LEGAL REFORM OF INTERCEPTION OF COMMUNICATIONS:
An initiative to establish an interception of communications law from human rights perspective

Authors:

Wahyudi Djafar
Bernhard Ruben Fritz Sumigar
Blandina Lintang Setianti

Institute for Policy Research and Advocacy (ELSAM)
Privacy International
2016

LEGAL REFORM OF INTERCEPTION OF COMMUNICATIONS:
An initiative to establish an interception of communications law from human rights perspective

Authors:

Wahyudi Djafar
Bernhard Ruben Fritz Sumigar
Blandina Lintang Setianti

First published in Indonesian by:
Institute for Policy Research and Advocacy (ELSAM) and Privacy International, 2016

All ELSAM publications are dedicated to victims of human rights violations, in addition to being a part of the effort to advance and protect human rights in Indonesia.

Except where otherwise noted, content on this report is licensed under a Creative Commons Attribution 3.0 License. Some rights reserved.

TABLE OF CONTENTS

CHAPTER I INTRODUCTION

CHAPTER II INTERCEPTION OF COMMUNICATIONS AND RIGHT TO PRIVACY: CONCEPTUAL BASIS

A. Privacy: Definition and Scope
B. Right to Privacy as a Human Right
C. Interception of Communications: Scope and Types
D. Ensuring Lawful Interception of Communications

CHAPTER III MODELS OF REGULATION OF COMMUNICATIONS INTERCEPTION

A. General Principles in the Regulation of Communications Interception
B. Separation of Intelligence Needs (National Security) and Rule of Law
C. Regulation of Interception of Communications in Various Countries

CHAPTER IV REGULATION OF COMMUNICATIONS INTERCEPTION IN INDONESIA

A. Privacy and Prohibition of Unlawful Interception of Communications
B. Interception of Communications in Various Legislations

CHAPTER V PROPOSAL FOR CHANGE: FORMULATION OF A LAW ON COMMUNICATIONS INTERCEPTION WITH A HUMAN RIGHTS PERSPECTIVE

A. Form of the Legal Regulation Related to Interception of Communications
B. Objectives of Communications Interception
C. Procedures for the Implementation of Communications Interception
D. Agencies Authorised to Conduct Interception of Communications
E. Agencies Supervising the Conduct of Interception of Communications
F. Remedy for Parties Harmed by Interception of Communications

CHAPTER VI CONCLUSION

ORGANISATIONAL PROFILES

CHAPTER I
INTRODUCTION

In the process of amendment of Law No. 11 of 2008 on Information and Electronic Transaction, which took place in mid-2016, the House of Representatives (DPR) and the Government have agreed to reconfirm Constitutional Court Decision No. 5/PUU-VIII/2010, on the need for the establishment of a Law on the Procedures for Interception of Communications. According to the Constitutional Court, establishment of this legislation is important to ensure the legal unity of interception of communications, as part of the principle of legal certainty, which must be adhered to by a modern constitutional state such as Indonesia. Although a variety of sectoral laws give the authority of interception of communications to a number of state institutions, especially the state intelligence and law enforcement institutions, these various mandates must be bound together in the same procedure, to provide legal certainty in the procedures.

This legal-political agreement is then accommodated by the House of Representatives and the Government in Article 31 paragraph (4) of Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 on Information and Electronic Transactions. The provision confirms that the further rules regarding the interception of communications are set by law. That is, this clause expressly gives orders to the legislators (the House of Representatives and the President) for the immediate establishment of a Law on Interception of Communications, which will regulate everything, especially the procedures for interception of communications.

In addition to the mandate to establish, in fact a number of laws and regulations in Indonesia have also acknowledged that interception of communications is an action with an intrusive nature on the civil liberties of a person, especially in the private life of a citizen. Therefore, granting this authorisation shall be applied in a limited manner, limited to particular needs and functions: national security and law enforcement. This acknowledgment of the prohibition of unlawful and arbitrary interception of communications can be found, for example, in the Criminal Code, Law No. 36 of 1999 on Telecommunications, and the Law on Information and Electronic Transactions.

The prohibition for intercepting communications unlawfully and arbitrarily is also consistent with the guarantee of protection of the right to privacy, which is granted by the 1945 Constitution. The formulation of the amendment to the Constitution has put the right to privacy as one of the constitutional rights of citizens, which are guaranteed and protected in their implementation. The same thing can also be found in Law No. 39 of 1999 on Human Rights, and the International Covenant on Civil and Political Rights, which has been ratified by Indonesia through Law No. 12 of 2005.

The existing background of constitution, legislations and top-level judicial decisions are of course more than enough to encourage the importance of the establishment of a Law on Interception of Communications, whose existence would be one of the features of the Indonesian legal state, affirming Article 1 (3) of the 1945 Constitution.

The need for a Law on Interception of Communications also increasingly gains a sociological and practical basis, given the increasing practices of intrusion towards communication and personal lives of citizens. The increasingly intrusive practice is in line with innovations and rapid development of information and communication technology, which also result in increasingly

open private spaces of communication between individuals, vulnerable to the possible intrusion of others. Intrusion to privacy is no longer solely committed by state institutions, such as intelligence or law enforcement agencies, but also individuals or private corporations for the sake of personal gain or business interests. In the case of Indonesia, intelligence agencies of other countries practice interception of communication to the users of telecommunication services in Indonesia. This practice has been revealed to be carried out, for example, by the intelligence services of Australia, New Zealand, the United Kingdom, and the United States.[1]

In practice, interception of communications is no longer limited to recording technology (wiretapping) or circuit-switched networks to packet-switched networks that have traditionally been specifically designed for telephone lines. It has evolved into other forms, such as cell phone monitoring, video monitoring, and intrusion technology, including monitoring of the Internet, such as e-mail and Skype communications. The high level of Internet penetration in Indonesia, which according to a survey from the Indonesian Internet Service Provider Association (APJII) has already reached more than half of Indonesia's population, definitely provides greater opportunities for this intrusive practice.[2]

This situation is also recognised by intelligence agencies and law enforcement officials in various countries, which generally state that in line with the development and growth of information and communication technology, there has been an increased need to use technologies for the interception of communications. Therefore, the term was changed into communications interception technology, because it is no longer limited to wiretapping of phone calls, but also of a variety of other communication devices. Telecommunication is no longer limited to long-distance phone calls, but implies a wider scope reaching all forms and methods of communication such as mobile phones, e-mail, text messaging and Skype.[3]

Departing from the legal and constitutional foundations mentioned above, as well as the practical sociological needs for the protection of privacy rights of citizens from the practice of unauthorised and arbitrary interception of communications, the Interception of Communications Law must be formulated. The existence of this law, other than being in line with Indonesia's constitutional and international obligations on human rights, is also necessary to keep pace with the needs of today's law, which is surrounded by increasingly rapid use of information and communication technology. The high penetration of the Internet in Indonesia, of course, requires a number of legal reform processes, including those related to legal interception of communication, so that the law will be compatible with the special characteristics of the Internet, as well as the right to privacy protection requirements, as well as other public and social interests.

