforms to United Kingdom Intelligence'.
[62] Bernhard Spalt, 'Current Challenges for Lawful Interception (LI)', *World Telecommunications Congress 2010, WTC 2010*, 2010, pp. 164 – 169 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092058893&partnerID=40&md5=17f1a2f72821c454c5ae57a1e7bd7f09>.

(Prosecutor) in the federal government may submit a request without the need for specific permission, as outlined in Section 3122 of the Pen/Trap Statute. A court order will be granted if the request specifies that the information to be intercepted pertains to the crime under investigation. The court is not obligated to authenticate the facts presented in the application. Similar to Title III warrants, Pen/Trap warrants may necessitate third-party assistance for executing wiretaps and fulfilling wiretapping capacity obligations in compliance with CALEA.[63]

The Pen/Trap court warrant remains valid for a maximum of 60 days. The warrant may be prolonged based on the identical application. Each extension shall not exceed 60 days in duration. This is governed by Section III (c) of the Pen/Trap Statute. According to Title III, the Pen/Trap Statute permits a law enforcement officer or investigator designated by a senior justice department official to execute wiretapping without a court order in exigent circumstances; however, a warrant request must be submitted within 48 hours following the execution of the wiretapping. The concept of emergency under the Pen/Trap Statute is more expansive than that specified in Title III. This legislation has instituted wiretapping measures with an explicit and legitimate objective, albeit one that infringes upon individual privacy rights. Consequently, any limitation of privacy rights must correlate with the state's urgent requirements through explicit and judicious wiretapping measures (proportionality) and the advantages derived from such invasive actions.[64]

Third, Safeguards Against Illegitimate Access. In this context, wiretapping in the United States is distinct due to three laws regulating the practice. The author elucidates this in the subsequent section: Protections Against Unauthorised Access in Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 delineates processes for the implementation of minimisation protocols to restrict infringements on private rights. Law enforcement officials typically regard the minimization requirement as satisfied by deactivating the wiretapping equipment when the intercepted content exceeds the parameters of the court order and reactivating it when the conversation falls within the scope of the court order. Intercepted communications must be documented on tape or an equivalent device to

---

[63] Tugba Basaran, *Security, Law and Borders: At the Limits of Liberties*, in *Security, Law and Borders: At the Limits of Liberties* (2010), doi:10.4324/9780203841921.

[64] Vittorio Fanchiotti and Jean Paul Pierini, 'Impact of Cyberspace on Human Rights and Democracy', *2012 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings* <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84866634610&partnerID=40&md5=3ac14c2ba8c53f5b07e4acd5525461e4>.

safeguard the recording from modification or change. Prior to the conclusion of the wiretapping period, these recordings must be sent to the issuing judge and sealed in accordance with the judge's directive. They may only be destroyed by judicial order or upon the judge's rejection, and must be retained for a duration of ten years.[65]

Section 2518(8)(d) Title III mandates a pragmatic timeline, requiring that no later than 90 days following the cessation of the court order, the presiding judge must ensure that the subject of the order and other pertinent parties are informed of the date and duration of the interception, particularly when the results deviate from the request. Individuals or entities impacted by the interception may petition the judge to get a portion of the intercepted material. The judge who authorizes the interception order typically mandates that the agency executing the interception provide regular updates, usually every 7 to 10 days, detailing the status of the interception operation.[66]

Furthermore, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 establishes a monitoring system after the execution of an interception. The oversight system involves the judiciary, the legislature, and the populace. To ensure judicial oversight, it is mandated that within 30 days following the expiration or rejection of a court order or its extension, the judge's decision must be communicated to the Administrative Office of the United States Courts. According to Section 2519 (1) Title III, the report must encompass: a. The identity of the office requesting the warrant and the individual authorising the request; b. The subject of the investigation. The type of wiretapping apparatus and its general location; and d. The duration of wiretapping authorised by the warrant.[67]

Section 2519(2) of Title III mandates that, each January, public prosecutors who submitted court order applications in the preceding year must report to the court's administrative office. The report must encompass: a. Details regarding the identity of the applicant and the individual authorising the application, the legal provisions invoked in the investigation, the type of wiretapping equipment utilised, and the duration of the wiretapping; b. The source and frequency of both incriminating and non-incriminating

---

[65] Micah Sherr and others, 'Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps', *Proceedings of the ACM Conference on Computer and Communications Security*, 2009, pp. 512 – 523, doi:10.1145/1653662.1653724.

[66] Vöeneky, *Espionage, Security Interests, and Human Rights in the Second Machine Age: NSA Mass Surveillance and the Framework of Public International Law*; Grabosky and Smith, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*.

[67] Moon, Jung, and Ra, 'Terminal Acceleration Stabilizing Guidance Law for Impact Angle Constrained Interception of a Non-Maneuvering Target'; Gleave, 'The Mechanics of Lawful Interception', 2007.

wiretapping results; c. The total number of individuals whose communications were intercepted. The quantity of wiretapping warrants issued and an assessment of whether the wiretapping facilitated or obstructed law enforcement efforts.[68]

The subsequent process involves legislative oversight, allowing Congress to monitor wiretapping actions conducted through various methods. Specifically, initially, parliamentary committees, such as the judiciary and intelligence committees, conduct hearings and submit written inquiries to investigators or law enforcement agencies. The House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence can also oversee investigative actions. The two committees are tasked with verifying the proper use of intelligence sources and the legality of intelligence operations, as well as reporting to Congress. Section 2519, subsection 3, Title III mandates that each April, the Director of the Administrative Office must submit a report to Congress detailing the quantity of wiretap requests and the number of warrants and extensions granted or denied in the preceding year, accompanied by an analysis of this information.[69]

The subsequent topic, also intriguing, is Public Monitoring. Section 2518(10)(a) Title III mandates that any individual belonging to a group whose communications are intercepted, or who is the target of eavesdropping in judicial proceedings, has the right to contest the content of any intercepted communications or any evidence derived from such acts. Reasons for such a request may encompass: the communication was illegal; the court order permitting the interception was inadequate or improper; and the interception was not executed in compliance with the court order. The Foreign Intelligence Surveillance Act (FISA) of 1978, as outlined in Title III, does not mandate notification to the target of surveillance of the interception of their communications. Federal officials may utilise and disclose the outcomes of wiretapping activities concerning U.S. citizens for legitimate purposes without violating their rights, as long as such measures adhere to minimal procedural standards.[70]