The writing of the results of this study is meant to observe the extent of legal interception of communications in Indonesia. It also presents a comparison of several countries. From observations and the comparison, the final part of this paper intends to provide recommendations for policymakers (government and parliament), for reviewing and renewing the law on interception of communications in Indonesia.

CHAPTER II

[1] For further information see Wahyudi Djafar and Miftah Fadhli, *Surveillance dan Hak Asasi Manusia: Rekomendasi Pengintegrasian Standar Hak Asasi Manusia dalam Pembentukan Kebijakan Surveillance di Indonesia*, (ELSAM and Privacy International, 2015).
[2] See: "More than Half of Indonesians are Internet Users", in http://jakartaglobe.id/news/half-indonesians-internet-users/.
[3] Mitchell Congram, Peter Bell, and Mark Lauchs, *Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology*, (London: Palgrave Macmillan, 2013).

INTERCEPTION OF COMMUNICATIONS AND RIGHT TO PRIVACY: CONCEPTUAL BASIS

A. Privacy: Definition and Scope

Along with the rapid innovations in information and communications technology, the issue of the right to privacy returns as a heated debate within the international community. One response was given by the UN Special Rapporteur on the right to freedom of opinion and expression, who declared that advances in information technology and communication have resulted in increasing the frequency of state action in conducting surveillance of its citizens, either in the form of interception of communications, data collection (data mining), or other surveillance practices. Not only is the state, similar practices are also carried out by private corporations for their business interests. Therefore, ensuring the protection of privacy as part of human rights is essential in nature, as the basis for each activity underlying information and communication technology in this digital era. It is expected that rapid and unbounded information exchange remains able to protect people's privacy.

As an inherent right of persons, the debate about the importance of the protection of a person's right to privacy initially surfaced in the court decisions in the United Kingdom and then in the United States. Samuel Warren and Louis Brandeis wrote the legal conception of the right to privacy in Harvard Law Review Vol. IV No. 5, 15 December 1890. The article, titled "The Right to Privacy", was the first to conceptualise the right to privacy as a legal right.[4] This paper appeared when newspapers began printing photographs of persons for the first time. In the article, Warren and Brandeis simply defined the right to privacy as "the right to be let alone". Their definition was based on two levels: (i) personal honour; and (ii) values such as the dignity of the individual, personal autonomy and independence.[5] The idea was later justified and recognised with the existence of several lawsuits that provided justification of the need for protection of the right to privacy, particularly based on morality grounds.

Developing the concept built by Warren and Brandeis, William L. Prosser (1960) tried to detail the scope of coverage of a person's right to privacy, with reference to at least four forms of interference against one's self, namely:[6]

(A) Disruption of seclusion or solitude, or disruption of personal relationships;
(B) Public disclosure of embarrassing private facts;
(C) Creating a false public impression;
(D) Misappropriation of name or likeness for the expropriator's advantage.

Alan Westin (1967) defined the right to privacy as a claim of individuals, groups, or institutions to determine for themselves about when, how, and to what extent information about them is communicated to others. The breadth of coverage usually creates various regulations regarding

[4] See: Samuel Warren and Louis Brandeis, The Right to Privacy, in *Harvard Law Review* Vol. IV No. 5, 15 December 1890, available at http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. The idea of these two Boston lawyers derived from the idea first stated by Judge Thomas Cooley in *Treatise on the Law of Torts* (1880), which first introduced the term 'the right to be let alone'.

[5] See E. Bloustein, Privacy as An Aspect of Human Dignity: an Answer to Dean Prosser, in *New York University Law Review* Vol. 39 (1964).

[6] William L. Prosser, "Privacy: A Legal Analysis", *California Law Review* 48: 338-423, 1960.

privacy in a country, both in kind and degree.[7] It is similar to the concept put forth by Arthur Miller (1971), which emphasised the concept of privacy on the individual's ability to control the dissemination of information related to himself.[8]

Julie Innes (1992) defined privacy as a condition when a person has no control over the private sphere of their decision, which includes decisions on private access, private information and private action. 'Private' itself was described as a product of love, joy and concern for others.[9] This is in line with the explanation of Solove (2008), which stated that the privacy context includes the family, the body, sex, home, and personal communications of a person.[10] Gavison (1980) saw privacy as a 'complex' concept, which consists of 'three independent and irreducible elements, namely: confidentiality, anonymity and solitude'. Each element is independent, and thus 'loss or infringement may occur as a result of encroachment against one of the three elements.[11]

Of the various proposed definitions of "privacy", it seems that they tend to cluster into several themes: those that essentially put privacy as a claim or right of the individual to determine what information about himself can be passed on to others; or as a measure of control of the individual against a number of elements of his personal life, which includes: (i) personal information; (ii) confidentiality of personal identity; or (iii) parties who have sensory access to a person's identity.[12]

B. Right to Privacy as a Human Right

In the compendium of international law of human rights, the conception of privacy legally formulated appeared for the first time in the provisions of Article 12 of the Universal Declaration of Human Rights of 1948, which states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Based on the Declaration, privacy is recognised as a human right that can be enjoyed by the entire international community. Every individual shall have autonomy, liberty, including interacting, in a "private space" with or without other people. Moreover, an individual also has the right to be free from state intervention and/or excessive intervention of other individuals. The provision is later restated in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which states:

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

According to Manfred Nowak (2005), the concept of the right to privacy under Article 17 of the ICCPR is closely related to the aspect of the right of access and control of one's data. Therefore,

---

[7] A. F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), pp. 7-8.
[8] Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, (Ann Arbor: University of Michigan Press, 1971) p. 25.
[9] Julie C. Inness, *Privacy, Intimacy, and Isolation*, (New York: Oxford University Press, 1992), p. 140.
[10] For further information see Daniel J. Solove, *Understanding Privacy*, (Cambridge, MA: Harvard University Press, 2008).
[11] Ruth Gavison, Privacy and the Limits of Law, in *Yale Law Journal* 89: 421-71 (1980).
[12] Ferdinand Schoeman, "Privacy: Philosophical Dimensions", in Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, (Cambridge: Cambridge University Press, 1984), p. 2.

the authority of the public and individuals or entities whose activities are related to the collection and storage of personal information on computers or data banks with other mechanical devices must have a legal justification. This means that the authority relating to a person's information should be regulated by law. This is mentioned by Nowak to ensure that information relating to a person's private life does not fall to parties who do not have the legal authority to receive, process and use it. This also includes utilisation of the information if it does not comply with the ICCPR.[13]

Nowak's explanation is in line with the elaboration formulated in General Comment No. 16 adopted by the Committee in 1988. This comment specifically provides a number of limitations of the interpretation of the provisions of Article 17 of the ICCPR. In this commentary, it is explained that the protection of the right to privacy aims to protect individuals from any unlawful interference and other arbitrary actions against one's privacy, family, home or correspondence, and the national legal framework should provide protection of this right.

This provision imposes certain obligations relating to the protection of privacy in communication. ICCPR underlines that any form of correspondence must be delivered to the addressee without interception and without opening or reading it. Besides, all forms of scanning, using either electronic or other devices, interception by telephone, telegraph and other forms of communication, wire-tapping and recording of conversations, should be prohibited. In the general comment, it was also confirmed that gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or individuals or the private sector, must be regulated by law.

The general comment at least has given a more detailed picture about the notion of 'arbitrary interference' or 'unlawful interference' to privacy. In that sense, the following elements are found: interference to privacy can only be done in cases stipulated by law; interference that are implemented on the basis of legislation must meet the following prerequisites: (i) conform/not conflict with the provisions and objectives of the Covenant (ICCPR); (ii) logical in certain contexts; (iii) describes in detail the specific conditions that justify interference to privacy; (iv) can only be performed by an authority designated by the legislation; and (v) only implemented on a case by case basis.[14]

In the context of international legal protection of human rights, in addition to the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), the guarantee to the protection of the right to privacy also appears in a number of international human rights conventions, and also several regional instruments. It is found in the provisions of Article 16 of the Convention on the Rights of the Child; and the provisions of Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families. In regional instruments, it can be found in the provisions of Article 8 of the European Convention on Human Rights; the provisions of Article 11 of the American Convention on Human Rights; and the provisions of Article 21 of the Arab Charter on Human Rights. The recognition has also been given in the ASEAN Human Rights Declaration of 2012, in point 21, which states:

[13] Manfred Nowak, *U.N. Covenant on Civil and Political Rights CCPR Commentary*, 2nd rev. Ed., (Kehl: N.P. Engel Verlag, 2005) pp. 401-402.

[14] See CCPR/C/GC/16, General comment No. 16, Article 17: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation, accessible at http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument.

> Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks.

The recognition and guarantee of the various international law and regional human rights instruments to the right to privacy have confirmed the right to privacy as a human right. It also gave rise to State responsibility for developing various legal instruments that thoroughly consider the rights of its citizens. Also included in the context are regulations at the national level aimed at creating the ideal and balanced conditions for all stakeholders in the framework of respect for human rights.

C. Interception of Communications: Scope and Types

Within the scope of privacy, as explained above, interception of communications as a form of intrusion on someone's private communications, is one form of violation of the right to privacy, besides various other forms of violations. In describing the various forms of violations of the right to privacy, Solove (2008) developed a "taxonomy of privacy", which classified different forms of violations of privacy into four basic categories: collection of information; processing of information; dissemination of information; and invasion; as well as 16 sub-groups: surveillance; interrogation; aggregation; identification; insecurity; secondary use; exclusion; breach of confidentiality; disclosure; exposure; increased accessibility; extortion (blackmail); appropriation; distortion; intrusion; and interference in decision-making (decisional interference).[15]

Interception of communications is the development of the telephone recording (wiretapping) whose technology was first used for reasons of national security (intelligence) as well as law enforcement. In its development, this practice is no longer solely limited to wire recording and tapping via placing a device on the radio or telephone network, but has experienced various forms of expansion.[16] Straw (1999) argues that the definition of interception of communications should be based on the process. According to him, interception of communications can occur when communication between two or more people who use a system for handling communications is monitored secretly to further understand their conversational content. Straw does not restrict the definition to the technical systems for the monitoring, whether snooping at the content of messages sent over the telephone network, electronic mail, or paper or wireless transmission. When the element of 'entering certain communications network' is carried out in secret in order to observe the speech content, it has become an activity that is definable as interception.[17]

In subsequent developments, even the term has shifted to *surveillance*, which of course has implications for the expansion of the scope and use, including advantages and disadvantages. The term was first introduced by Michel Foucault (1975), who attached surveillance practices to the structure of the Panopticon prison – a prison model designed by Jeremy Bentham – that is, a structure consisting of a wall encircling a high tower in the middle of the complex. The Panopticon is a watchtower from which observers can monitor the entire activities of inmates living within the circular wall, all 360 degrees of them. Broadly speaking, surveillance is

[15] Daniel J. Solove, *Understanding … op. cit.*, pp. 104-105.
[16] Whitfield Diffie and Susan Landau, *Privacy on the Line The Politics of Wiretapping and Encryption*, (Massachusetts: MIT Press, 2007), p. 173.
[17] Jack Straw, 'Interception of Communications in the United Kingdom: A Consultation Paper' (Home office, 1999).

intended to bring a more modern attitude of discipline. The operational power of technology takes up the arena of power to discipline, control or normalise behaviour.[18]

Anthony Giddens (1985) put surveillance as a 'symbol of collective coordination activities performed by a particular institution'. Giddens emphasised surveillance technology as an instrument to facilitate coordination in a function. He saw the phenomena of countries using surveillance to mobilise administrative functions. Giddens imagined that the control of information would be the main means for concentrating authoritative sources involved in the management of state power.[19]

Meanwhile, Frank La Rue (2013) in his report as the UN Special Rapporteur on Freedom of Expression and Opinion defined surveillance of communications as acts comprising of monitoring, interception, collection, containment and storage of information to be communicated, delivered or produced through communications networks by a third party to a group of recipients.[20] The third party in question here could include law enforcement agencies, intelligence agencies, private companies, as well as those with malicious intent.