The subsequent topic pertains to Safeguards Against Unauthorized Access under the Pen Register and Trap and Trace Devices Chapter of Title 18 (the Pen/Trap Statute), as outlined in 18 U.S.C. §§ 3121-3127. The Pen/Trap Statute imposes limitations on the

[68] Lock, 'Form Over Substance: Human Rights Law's Search for Effective Protections Against the Abuse of Surveillance Powers'; Gleave, 'The Mechanics of Lawful Interception', 2007.
[69] Fanchiotti and Pierini, 'Impact of Cyberspace on Human Rights and Democracy'; Basaran, *Security, Law and Borders: At the Limits of Liberties*.
[70] Basaran, *Security, Law and Borders: At the Limits of Liberties*; Lock, 'Form Over Substance: Human Rights Law's Search for Effective Protections Against the Abuse of Surveillance Powers'.

utilisation of Pen/Trap technology by agencies with wiretapping jurisdiction. The recording or decoding of alternative electronic frequencies must be limited. This complies with Section 3121 (c) of the Pen/Trap Statute. Furthermore, this legislation establishes a surveillance or monitoring system, incorporating the following mechanisms: Initially, judicial oversight is implemented when Pen/Trap devices are employed for eavesdropping, and this usage must be communicated to the court's administrative office. Secondly, oversight by the legislature. According to Section 3126 of the Pen/Trap Statute, the Attorney General must submit a report to Congress. The report must encompass: a. The duration of wiretapping mandated by the court warrant and any extensions thereof; b. The specification of particular criminal offences within the application and warrant or its extension; c. The quantity and facilities utilised. The identity, including district, of the law enforcement or investigative officer who submitted the application and the official who sanctioned the warrant. In conclusion, the United States legislation has established safeguards against unauthorised access by implementing both internal and external monitoring or evaluation systems to manage such access.[71]

Fourthly, the dimension of due process within the wiretapping legal framework in the United States, as delineated by three statutes regulating wiretapping, can be articulated as follows:

The acceptability of evidence in accordance with Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Sections 2515 and 2518 (9) of Title III stipulate that evidence acquired via wiretapping can be presented in court, provided that both parties receive a copy of the wiretapping order and that the request is submitted no less than ten days prior to the trial. The judge may choose to waive the ten-day period during which the relevant parties were not under suspicion if he determines that there was a delay in obtaining such information. The criteria for the admissibility of evidence are grounded in the Foreign Intelligence Surveillance Act (FISA) established in 1978. Authorisation from the Attorney General renders the outcomes of interception permissible as evidence within a judicial context. Prior to the utilisation of wiretapping results, the government must inform the defendant, who retains the right to contest the admissibility of evidence acquired through unlawful means. Nonetheless, the defendant's ability to access the FISA warrant or application will be obstructed should the Attorney General assert that disclosing these

[71] Spalt, 'Current Challenges for Lawful Interception (LI)'; Landau, 'Security, Wiretapping, and the Internet'.

documents would jeopardise national security.[72]

The acceptability of evidence as outlined in the Pen Register and Trap and Trace Devices Chapter of Title 18, specifically within the provisions of 18 U.S.C. 3121-3127. The court order must remain sealed or closed until the issuing court provides further direction. Individuals or entities offering support to the applicant must refrain from revealing the outcomes of the wiretapping conducted with The Pen/Trap equipment to any party, until such disclosure is mandated by the court, as outlined in Section 3123 (d) of The Pen/Trap Statute. In response to the events of September 11, 2001, and the advancements in communications technology, the US Congress aimed to consolidate and fortify the United States by equipping law enforcement with the necessary tools for wiretapping and combating acts of terrorism. The enactment of the Patriot Act stands as one of the most contentious measures in recent history. This legislation modified various provisions concerning surveillance and wiretapping as outlined in Title III of the Foreign Intelligence Surveillance Act and the Pen/Trap Statute..

Reformulation of Wiretapping Regulations Based on Criminal Justice Reform in Indonesia: Efforts to Realise Fair Law Enforcement

Indonesia has regulated wiretapping through legislation, but this legislation does not yet incorporate values that respect human rights in accordance with the UDHR and ICCPR. The regulation of interception powers in legislation has fulfilled the principle of legality, but without applying the principle of due process of law. This indicates that Indonesia is based solely on legislation and governed by law. However, this understanding does not guarantee activities that are free from government intervention or interference. A law that is not based on the application of moral goodness and respect for human rights is prone to abuse.[73]

Examining the comparison Table of compliance and due process of law, it becomes apparent that Indonesia only fulfills the principles of legality and legitimate aim, albeit in a material sense, rather than a formal one. Therefore, it can be said that Indonesian legislation in regulating interception does not yet meet human rights standards and is

[72] Landau, 'Security, Wiretapping, and the Internet'; Sherr and others, 'Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps'.
[73] Rudi Natamiharja and others, 'BALANCING TWO CONFLICTING PERSPECTIVES ON WIRETAPPING ACT: Rights to Privacy and Law Enforcement', *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, 22.1 (2022), pp. 18 – 30, doi:10.30631/alrisalah.v22i1.1226.

prone to abuse by certain parties.[74] However, the question that needs to be discussed in greater depth is why interception measures regulated by Indonesian legislation, which have been proven not to meet the principle of respect for human rights, are still used and accepted by the criminal justice system in Indonesia. In Indonesia, wiretapping is regulated in the Criminal Procedure Code (KUHAP). However, the regulations are limited and not very detailed, especially regarding the procedures and supervision of wiretapping by law enforcement officials. To better understand this, we need to examine several key points from the KUHAP and other regulations governing wiretapping in Indonesia.[75]

A significant change in the Draft KUHAP pertains to the establishment of a new institution, specifically the Preliminary Examination Judge, which replaces the pretrial court. The pretrial court is an institution unique to the KUHAP, which has proven to be ineffective because it is passive in waiting for lawsuits to be filed by the parties. Moreover, it is not an independent institution but is attached to the district court. The head of the district court appoints a judge to serve as a pretrial judge upon receipt of a request. The idea of a Preliminary Examination Judge differs from that of a pretrial judge. However, it is not the same as a rechtercommissaris in the Netherlands or a juge d'instruction in France, because the Preliminary Examination Judge in the Draft Criminal Procedure Code does not lead the investigation at all. So it is a revitalisation of the preliminary hearing that already exists in the current Criminal Procedure Code.[76]

Inadvertently, it is similar to the Giudice per le indagini preliminari (Preliminary Examination Judge) in Italy. Italy has even abolished the Giudice Istruttore, which is similar to the juge d'instruction in France and the rechtercommissaris in the Netherlands. The duties of the Giudice per le indagini preliminary (Preliminary Investigating Judge), who oversees the investigation and prosecution, are similar to those of the preliminary investigating judge in the Draft.[77] Some of the powers of the District Court judge, such as issuing search warrants, conducting seizures, wiretapping, and extending detention, have

---

[74] Jonathan Klaaren, 'Human Rights: Legal Aspects', in *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, ed. by James D Wright, Second Edi (Elsevier, 2015), pp. 375–79, doi:https://doi.org/10.1016/B978-0-08-097086-8.86158-9.

[75] Mohammad Fadhil, 'The Harmonization of Wiretapping Regulations in Indonesia: Law Enforcement Perspective', *Substantive Justice International Journal of Law*, 3.2 (2020), pp. 125 – 146, doi:10.33096/substantivejustice.v3i2.75.

[76] Yue Ma, 'Prosecutorial Discretion and Plea Bargaining in the United States, France, Germany, and Italy: A Comparative Perspective', *International Criminal Justice Review*, 12.1 (2002), pp. 22 – 52, doi:10.1177/105756770201200102.

[77] Renze Salet and Jan Terpstra, 'Criminal Justice as a Production Line: ASAP and the Managerialization of Criminal Justice in the Netherlands', *European Journal of Criminology*, 17.6 (2020), pp. 826–44, doi:10.1177/1477370819828332.

been transferred to the Preliminary Investigating Judge to expedite the process and avoid interfering with the District Court judge, who is busy hearing criminal, civil, and other cases. There are also powers of the prosecutor that are transferred to the Preliminary Examination Judge, such as the extension of detention from 40 (forty) days to 25 (twenty-five) days.

There should be an institution between the public prosecutor and the judge, namely, the Preliminary Examination Judge. In the discussion section, the differences between the Rechtercommisaris in the Netherlands and the Juge d'instruction in France on the one hand, and the Preliminary Investigating Judge introduced in the Draft Criminal Procedure Code on the other, will be highlighted. Several issues include the relationship between investigators and public prosecutors, which is regulated within an integrated judicial system rather than a domino-like chain. This issue is the most difficult to formulate.[78]

Currently, due to the back-and-forth transfer of case files between investigators and public prosecutors, the whereabouts of thousands of cases are unknown. Wiretapping is introduced in the Draft, but is subject to strict conditions. Article 83 paragraph (1) of the Draft states: 'Wiretapping of conversations via telephone or other telecommunications devices is prohibited, except in cases involving serious crimes or where there is strong suspicion that a serious crime will occur, which cannot be uncovered without wiretapping.' Thus, in principle, wiretapping is prohibited. Wiretapping is therefore an exception.[79] Serious criminal offences are explained in Article 83, paragraph (2) of the Draft. Wiretapping is conducted following a formal written directive from the local investigating officer, after securing authorisation from the Preliminary Examination Judge. Consequently, the KPK must secure authorisation from the Preliminary Examination Judge prior to engaging in wiretapping activities. In urgent circumstances, exceptions to the Preliminary Examination Judge's permission are constrained and must be communicated to the judge via the public prosecutor.

Wiretapping, even when authorised, is confined to particular offences including national security threats, deprivation of liberty or kidnapping, violent robbery, extortion, threats, human trafficking, smuggling, corruption, money laundering, counterfeiting, immigration violations, explosives and firearms offences, terrorism, severe human rights abuses, psychotropic substances and narcotics, rape, murder, illegal mining, illegal fishing

[78] Francis Pakes, *Comparative Criminal Justice, Second Edition*, in *Comparative Criminal Justice, Second Edition* (2012), doi:10.4324/9780203118290.
[79] Mohamad Mahdy, Hartiwiningsih, and Isharyanto, 'Wiretapping Law in Indonesia; Realising Due Process of Law', *Asian Journal of Human Services*, 28 (2025), pp. 242 – 272, doi:10.14391/ajhs.28.242.

in waters, and illegal logging. Nonetheless, within the framework of wiretapping as a means to enhance and expedite law enforcement efforts, such measures must be employed judiciously and in accordance with established legal protocols. The Criminal Procedure Code stipulates that all wiretapping activities require formal reporting and must secure authorisation from a preliminary examining judge. The existence of particular regulations governing wiretapping serves as the foundation for judicial determinations regarding the legal justification of such actions.[80]

In Indonesia, the legal framework governing wiretapping primarily focuses on empowering law enforcement officials to conduct investigations. At the same time, it lacks comprehensive provisions regarding the methodologies of wiretapping and the safeguarding of privacy rights associated with such practices. Consequently, wiretapping presents a significant risk of infringing upon the privacy rights of citizens by law enforcement authorities. In accordance with the principle of the rule of law, Article 1 paragraph (3) of the 1945 Constitution articulates that the State of Indonesia is fundamentally a state governed by the rule of law. Indonesia stands among the nations that endorsed the International Covenant on Civil and Political Rights (ICCPR) in 1966, formalized through the enactment of Law No. 12 of 2005, which pertains to the ratification of this significant Covenant. Article 17, paragraph (1) of the International Covenant on Civil and Political Rights articulates that individuals shall not endure arbitrary or unlawful intrusions into their privacy, family, home, or correspondence, nor shall they face unlawful assaults on their honour and reputation.[81]

Article 12 of the Universal Declaration of Human Rights (UDHR) of 1948 asserts that individuals shall not be subjected to arbitrary intrusions into their privacy, family, home, or correspondence, nor shall they face attacks on their honour and reputation. All individuals are entitled to legal safeguards against such intrusions or breaches of their rights. Furthermore, Article 28G paragraph (1) of the 1945 Constitution articulates that every individual possesses the right to safeguard their personal self, honour, dignity, and property under their stewardship, in addition to the right to experience safety and protection from the apprehension associated with exercising or refraining from actions that constitute a fundamental right. According to these three laws, the right to privacy constitutes a fundamental aspect of human rights that necessitates safeguarding by the state. Any action undertaken by the state via its officials must adhere to these human