The practice of surveillance itself has been done since a long time ago, following each development of information and communication technology instruments. In the past, especially during the world wars, the work of a letter courier was not easy, due to vulnerability of blocking or stopping by force, breaking of seals or reading without permission. Along with the development of communication technology, the process of 'intercepting' conversation was conducted via a recorder or a parabolic microphone. Examples include telephone tapping (wiretapping) to theft of the communication waves.

In its development, surveillance of communication no longer required human intervention to record, intercept or read text information or communications of the parties. It can even be done on a mass scale, or at least a more disturbing scale, such as installation of malicious software (malwares) on computers. Despite surveillance becoming one of the alternatives to solve contemporary world problems (such as terrorism, narcotics trafficking, cyber crime, etc.), it still raises concerns because of its ability to explore certain information without the knowledge of the owner of information.

In practice, some forms of surveillance are carried out by means of cooperation with the telecommunications operators based on the authorities' requests. The mechanism to request the cooperation of telecommunications providers is often regarded as justifiable by the pro-surveillance party, especially when the law requires operators of communications services to provide information to law enforcement authorities or intelligence agencies. This is often mentioned in the transparency report issued by the telecommunications companies.

In addition to cooperation with operators, there are also methods or means of surveillance that enable the authorities to have direct access to telecommunications networks and services and perform tapping or recording. This is done by government agencies without the knowledge of the service provider using communications surveillance technology that interface directly with

[18] Michel Foucault, *Discipline and Punish*, (New York: Vintage Books, 1995), pp. 195-228.
[19] Anthony Giddens, *The Nation-State and Violence: Volume Two of a Contemporary Critique of Historical Materialism*, (Cambridge: Polity Press, 1985).
[20] See: "Report of Special Rapporteur on the Promotion and Protection of the right to Freedom of opinion and expression, Frank La Rue", accessible at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

the communication lines. One of these technologies is IMSIcatcher that can disguise itself into a base mobile station, to collect information from mobile phones in the vicinity.

In its development, as noted above, as information and communication technologies are increasingly becoming more sophisticated, it has become easier for a diverse set of practices for accessing communication networks: starting from the telegraph, landline to mobile phones and the Internet. That is, this fact also opens opportunities for more advanced surveillance technology equal to the sophisticated communication technologies, so as to conduct greater levels of surveillance to obtain much more information than the previous technology. Surveillance of communication is not limited to inhibition of the delivery of messages or attaching tapping implements through crocodile clips on the phone line. More than that, there are currently a number of cutting-edge methods in surveillance of communications, namely: (i) Internet monitoring; (ii) tapping of cell phones (mobile phones); (iii) interception of landline telephone; (iv) video monitoring; (v) location monitoring; and (vi) communication intrusion technology. A number of these communications surveillance practices, both on the Internet, mobile phone, or a landline, can be done with or without the cooperation of the telecommunications network operator.[21]

1. Internet monitoring

Internet monitoring is the act of capturing data in transit on the Internet to the intended destination. The units monitored or captured are commonly termed 'packets'. Packets are bits of data (messages, e-mails, pictures, Web pages and files) sent through Internet protocol, broken down by the computer into smaller units, delivered through computer networks and reassembled in the destination into the messages, e-mails, pictures, Web pages and files served to the recipient on their screens. Infrastructure supporting the Internet includes physical infrastructure and electronic systems connecting the entire globe. Internet monitoring can occur at any point in the infrastructure, depending on which information is being collected.

2. Cell phone tapping

Cell phone tapping is the act of collecting information sent through cellular telephone networks. One of the most common forms of cell phone tapping is the use of IMSI Catcher technology. Placing the technology in certain locations, it will masquerade as a BTS that can net all cell phones in the surrounding area to enter its network, and find out the unique identification number of the cellular phone, known as IMSI.

3. Landline phone interception

This refers to the act of intercepting information passing landline telephone networks (PSTN), which is the basis of the international communications network. The initial form of this interception technology is the placing of a tapping device on the physical network of the telephone landlines. More modern forms of the technology operate on a similar basis, in which a device is placed on the telephone network, allowing it to monitor all telephone calls. As networked computer technology develops and communications become faster, the scale of interception of landline telephones also increases exponentially. Currently, companies sell commercial grade telephone tapping technologies that allow tapping of entire telephone networks of a country.

[21] For further detail see Wahyudi Djafar, et al. (Eds.), *Privasi 101: Panduan Memahami Privasi, Perlindungan Data Pribadi, dan Surveilans Komunikasi*, (Jakarta: ELSAM and Privacy International, 2015).

4. Video monitoring

This technology focuses on night vision technology. In general, video-monitoring technology is deployed in public and private places for monitoring purposes. Closed-circuit television (CCTV) - a connected network that consists of still and video cameras – is increasingly used in public places, private companies and public institutions such as schools and hospitals. Systems that incorporate video surveillance technology have far greater powers than what the camera sees. Biometric technology uses videos submitted to create a profile, sort and identify population members through facial recognition software. The dangers posed by biometric technology will become more prominent along with improvement of the quality and coverage of video surveillance technology. Three-dimensional video cameras reduce the distorting effect of light on the face and allows for careful skin texture analysis. The development of such video technology will no doubt be applied in a useful context. However, the terrible ability made possible by such technologies is a major potential concern due to arbitrary implementation.

5. Location monitoring

Location monitoring technology tracks the location of the target through devices or networks. The device method uses software that records and reports the device's location using GPS or Wi-Fi position data. The network method looks for devices through performing computations on the radio signals transmitted to and from the communication device. Once the location is determined, the coordinates are transferred to a phone or computer interface that can present a visualisation of the current, past and predicted location, in addition to a variety of features such as tracking, satellite imagery and proximity alert. Location monitoring is often used without the consent of the target and is an effective tool to determine daily activities, deviations from regular activities and interpersonal interactions.

6. Communication intruder (intrusion technology)

This refers to the spread of malicious software (malware) on phones and computers. The malicious software, or Trojan, allows operators to take full control of the targeted device by embedding the tool in all system functions. These technologies include the most virulent forms of tapping technology that exists at present. With more and more communication devices attached to the communications network and becoming an integral part of our lives, we become increasingly dependent on storing personal information on these devices. This communication intrusion technology gives operators full access to communication devices and all the tools attached to it to copy and transmit data to the Trojan operator, without the users' awareness of the wiretapping because the communication device functions normally.

So far, communication intrusion technology can monitor everything that appears on the screen, keep track of keyboard entries and other input devices, and monitor content of communications sent from these devices, including communications made in the past, such as e-mail or conversations (chats). This technology can tap more information than what is contained in a communication device. Data intercepted by the operator can be recorded directly from the audio recorders and video cameras from the devices, so that communication devices belonging to the user becomes a means of surveillance itself: extracting information around the user, including intercepting users' conversations with others and monitor online and offline activities of the user.

D. Ensuring Lawful Interception of Communications

Referring to the provisions of Article 4 paragraph (1) of the ICCPR, it can be reiterated that the protection to the right of privacy is classified as a human right that is derogable (derogable rights). That is, the enjoyment of this right can be derogated in certain circumstances; insofar it is not in the form of arbitrary interference or unlawful interference.

The UN Human Rights Committee (HRC) defines the concept of arbitrary interference differently from unlawful interference. The concept of unlawful interference is completely prohibited, unless specified by the law that in principle is in line with the provisions and objectives of the ICCPR.[22] Put simply, all forms of activities that reduce a person's right of privacy or any disturbance outside the applicable law may be categorised as unlawful interference.

The concept of arbitrary interference, in turn, is a form of disturbance that although regulated law, is not in accordance with the corridors of reasonableness as determined by the Covenant (ICCPR).[23] Therefore any form of disturbance that is set within a legal framework, to be not classified as being arbitrary, must pay attention to the elements of limitation contained in the ICCPR and instruments relating to the Covenant.

Relying on the provisions of Article 17 paragraph (2) of the ICCPR, it is stipulated that every person has the right to legal protection against unlawful or arbitrary interference with their privacy. This means that any activity of interception of communication should be carried out on the basis of laws that are publicly accessible, which in practice must also comply with the rule of law. In the context of accessibility of the state to the privacy of its citizens, the legal regime of international human rights requires not only the issuance of a law as the basis for such access (prescribed by law), but also must strictly regulate the procedure for its implementation, as well as the consequences that may occur, which may require recovery for each person whose privacy is violated.

The state is obliged to ensure that any interference with the right to privacy of a person, family, home or correspondence, must be authorised by law that is: (a) publicly accessible; (b) contain provisions ensuring that the collection, access to and use of communication data are designed for legitimate and specific purposes; (c) quite appropriate, specifying in detail the precise circumstances in which any such interference is permitted, the procedure for authorisation, the categories of people who may be targeted for scanning, duration limit of the scan, and procedures for the use and storage of the data collected; and (d) provide effective protection against the possibility of abuse.

In the case a rule or law concerning the interception of communications includes the materials above or the state provides rules as above, as a guide in the practice of interception of communications, both in the interests of national security or law enforcement, then the practice is said to be lawful. Conceptually there are many definitions of the lawfulness of an act of interception of communications, referring to the legality of the law and the purpose of the implementation of such practices. Some experts in the UK claim that the practice of lawful interception has an important role to achieve national security. This practice is considered lawful when "the legally authorised process by the which network operators or services

[22] UN Doc.CCPR/C/GC/16 (1994) para. 3
[23] *Ibid.,* para. 4.

providers give law enforcement officials access to the communications (telephone calls, e-mail message, etc.) of private individuals or organisation".[24]

In essence, lawful interception is an oversight of communication activities in a legal manner on behalf of the law by a government agency (intelligence or law enforcement) that has the authority determined by a specific regulation, against an individual or group. One of the schemes of interception described in the journal 'Technical Aspects of Lawful Interception" published by the European Telecommunications Standards Institute is described as follows:[25]

Figure 1: Organizational flow chart for Lawful Interception

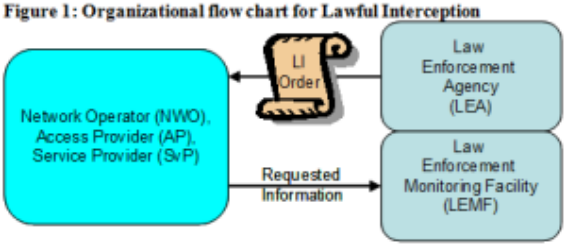
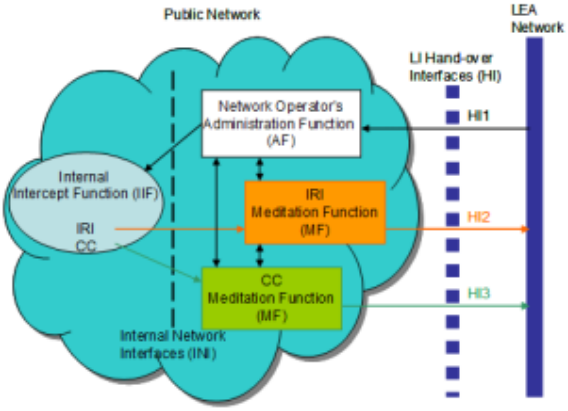


Figure 2: Generalised view of the Lawful Interception architecture



One of the yardsticks of the legality of an act of interception is the presence or absence of regulation that gives mandate to the authority, including the appropriate technical and regulatory requirements. It also has to regulate the relationship with security of digital forensic evidence when submitted at hearings.

The European Council Resolution is building international cooperation related to interception practices to create standardisation as the conditions to perform these activities. These standards are based on the necessity for legality of interception practices in some countries, thus simplifying the process of adoption of this standard. From the above description, an element of legal interception is the intent of protecting national security, investigating serious crimes, or combating terrorism. As one of the powerful tools to fight crime, on the other hand interception also backfires when used as a tool to commit a crime if there is no protection in the implementation. One issue is the legal vacuum related to ordinances in the interception of communication, so that the authority is used by the government to conduct reconnaissance and surveillance in order to control people's behaviour.

[24] Yochai Benkler, 'Overcoming Agoraphobia: Building the Commons of Digitally Networked Environment', in *Harvard Journal of Law & Technology 286* (1999).
[25] Can be accessed at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:1996:329:TOC.