[80] Fadhil, 'The Harmonization of Wiretapping Regulations in Indonesia: Law Enforcement Perspective'.
[81] Fadhil, 'The Harmonization of Wiretapping Regulations in Indonesia: Law Enforcement Perspective'; Mahdy, Hartiwiningsih, and Isharyanto, 'Wiretapping Law in Indonesia; Realising Due Process of Law'.

rights provisions, as such rights constitute the constitutional entitlements of every citizen.[82]

The advancement of technology in contemporary society has led to an increase in criminal activity, necessitating reforms within the law enforcement sector. The techniques typically employed by law enforcement agencies are increasingly inadequate in addressing contemporary advancements. Consequently, law enforcement officials must adopt methodologies that align with contemporary technological advancements. The emergence of wiretapping methods for legal purposes can be attributed to the recognition of wiretapping as an effective means of adapting to contemporary technological advancements. The function of wiretapping as a mechanism for crime detection positions it as an instrument for law enforcement officials in the pursuit of uncovering a range of serious offences. The legal framework governing interception or wiretapping in Indonesia is dispersed across various statutes and regulatory provisions.[83] The existence of multiple regulations about the same subject can lead to divergent interpretations, influenced by both the viewpoints of law enforcement and the broader community.

According to Article 26A of the Amendment to the TPK Law, it is articulated that circumstantial evidence, as referenced in Article 188 paragraph (2) of the Criminal Procedure Code, may also be acquired through electronic recordings or wiretapping. Consequently, wiretapping evidence is regarded as an augmentation of evidence within the framework of the Criminal Procedure Code.[84] Article 5 of the Electronic Information and Transactions Law articulates that electronic information and documents are recognised as valid evidence, serving as an extension of valid evidence in alignment with the procedural law currently in effect in Indonesia. Conversely, wiretapping presents significant vulnerabilities regarding the infringement of individual privacy rights. According to the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Constitution of 1945, it is articulated that the right to privacy constitutes a fundamental human right that necessitates safeguarding by the

[82] Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation', *International Review of Law, Computers and Technology*, 33.1 (2019), pp. 76–99, doi:10.1080/13600869.2019.1562604.
[83] Giovanni De Gregorio and Roxana Radu, 'Digital Constitutionalism in the New Era of Internet Governance', *International Journal of Law and Information Technology*, 30.1 (2022), pp. 68–87, doi:10.1093/ijlit/eaac004.
[84] Satryo Sasono, Isharyanto Isharyanto, and Delasari Krisda, 'Child and Women Domestic Abuse Victims ' Social Health Insurance Protection : An Affirmative Justice Perspective', *Journal of Law, Environmental and Justice*, 1.2 (2023), pp. 105–21, doi:10.62264/jlej.v1i2.8.

state.[85]

The rights of individuals can be classified into two distinct categories: derogable rights and non-derogable rights. According to Article 4 of Law Number 39 of 1999 regarding Human Rights, which is referred to as the Human Rights Law, it states that certain rights are non-derogable. These include the right to life, the right to be free from torture, the right to personal liberty, the freedom of thought and conscience, the right to practise one's religion, the right to freedom from enslavement, the right to recognition as a person, equality before the law, and the right to protection against prosecution.[86] The right to privacy constitutes a personal entitlement that is categorised among derogable rights. The Telecommunications Law clearly articulates, in Article 40, that the information held by an individual constitutes a personal right that warrants protection. Consequently, the right to privacy stands as a fundamental right that necessitates safeguarding. Article 28J paragraph (2) of the 1945 Constitution articulates that legal provisions must establish all limitations on the exercise of an individual's rights and freedoms. Consequently, it is essential to establish precise regulations concerning wiretapping, as delineated in the Telecommunications Law.

Table: Model of interception policy

Subject	Explanation	Current Conditions	Recommendations
Duration of wiretapping	Duration of wiretapping: From the date of issuance until the expiry of the permit.	1.30 days (Psychotropic Substances Act) 2. 1 year (Anti-Terrorism Act) 2.1 year (Act on the Eradication of Trafficking in Persons) 3.3 months, extendable once for another 3 months (Narcotics Act)	30 days and can be extended by 1 x 30 days.
Law enforcement officials who carry out	The authority of officials conducting wiretapping activities	1. Indonesian National Police investigators (Psychotropic Substances Law); 2. Investigators (Corruption Eradication Law, Anti-Terrorism Law,	Investigators (Police); KPK Investigators; Intelligence (in cases related to national security).

[85] O L van Daalen, 'The Right to Encryption: Privacy as Preventing Unlawful Access', *Computer Law & Security Review*, 49 (2023), p. 105804, doi:https://doi.org/10.1016/j.clsr.2023.105804.
[86] Rudi Natamiharja and others, 'BALANCING TWO CONFLICTING PERSPECTIVES ON WIRETAPPING ACT: Rights to Privacy and Law Enforcement', *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, 22.1 (2022), pp. 18 – 30, doi:10.30631/alrisalah.v22i1.1226.

		Trafficking in Persons Law); 3. Corruption Eradication Commission (Corruption Eradication Commission Law); 4. Police and National Narcotics Agency investigators (Narcotics Law); 5. Investigators (Joint Team)	
Licensing Authority	The agency or institution authorised to grant permission to law enforcement officials to conduct wiretapping activities. In terms of administrative authority, this permitting institution automatically becomes the supervisory institution.	1. Chief of Police (Psychotropic Substances Act); 2. Attorney General and/or Chief of Police (Telecommunications Act); 3. Order of the Chief Justice (Anti-Terrorism Act); 4. Written order of the Chief Justice (Narcotics Act); 5. Order or permission from the Attorney General (Joint Corruption Eradication Team Regulation); 6. Request from the Attorney General, Chief of the Indonesian National Police, Investigator (Telecommunications Regulation)	Court. In terms of administrative authority, this licensing institution automatically becomes a supervisory institution.

Purpose/reason	Several reasons or objectives for which authority may be requested	1. Investigative interests (Anti-Terrorism Law); 2. Performance of criminal investigation duties, 2. For investigations, prosecution interests (National Corruption Eradication Security Law); 3. Investigative interests (Narcotics Law); 4. Investigative interests (Government Regulation on Joint Teams, Corruption Eradication)	1. For the purposes of criminal investigation; 2. For the purposes of national security.
Requirements	Possess authority as stipulated in each law.		
Accountability/Report	What are the restrictions on wiretapping?	No liability	Regulation of accountability in every act of illegal wiretapping
Mechanism & Technicalities of Wiretapping	Wiretapping Standards	Regulated in each Regulation of Law Enforcement Agencies	Integrated into the Wiretapping Bill
Wiretapping Application Procedure	Wiretap procedure standards	Not regulated	Integrated into the Wiretapping Bill
Types of prohibited acts related to wiretapping	Circumstances in which wiretapping is not permitted	Not regulated	In diplomatic circumstances, without court authorisation and in relation to intelligence activities
Complaints Mechanism	The complaint mechanism for members of the public who feel they have been harmed is delegated to the wiretapping court process. 2. Criminal charges have been or are being brought.	There are no regulations.	1. Preliminary hearing if the case has not yet been transferred to court; 2. Criminal charges for misconduct in office
Legal Instrument	The form of legislation used as the legal umbrella for wiretapping activities carried out by law enforcement officials.	Still scattered across various laws and regulations, ranging from laws to ministerial regulations.	Laws and Government Regulations on wiretapping

Source: created by the Authors

The ideal legislation for implementing wiretapping, aimed at ensuring the integrity of due process, must consider a range of significant principles and factors. Wiretapping should be governed by precise and well-defined legal frameworks that delineate the circumstances, methods, and locations in which such activities may be conducted. The legal framework should stipulate that wiretapping is permissible only under specific,

rigorously defined conditions, particularly in the context of investigating serious offenses or threats to national security.[87] The legislation should mandate the requirement to inform the individual who has been intercepted post-interception, except in cases where compelling justifications exist to uphold confidentiality for the sake of the ongoing investigation. The legislation should mandate that interception is commensurate with the goals intended to be realized. Interception should be employed only when alternative investigative techniques are not likely to be effective. The legal framework should establish guidelines for safeguarding the privacy of individuals subjected to wiretapping, including stipulations regarding the categories of information that may be gathered and retained, as well as restrictions on the permissible duration of such surveillance activities.

An autonomous oversight mechanism should be established to ensure that wiretapping is conducted in compliance with legal standards and is not subject to misuse. Law enforcement officials who violate wiretapping regulations should be held accountable for their actions. Those subjected to wiretapping should be allowed to engage in a just and efficient legal framework to contest the legitimacy of the wiretapping and to seek redress should it be determined that the wiretapping was executed unlawfully.[88] The legal framework must consider particular contexts, such as the wiretapping of advocates, journalists, or parliamentarians, necessitating distinct treatment to ensure their freedom to perform their responsibilities is not compromised. Considering these elements, an optimal legal framework can effectively govern wiretapping to meet the goals of investigation and security, while simultaneously safeguarding individual human rights and upholding the principle of due process.[89]

The Wiretapping Bill aims to serve as a cohesive framework; however, within its contextual parameters, this unification implies that the Bill will establish itself as the overarching regulation governing all wiretapping activities conducted under various

---

[87] Natamiharja and others, 'BALANCING TWO CONFLICTING PERSPECTIVES ON WIRETAPPING ACT: Rights to Privacy and Law Enforcement'; Tutik Nurul Ramadhan, Bambang Sugiri, and Yuliati, 'Dinamika Regulasi Penyadapan Dalam Undang-Undang Dan Putusan Mahkamah Konstitusi', *Media Iuris*, 5.3 (2022), pp. 529 – 556, doi:10.20473/mi.v5i3.34204.

[88] Rian Saputra, M Zaid, and Devi Triasari, 'Executability of the Constitutional Court ' s Formal Testing Decision : Indonesia ' s Omnibus Law Review', *Journal of Law, Environmental and Justice*, 1.3 (2023), pp. 244–58, doi:10.62264/jlej.v1i3.18.

[89] Satria Unggul Wicaksana Prakasa and P E Noviandi Nur, 'Analysist of Cyber Espionage in International Law and Indonesian Law', *Humanities and Social Sciences Reviews*, 7.3 (2019), pp. 38 – 44, doi:10.18510/hssr.2019.736; Sinta Dewi, 'Privacy: An Overview of Indonesia Statutes Governing Lawful Interception', *Central European Journal of International and Security Studies*, 12.4 (2018), pp. 587 – 597 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059703271&partnerID=40&md5=5e245cd4c7825b92670008c0042f95f5>.

Special Laws that address particular criminal offences, including corruption. Consequently, careful consideration must be exercised in its formulation to ensure that this proposed wiretapping regulation serves as a cohesive framework, capable of meeting the legal standards outlined in current special laws, while avoiding any complications or restrictions that could undermine the efficacy of these laws in addressing specific criminal activities detrimental to the public good.[90]

Wiretapping should not be deemed unlawful unless a precise legal framework thoroughly delineates the mechanisms and constraints governing such practices. The legal framework in Indonesia operates under the principle of legality, asserting that no action is deemed unlawful unless explicitly outlined in the legislation, a concept articulated in Dutch as: nullum delictum nulla poena sine praevia lege. In this instance, it is essential to clarify that the processes of investigation and inquiry possess a distinct conceptual framework when compared to the due process of law or law enforcement, particularly in relation to the principle of presumption of innocence. This is due to the necessity for investigators to presuppose culpability in order to elucidate the modus operandi and seek evidence that satisfies the requisite elements of proof.[91]

To establish a system of checks and balances within law enforcement, it is essential to impose restrictions on wiretapping regulations to mitigate the risk of arbitrary surveillance. It is essential to establish a definitive affirmation of wiretapping authority within the regulations governing this practice, accompanied by a rigorous monitoring system that spans the entire process—from the application for a wiretapping permit, through its execution, to the eventual cessation of wiretapping activities.