The concept of unlawful interception is an action that has no legal basis and is done by those who do not have the legal authority to carry invasion of privacy. According to General Comment No. 16 'unlawful' means that no intervention should be allowed other than those allowed by law. Including interventions made by the state authorities, a legal basis underlying the practice of surveillance is required. The rules must also comply with the provisions, aims and objectives of respecting human rights. States have a duty to adopt a number of regulations and other legislative measures to prohibit arbitrary interception action as a form of assault to privacy rights.[26] It is also explicitly expected that arrangements to the right to privacy are protected by legislative, administrative and even the judicial authority.

[26] General Comment No. 16 for article 17 (*The right to respect of privacy, family, home and correspondennce, and protection of honour and reputation).* HRI/Gen/1/Rev.9 (Vol.1)

CHAPTER III
MODELS OF REGULATION OF COMMUNICATIONS INTERCEPTION

A. General Principles in the Regulation of Communications Interception

The efforts to protect the privacy rights from any form of intrusion for the basic freedoms to communicate, including the right to be free from the practice of interception of communications, is a concern to many parties in today's digital age. It is realised by the international community through establishing a basic principle that must be met by relevant stakeholders, named the International Principles on the Application of Human Rights to Communications Surveillance.[27]

The document issued by the UN Human Rights Council in 2013, and revised and re-launched in May 2014, is a result of a global consultation among civil society organisations, the business and international experts in the field of law, policy and communications technologies.

Up to the present, the international principles have been signed by more than 400 organisations and 300,000 individuals around the world, and have been endorsed by the Liberal Democratic Conference in the UK and in mainland Europe, Canada, and the German Parliament. Moreover, these principles have also been cited in the report of United States President Review Group on Intelligence and Communications Technologies, Inter-American Commission on Human Rights and others.[28]

As an instrument that has been widely accepted by the international community, this document contains thirteen principles that should be considered before the practice of lawful interception, namely:

1. The principle of legality;
2. The principle of legitimate aim;
3. The principle of necessity;
4. The principle of adequacy;
5. The principle of proportionality;
6. The principle of competent judicial authority;
7. The principle of due process;
8. The principle of users notification;
9. The principle of transparency;
10. The principle of public oversight;
11. The principle of honesty/integrity of communication and systems;
12. The principle of safeguards for international cooperation; and
13. The principle of safeguards against illegitimate access and the right to effective remedy.

These thirteen basic principles should be used as a reference for all countries in the world, including Indonesia, in formulating policies governing interception of communications in each of these countries. Therefore, in order to understand more about these principles, the following explanation of the thirteen principles in question is presented.

[27] See http://en.necessaryandproportionate.org/text (last accessed 17 November 2015).
[28] EFF and Article 19, *Necessary & Proportionate International Principles on the Application of Human Rights Law to Communications Surveillance: Background and Supporting International Legal Analysis*, (2014) p. 2.

1. The principle of legality

The principle of legality stresses that all forms of restrictions on human rights, particularly the right to privacy through the practice of interception of communications, should be regulated by law. The state should not be intercepting communications without laws that govern them. In addition, any legislation that restricts the enjoyment of human rights should be reviewed periodically, so these can still be effectively used in the face of rapid technological advances.

2. The principle of legitimate aim

Laws governing the interception of communications only allow any form of interception insofar it fulfils legitimate aims according to law and is not discriminatory.

3. The principle of necessity

Provisions of the legislation on the interception of communications may only be valid insofar it is necessary to achieve legitimate purposes, or when intercepting communications is seen as the least intrusive method of enforcement of international human rights. The burden of proof for this principle lies in countries that place the restrictions.

4. The principle of adequacy

Every act of communication interception ordered by law to be done ought to be done appropriately to fulfil legitimate purposes that are permitted by applicable law.

5. The principle of proportionality

Interception of communications should be implemented proportionally or commensurate with the objectives to be achieved. The level of proportionality of an interception of communication to the objectives to be achieved can be measured through the following indicators:

- ✓ The possibility for the emergence of a serious threat or a serious criminal offense;
- ✓ The likelihood that relevant evidence may be obtained;
- ✓ Interception of communication should be seen as the least intrusive means and should take into account sensitivities and other impacts arising;
- ✓ Information gathered from interception will be limited to things that are relevant, and all sorts of irrelevant information to be returned or destroyed;
- ✓ Information accessed will be used by the authorities for the purpose given to the party; and
- ✓ The use of interception of communications does not detract from the purpose of privacy rights or fundamental freedoms owned by the intercepted party.

6. The principle of competent judicial authority

Any decision relating to the interception of communications are to be made by legal authorities, not limited to the judiciary. That is, this authority can be given to government ministries or a special committee that has the specific authority in the field of interception of communications.[29] The legal authority should (i) be separate and independent from the

[29] UN Doc.A/HRC/23/40 (2013) para. 54.

institutions that perform interception actions, (ii) have knowledge relevant to the issue of interception and have the competence to make a legal decision on the legality of a practice of interception, and (iii) have the sufficient resources to carry out the mandate given.

7. The principle of due process

The principle of due process requires the participation of the state to respect and ensure the rights of every individual by providing a procedure that is lawful, consistent and known to the public in carrying out the practice of interception of communications.[30]

8. The principle of users notification

Every individual who becomes the target of interception practice must be informed about the decision that permits an act of interception of communication in due course and with adequate information, so as to give an opportunity to the intercepted party to raise objections against the decision of the interception to the authorities.

9. The principle of transparency

The state must be transparent about the use and scope of authority, power, activity, regulation and judicial actions related to interception of communications. In addition, the state must provide the applicant who will perform the interception with the requested information. The application note must also be published to the public.

10. The principle of public oversight

The state should establish an independent oversight mechanism to ensure transparency in the implementation of interception and accountability of perpetrators of communication interception. The party holding the oversight position is entitled to have access to potential information, to assess whether the state has taken the appropriate steps in interception, to evaluate whether the state has implemented the function of transparency, and to encourage the public to determine the legality of it.