4. Conclusion

Following the research findings and discourse, the author concludes that the regulation of wiretapping in Indonesia fails to address privacy rights protection and does not incorporate the various rulings of the Constitutional Court (Constitutional Court Decision

[90] Mohammad Fadhil, 'The Harmonization of Wiretapping Regulations in Indonesia: Law Enforcement Perspective', *Substantive Justice International Journal of Law*, 3.2 (2020), pp. 125 – 146, doi:10.33096/substantivejustice.v3i2.75; Mohamad Mahdy, Hartiwiningsih, and Isharyanto, 'Wiretapping Law in Indonesia; Realising Due Process of Law', *Asian Journal of Human Services*, 28 (2025), pp. 242 – 272, doi:10.14391/ajhs.28.242.

[91] Elstonsius Banjo, 'CYBERSPACE AND WIRETAPPING ON THE CRIMINAL LAW ENFORCEMENT OF CORRUPTION CASES IN INDONESIA', *Petita: Jurnal Kajian Ilmu Hukum Dan Syariah*, 9.2 (2024), pp. 561 – 578, doi:10.22373/petita.v9i2.405; Hwian Christianto, 'From Crime Control Model to Due Process Model: A Critical Study of Wiretapping Arrangement by the Corruption Eradication Commission of Indonesia', *Padjadjaran Jurnal Ilmu Hukum*, 7.3 (2020), pp. 421–42, doi:10.22304/pjih.v7n3.a7.

Number 006/PUU-I/2003 and Constitutional Court Decision Number: 5/PUU-VIII/2010), which require that wiretapping regulations be established in a dedicated statute while safeguarding human rights. Through a comparative legal analysis of the wiretapping frameworks in the United States and the United Kingdom, the author determined that optimal regulations on wiretapping necessitate not only specific legislative provisions but also robust checks and balances within law enforcement to mitigate the risk of arbitrary wiretapping. Consequently, limitations should be imposed on wiretapping regulations. The legislation must mandate that wiretapping be proportional to the intended objectives. The wiretapping regulations must contain an unequivocal declaration of the authority to perform wiretapping and establish a rigorous monitoring framework, encompassing internal, external, and independent oversight, from the initiation of a wiretapping permit request through the execution and cessation of wiretapping, with a focus on safeguarding personal data and citizen privacy. Furthermore, it must encompass the following elements: a. legality; b. due process; c. safeguards against illegitimate access; and d. legitimate aims, necessity, and proportionality.

5. References

Banjo, Elstonsius, 'CYBERSPACE AND WIRETAPPING ON THE CRIMINAL LAW ENFORCEMENT OF CORRUPTION CASES IN INDONESIA', *Petita: Jurnal Kajian Ilmu Hukum Dan Syariah*, 9.2 (2024), pp. 561 – 578, doi:10.22373/petita.v9i2.405

Basaran, Tugba, *Security, Law and Borders: At the Limits of Liberties*, in *Security, Law and Borders: At the Limits of Liberties* (2010), doi:10.4324/9780203841921

Bequai, August, 'Monitoring Employee Communications in Cyberspace: The Pitfalls Facing Management', *Computers & Security*, 18.2 (1999), pp. 109–12, doi:https://doi.org/10.1016/S0167-4048(99)80028-5

Bloss, William P, 'Transforming US Police Surveillance in a New Privacy Paradigm', *Police Practice and Research*, 10.3 (2009), pp. 225 – 238, doi:10.1080/15614260802381083

Bright, David, Russell Brewer, and Carlo Morselli, 'Reprint of: Using Social Network Analysis to Study Crime: Navigating the Challenges of Criminal Justice Records', *Social Networks*, 69 (2022), pp. 235–50, doi:https://doi.org/10.1016/j.socnet.2022.01.008

Brill, Julie, *The Intersection of Privacy and Consumer Protection*, in *The Cambridge Handbook of Consumer Privacy* (2018), doi:10.1017/9781316831960.020

Casagran, Cristina Blasi, *Surveillance in the European Union*, in *The Cambridge Handbook of Surveillance Law* (2017), doi:10.1017/9781316481127.028

Celeste, Edoardo, 'Digital Constitutionalism: A New Systematic Theorisation',

International Review of Law, Computers and Technology, 33.1 (2019), pp. 76–99, doi:10.1080/13600869.2019.1562604

Chan, Jason, Jin-Hyuk Kim, and Liad Wagman, 'State versus Federal Wiretap Orders: A Look at the Data', *International Review of Law and Economics*, 70 (2022), p. 106064, doi:https://doi.org/10.1016/j.irle.2022.106064

Christianto, Hwian, 'From Crime Control Model to Due Process Model: A Critical Study of Wiretapping Arrangement by the Corruption Eradication Commission of Indonesia', *Padjadjaran Jurnal Ilmu Hukum*, 7.3 (2020), pp. 421–42, doi:10.22304/pjih.v7n3.a7

Crain, Zachary, *Wiretapping*, in *The Encyclopedia of Civil Liberties in America: Volumes One-Three* (2015), III, doi:10.4324/9781315699868-738

Daalen, O L van, 'The Right to Encryption: Privacy as Preventing Unlawful Access', *Computer Law & Security Review*, 49 (2023), p. 105804, doi:https://doi.org/10.1016/j.clsr.2023.105804

Desai, Deven R, 'Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding', *Notre Dame Law Review*, 90.2 (2015), pp. 579 – 632 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84922426795&partnerID=40&md5=6f205f1d1149dd6f7d3895c6ddb07a22>

Dewi, Sinta, 'Privacy: An Overview of Indonesia Statutes Governing Lawful Interception', *Central European Journal of International and Security Studies*, 12.4 (2018), pp. 587 – 597 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059703271&partnerID=40&md5=5e245cd4c7825b92670008c0042f95f5>

Dobinson, Ian, and Francis Johns, 'Qualitative Legal Research', 1 in *Research Methods for Law*, ed. by Mike McConville and Wing Hong Chui (Edinburgh University Press Ltd., 2007)

Elena, Tudurachi, 'Wiretaps Interference of Public Authorities in the Right to Privacy and Correspondence', *Procedia - Social and Behavioral Sciences*, 116 (2014), pp. 4591–95, doi:https://doi.org/10.1016/j.sbspro.2014.01.991

Elwyn, Glyn, and others, 'Individuals Recording Clinical Encounters: A Review of Applicable Law in Multiple Countries', *Communication and Medicine*, 19.1 (2024), pp. 58 – 76, doi:10.1558/cam.20257