11. The principle of honesty/integrity

To ensure the integrity, security and privacy of communications systems, and the recognition of the threat of national security and stability, the state should not compel service providers or hardware and software providers to establish communication devices that have the ability to carry out interception or monitoring, because everyone has the right to express himself in an anonymous manner through electronic means.[31]

12. The principle of safeguards of international cooperation

In the case states are bound by international obligations to a treaty of mutual legal assistance (mutual legal assistance treaty (MLAT)) or bilateral/other multilateral agreements) resulting in overlaps of jurisdictions, the provisions contained in the instruments of law should be able to

[30] This principle is closely tied to the provisions on the right to a fair trial in Article 10 of UDHR and Article 14 paragraph (1) of ICCPR.
[31] UN Doc.A/HRC/17/27 (2011) para. 82.

ensure that the services offered can guarantee protection of the right to privacy of a person from a form of communication interception practices involving parties from other countries.

13. The principle of safeguards against illegitimate access and the right to effective remedy

The state should establish a legislation that explicitly regulates the practice of unauthorised interception of communications, as well as providing an effective and adequate mechanism to provide remedy to a person whose rights have been violated by illegal interception practices.

B. Separation of Intelligence Needs (National Security) and Law Enforcement

As a form of practice that is often regarded as intrusive and in violation of the privacy of one's privacy, interception of communication is basically prohibited.[32] However, this prohibition is not absolute.

In certain occasions, a person's right to privacy can be limited by the practice of interception of communication, insofar as it is in conformity with the terms of the restrictions set forth in international human rights law.[33] The terms of the restriction of the right to privacy in question has been previously discussed by Frank La Rue, UN Special Rapporteur on Freedom of Opinion and Expression, in his report in 2013, which consisted of:[34]

1. All forms of limitation shall be regulated by law;
2. Restrictions must not violate the essence of the protection of human rights;
3. Restrictions must be conducted in a democratic society;
4. Restrictions should not curb the enjoyment of other human rights;
5. Restrictions must be absolutely necessary to achieve a legitimate purpose (necessity principle); and
6. Restrictions should be commensurate to the legitimate objective to be achieved (principle of proportionality).

Thus, the primary legitimacy of the implementation of the interception of communication as a form of restriction of the right to privacy, which is in conformity with international human rights standards, can be evaluated from the legitimate purpose to be achieved. According to Frank La Rue, the prohibition on the practice of interception can be transgressed as long as it is done for the administration of criminal justice, prevent crime or tackle terrorism.[35] In other words, at the international level, the recognition of the legality of interception of communications can be grouped into two categories, namely:

1. The interests of national security and intelligence; and
2. The interests of law enforcement.

The recognition of the justification of the interception of communications on the basis of national security and law enforcement interests is also in fact already publicly regulated in a number of legislations in Indonesia.[36] For the purposes of national security, Articles 31, 32 and 47 of Law No. 17 of 2011 on State have authorised a number of state intelligence institutions, including the State Intelligence Agency (BIN), Strategic Intelligence Agency (BAIS), Police

[32] UN Doc.CCPR/C/GC/16 (1994) para. 8; Decision of the Constitutional Court No.5/PUU-VIII/2010, (2011) para. 3.21.
[33] UN Doc.A/HRC/17/27 (2011) para. 59.
[34] UN Doc.A/HRC/23/40 (2013) para. 29.
[35] UN Doc.A/HRC/17/27 (2011) para. 59.
[36] Wahyudi Djafar and Miftah Fadhli, *Surveillance … op. cit., p.* 25.

Intelligence Agency (BIK), Attorney General Office of Intelligence, as well as, the Intelligence Offices of Ministries/Agencies for intercepting communications with close ties to national security.

For the purpose of law enforcement, the mandate to intercept communications is given not only to the investigating authorities of the Indonesian National Police (Polri). This authority is also expanded and given to other bodies, such as the Corruption Eradication Commission (KPK) and the National Narcotics Agency (BNN), to conduct wiretaps in corruption and narcotics cases that are being handled by each of these bodies.

Strictly speaking, in a legal and civilised state, the guarantee of the protection of personal privacy rights from all kinds of interference, including from interception of communications, is absolutely necessary. Therefore, communications interception activities should be limited strictly to governing laws in effect, solely for legitimate purposes as set out in international law.

C. Regulation of Interception of Communications in Various Countries

Recently, the practice of interception of communications has become commonplace in various countries. Therefore, a number of countries in the world have provided legal frameworks at the domestic level that can be used to respond to the needs of legal certainty and the protection of human rights of such practices. States with sufficiently high technology literacy rate are already preparing packages of legal policies that outline in detail issues that need to be regulated related to the implementation of interception of communications.

To see the various practices in different countries, the following section will described briefly the practices applied in four selected countries, namely, (1) the United States, (2) Australia, (3) the Philippines, and (4) United Kingdom, which can be used as a reference comparison in discussing the proposed policy changes related to interception of communications in Indonesia, which will be reviewed in Chapter V. The selection of these four countries is based on the success in these countries in providing comprehensive legal rules relating to the interception of communications.

1. United States

Regulations related to the interception of communications in the United States have had a long history. Although since 1862 a number of rules in some states had banned the practice of interception, these rules have not been confirmed at the federal level.[37] In 1928, the Supreme Court of the United States saw in *Olmstead v. United States* that the practice of interception of communications did not conflict with the guarantee of the right to privacy, as set out in the Fourth Amendment to the US Constitution.[38]

It was only in 1934 that United States federal law prohibited the practice of interception of communications in the Federal Communications Act. Ironically, in the implementation, the law was often violated. This is due to executive power, who often continue this practice on the grounds of national security.[39]

[37] Thomas Wong, *Regulation of Interception of Communications in Selected Jurisdictions*, (2005) p. 17.
[38] *Ibid.*
[39] Sarah Boucher, et al., *Internet Wiretapping and Carnivore*, (2001) pp. 3,14.

The orientation of the protection of the right to privacy of every individual from the practice of communications interception practice experienced a shift in the 1960s, particularly in 1967 when the United States Supreme Court reversed its views in the *Olmstead* case by in *Katz v. United States* (40) [40] and *Berger v. New York*[41] that interception without a warrant was a violation of the Fourth Amendment to the US Constitution.

One year after the *Katz* and *Berger* decisions, the United States Congress published Title III of the Omnibus Safe Streets and Crime Control Act 1968 (Wiretap Act).[42] This began efforts in the United States to revitalise a number of other regulations to create a better legal framework of interception. This was evidenced by revisions to several legislations.