Fadhil, Mohammad, 'The Harmonization of Wiretapping Regulations in Indonesia: Law Enforcement Perspective', *Substantive Justice International Journal of Law*, 3.2 (2020), pp. 125 – 146, doi:10.33096/substantivejustice.v3i2.75

Fanchiotti, Vittorio, and Jean Paul Pierini, 'Impact of Cyberspace on Human Rights and Democracy', *2012 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings* <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84866634610&partnerID=40&md5=3ac14c2ba8c53f5b07e4acd5525461e4>

'FBI Outlines a Wiretapping Future', *Network Security*, 1995.11 (1995), pp. 2–3, doi:https://doi.org/10.1016/1353-4858(95)90144-2

Gleave, Stephen, 'The Mechanics of Lawful Interception', *Network Security*, 2007.5 (2007), pp. 8 – 11, doi:10.1016/S1353-4858(07)70034-X

——, 'The Mechanics of Lawful Interception', *Network Security*, 2007.5 (2007), pp. 8–11, doi:https://doi.org/10.1016/S1353-4858(07)70034-X

Gollini, Isabella, Alberto Caimo, and Paolo Campana, 'Modelling Interactions among Offenders: A Latent Space Approach for Interdependent Ego-Networks', *Social Networks*, 63 (2020), pp. 134–49, doi:https://doi.org/10.1016/j.socnet.2020.07.001

Grabosky, Peter N, and Russell G Smith, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, in *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities* (2018), doi:10.4324/9780203794401

Gregorio, Giovanni De, and Roxana Radu, 'Digital Constitutionalism in the New Era of Internet Governance', *International Journal of Law and Information Technology*, 30.1 (2022), pp. 68–87, doi:10.1093/ijlit/eaac004

Griebel, Cornelia, and Franziska Hohl Zürcher, 'The Work of Intercept Interpreters in Lawful Communication Surveillance: A Daily Trade-off between Formal Requirements and Informal Needs', *International Journal of Law, Crime and Justice*, 74 (2023), p. 100609, doi:https://doi.org/10.1016/j.ijlcj.2023.100609

Hancock, Bill, 'US Government Fighting for Expanded Wiretap Laws', *Computers & Security*, 19.6 (2000), p. 477, doi:https://doi.org/10.1016/S0167-4048(00)06003-X

——, 'Wiretaps in Europe — EU Debates a Resolution', *Computers & Security*, 18.5 (1999), pp. 388–89, doi:https://doi.org/10.1016/S0167-4048(99)90599-0

Katulic, Tihomir, and Goran Vojkovic, 'From Safe Harbour to European Data Protection Reform', *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings*, 2016, pp. 1447 – 1451, doi:10.1109/MIPRO.2016.7522367

Keesoony, Selina, 'International Anti-Money Laundering Laws: The Problems with Enforcement', *Journal of Money Laundering Control*, 19.2 (2016), pp. 130–47, doi:https://doi.org/10.1108/JMLC-06-2015-0025

Kestemont, Lina, *Handbook on Legal Methodology* (Intersentia, 2018), doi:10.1017/9781839702389

Klaaren, Jonathan, 'Human Rights: Legal Aspects', in *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, ed. by James D Wright, Second Edi (Elsevier, 2015), pp. 375–79, doi:https://doi.org/10.1016/B978-0-08-097086-8.86158-9

Koops, Bert-Jaap, and Rudi Bekkers, 'Interceptability of Telecommunications: Is US and Dutch Law Prepared for the Future?', *Telecommunications Policy*, 31.1 (2007), pp. 45–67, doi:https://doi.org/10.1016/j.telpol.2006.11.006

Landau, Susan, 'Security, Wiretapping, and the Internet', *IEEE Security and Privacy*, 3.6 (2005), pp. 26 – 33, doi:10.1109/MSP.2005.158

Leigh, Ian, 'Changing the Rules of the Game: Some Necessary Legal Reforms to United Kingdom Intelligence', *Review of International Studies*, 35.4 (2009), pp. 943 – 955, doi:10.1017/S0260210509990374

Liu, Qiao, and others, 'Wiretap Resisting and Privacy Preserving Data Exchange with Physical Layer Security and Blockchain Based Authentication in Internet of Vehicles', *Microprocessors and Microsystems*, 104 (2024), p. 104965, doi:https://doi.org/10.1016/j.micpro.2023.104965

Liu, Yantao, and Yasser Morgan, 'Security against Passive Attacks on Network Coding System – A Survey', *Computer Networks*, 138 (2018), pp. 57–76, doi:https://doi.org/10.1016/j.comnet.2018.03.013

Lock, Daniella, 'Form Over Substance: Human Rights Law's Search for Effective Protections Against the Abuse of Surveillance Powers', *European Human Rights Law Review*, 2022.3 (2022), pp. 299 – 309 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85135443824&partnerID=40&md5=4c64619bbe5af57c9c8694828bf1cb7a>

Ma, Yue, 'Prosecutorial Discretion and Plea Bargaining in the United States, France, Germany, and Italy: A Comparative Perspective', *International Criminal Justice Review*, 12.1 (2002), pp. 22 – 52, doi:10.1177/105756770201200102

Mahdy, Mohamad, Hartiwiningsih, and Isharyanto, 'Wiretapping Law in Indonesia; Realising Due Process of Law', *Asian Journal of Human Services*, 28 (2025), pp. 242 – 272, doi:10.14391/ajhs.28.242

Mahendra, Januar Rahadian, Edwin Setiawan, and Arbend Ficasso Van Hellend, 'Corruption Eradication in Four Asian Countries : A Comparative Legal Analysis', *Journal of Law, Environmental and Justice*, 2.2 (2024), pp. 162–84, doi:10.62264/jlej.v2i2.98

Meneses, Flavio G A de, Brian P Mulcahy, and Karolina Brook, 'Wiretap Laws and the Perioperative Physician – The Current State of Affairs', *Journal of Clinical Anesthesia*, 89 (2023), p. 111178, doi:https://doi.org/10.1016/j.jclinane.2023.111178

Moon, Han-Bit, Young-Kwang Jung, and Won-Sang Ra, 'Terminal Acceleration Stabilizing Guidance Law for Impact Angle Constrained Interception of a Non-Maneuvering Target', *International Journal of Control, Automation and Systems*, 13.6 (2015), pp. 1410 – 1422, doi:10.1007/s12555-014-0196-z

Muñoz, Alfonso, and others, 'Digital Wiretap Warrant: Improving the Security of ETSI Lawful Interception', *Digital Investigation*, 14 (2015), pp. 1–16, doi:https://doi.org/10.1016/j.diin.2015.04.005

Natamiharja, Rudi, and others, 'BALANCING TWO CONFLICTING PERSPECTIVES ON WIRETAPPING ACT: Rights to Privacy and Law Enforcement', *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, 22.1 (2022), pp. 18 – 30, doi:10.30631/alrisalah.v22i1.1226

Nguyen, Nam-Phong, and others, 'Secure Communications in Cognitive Underlay Networks over Nakagami-m Channel', *Physical Communication*, 25 (2017), pp. 610–18, doi:https://doi.org/10.1016/j.phycom.2016.05.003

Nurcahyo, Nanang, and others, 'Reform of the Criminal Law System in Indonesia Which Prioritizes Substantive Justice', *Journal of Law, Environmental and Justice*, 2.1 (2024), pp. 89–108, doi:10.62264/jlej.v2i1.91

Pakes, Francis, *Comparative Criminal Justice, Second Edition*, in *Comparative Criminal Justice, Second Edition* (2012), doi:10.4324/9780203118290

Prakasa, Satria Unggul Wicaksana, and P E Noviandi Nur, 'Analysist of Cyber Espionage in International Law and Indonesian Law', *Humanities and Social Sciences Reviews*, 7.3 (2019), pp. 38 – 44, doi:10.18510/hssr.2019.736

Pratiwi, L. Yes Esty, and others, 'In-Depth Review : Legal Review on Human Rights Enforcement in the ASEAN and EU Context', *Journal of Law, Environmental and Justice*, 1.3 (2023), pp. 202–24, doi:10.62264/jlej.v1i3.16

Price, David H, *The American Surveillance State: How the U.S. Spies on Dissent*, in *The American Surveillance State: How the U.S. Spies on Dissent* (2022) <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85209977301&partnerID=40&md5=641c5519f8626ad9fb3b622fc718cf7a>

Ramadhan, Tutik Nurul, Bambang Sugiri, and Yuliati, 'Dinamika Regulasi Penyadapan Dalam Undang-Undang Dan Putusan Mahkamah Konstitusi', *Media Iuris*, 5.3 (2022), pp. 529 – 556, doi:10.20473/mi.v5i3.34204

Reyes, Anthony, and others, 'Chapter 6 - Legal Issues of Intercepting WiFi Transmissions', in *Cyber Crime Investigations*, ed. by Anthony Reyes and others (Syngress, 2007), pp. 111–31, doi:https://doi.org/10.1016/B978-159749133-4/50007-3

Salet, Renze, and Jan Terpstra, 'Criminal Justice as a Production Line: ASAP and the Managerialization of Criminal Justice in the Netherlands', *European Journal of Criminology*, 17.6 (2020), pp. 826–44, doi:10.1177/1477370819828332

Saputra, Imran Eka, and Muhammad Miftah Fauzan, 'The Authority of the Supervisory Board in the Supervision of the Corruption Eradication Commission in Indonesia', *Journal of Forensic Science and Medicine*, 11.3 (2025), pp. 186 – 194, doi:10.4103/jfsm.jfsm_100_21

Saputra, Rian, M Zaid, and Devi Triasari, 'Executability of the Constitutional Court ' s Formal Testing Decision : Indonesia ' s Omnibus Law Review', *Journal of Law, Environmental and Justice*, 1.3 (2023), pp. 244–58, doi:10.62264/jlej.v1i3.18

Sarabdeen, Jawahitha, 'Protection of the Rights of the Individual When Using Facial Recognition Technology', *Heliyon*, 8.3 (2022), p. e09086, doi:https://doi.org/10.1016/j.heliyon.2022.e09086

Sasono, Satryo, Isharyanto Isharyanto, and Delasari Krisda, 'Child and Women Domestic Abuse Victims ' Social Health Insurance Protection : An Affirmative Justice Perspective', *Journal of Law, Environmental and Justice*, 1.2 (2023), pp. 105–21, doi:10.62264/jlej.v1i2.8

Sherr, Micah, and others, 'Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps', *Proceedings of the ACM Conference on Computer and Communications Security*, 2009, pp. 512 – 523, doi:10.1145/1653662.1653724

——, and others, 'Signaling Vulnerabilities in Wiretapping Systems', *IEEE Security and Privacy*, 3.6 (2005), pp. 13 – 25, doi:10.1109/MSP.2005.160

Spalt, Bernhard, 'Current Challenges for Lawful Interception (LI)', *World Telecommunications Congress 2010, WTC 2010*, 2010, pp. 164 – 169 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092058893&partnerID=40&md5=17f1a2f72821c454c5ae57a1e7bd7f09>

Suhendi, Dadang, and Erwin Asmadi, 'Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia', *International Journal of Cyber Criminology*, 15.2 (2021), pp. 135–43, doi:10.5281/zenodo.4766552

Sun, Jia-Rong, Mao-Lin Shih, and Min-Shiang Hwang, 'Cases Study and Analysis of the Court Judgement of Cybercrimes in Taiwan', *International Journal of Law, Crime and*

Justice, 43.4 (2015), pp. 412–23, doi:https://doi.org/10.1016/j.ijlcj.2014.11.001

Thongraweewong, Kanathip, 'State Telecommunication Surveillance: A Comparative Study of the US and Thai Telecommunication Privacy Laws', *2014 4th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2014*, 2014, pp. 347 – 352, doi:10.1109/DICTAP.2014.6821709

Vöeneky, Silja, *Espionage, Security Interests, and Human Rights in the Second Machine Age: NSA Mass Surveillance and the Framework of Public International Law*, in *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (2017), doi:10.1017/CBO9781316658888.019

Volovelsky, Uri, 'Civilian Uses of Unmanned Aerial Vehicles and the Threat to the Right to Privacy – An Israeli Case Study', *Computer Law & Security Review*, 30.3 (2014), pp. 306–20, doi:https://doi.org/10.1016/j.clsr.2014.03.008