As an illustration, since 1986 the Wiretap Statute had been declared null and void and replaced by the Electronic Communications Privacy Act (ECPA), which was then revised in 1994 with the Communications Assistance for Law Enforcement Act (CALEA).[43] For the purposes of law enforcement and national security, a number of legislations in the United States also regulate the legality of interception of communications. This can be seen in the Foreign Intelligence Surveillance Act (FISA)[44], which was amended in 2008, and Pen Registers and Trap and Trace Devices chapter of Title 18 (Pen/Trap Statute).[45] The most recent renewal of the laws related to interception of communications in the United States is with the implementation of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act)[46], of which the status of validity has been extended to 2019.[47]

According to the Wiretap Act and the Pen/Trap Statute, interception of communications can only be done by law enforcement officials after having obtained an order from the judge of the lower court (US District Court) or level two (US Court of Appeals).[48] As for the interception mechanism in FISA, the party with the authority to conduct interception against foreign nationals is the FISA Court, which consists of 11 judges from the US District Courts appointed by the chairman of the Supreme Court of the United States.[49]

Legitimate purposes for interception of communication are confirmed in the Wiretap Act for cases related to violations of the following:[50] (50)

a. any offense punishable by death or by imprisonment for more than one year;
b. a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labour organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;
c. any offense which is punishable under the following sections of title 18 of the United States Code including bribery of public officials and witnesses, bank officials and in sporting contests; relating to nuclear and weapons of mass destruction, biological weapons; interference with commerce by threats or violence; terrorist attacks against

[40] *Katz v. United States*, 388 U.S. 41 (1967).
[41] *Berger v. New York*, 389 U.S. 347 (1967).
[42] 18 U.S.C. §§2510-2522 [*Wiretap Act*].
[43] 47 U.S.C. §§1001-1010 [*CALEA*].
[44] 50 U.S.C. §§1801-1811 [*FISA*].
[45] 18 U.S.C. §§3121-3127 [*Pen/Trap Statute*].
[46] 115 Stat. 272 (2001) [*USA PATRIOT Act*].
[47] Erin Kelly, "Senate approves USA Freedom Act", USA Today, 2 June 2015 <http://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/>.
[48] *Wiretap Act, op. cit.*, §2510(9); *Pen/Trap Statute, op. cit.*, §§3122,3127(2).
[49] *FISA, op. cit.*, §1803.
[50] *Wiretap Act, op. cit.*, §2516(a)-(r).

public transportation facilities; child obscenity; torture; hostage taking; fraud and related activity in connection with computers; conspiracy to harm persons or property overseas;

d. any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;
e. any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;
f. any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;
g. a violation related with the reporting of currency transactions, or relating to structuring transactions to evade reporting requirement prohibited;
h. any felony violation relating to interception and disclosure of certain communications and to certain intercepting devices;
i. any felony violation relating to obscenity;
j. any violation relating to destruction of a natural gas pipeline; aircraft piracy; assault on a flight crew with dangerous weapon; explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft;
k. any criminal violation the Arms Export Control Act;
l. the location of any fugitive from justice from an offense described in this section;
m. smuggling of aliens;
n. any felony violation relating to firearms;
o. any violation of section 5861 of the Internal Revenue Code of 1986 relating to firearms;
p. a felony violation relating to production of false identification documents; false statements in passport applications; fraud and misuse of visas, permits, and other documents; aggravated identity theft; relating to the smuggling of aliens;
q. any criminal violation relating to chemical weapons or terrorism;
r. any criminal violation relating to illegal restraints of trade or commerce; monopolizing of trade or commerce;
s. any violation relating to theft of medical products;
t. any cybercrime, computer crime and terrorism;[51] or
u. any conspiracy to commit any offense described in subparagraphs a-t.

Similar to the Wiretap Act, the Pen/Trap Statute also justifies the interception of all communications relevant to the investigation purposes of on-going criminal cases.[52] Meanwhile, the FISA states the following conditions relating to the legality of an interception:[53]

a. The President of the United States has given a permit to the Attorney General to approve the request for interception;
b. The application for interception has been made by a federal officer and approved by the Attorney General;
c. There is a probable cause to believe that a citizen of the United States targeted by electronic surveillance, is a foreign power or an agent of a foreign power, and each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of foreign power. An agent of a foreign power

[51] *USA PATRIOT Act, op. cit.*, §§201-202.
[52] *Pen/Trap Statute, op. cit.*, §§3122,3127(2).
[53] *FISA, op. cit.*, §1805(a).

includes persons who knowingly aids or abets any person engaging in clandestine intelligence activities, sabotage or international terrorism;
d. The institution conducting the surveillance has declared the adoption of minimisation procedures to obtain and disseminate information obtained from the surveillance.

Regarding the time span, the Wiretap Act allows communications interception of no more than 30 days and can be extended up to 30 days afterwards.[54] Meanwhile, according to FISA, interception of communications in general can only be done for 90 days. If the target of the interception is a foreign power, then the interception order can effectively apply for up to one year; whereas if the target is an agent of a foreign power, the interception order can only be exercised up to 120 days.[55] In the Pen/Trap Statute, interception of communications can be carried out during 60 days, which can be extended up to 60 days afterwards.[56]

Furthermore, regulations on interception of communications in the United States also made possible the interception of communications without a court warrant. This at least has been set in the Wiretap Act, FISA and the Pen/Trap Statute.

According to the Wiretap Act and the Pen/Trap Statute, interception of communications can be carried out by law enforcement established by the Attorney General, Deputy Attorney General or Associate Attorney General insofar it is done for emergency purposes of the following nature:[57]

a. The threat of danger can cause death or serious injury to a person;
b. Conspiracy activities that threaten national security;[58] or
c. Conspiracy activities that can be categorised as organised crime.

In its connection, procedurally, the two instruments require the party conducting the surveillance to submit an application for interception with the court no later than 48 hours after the interception was done. Thus, if the perpetrator does not apply for the interception or the court rejects the application, the interception is considered as an unlawful interception.[59]

According to the FISA, the implementation of interception of communications without a court order is only possible if the President, through the Attorney General, has been authorising electronic eavesdropping to obtain foreign intelligence information for a period of one year, insofar the Attorney General has certified the following:[60]

a. The surveillance is done solely to obtain communication data transmitted in particular among foreign powers; or to obtain technical intelligence of the property or place under the open and exclusive control of foreign powers;
b. The surveillance does not include communications in which one of the parties is "a United States person"; and
c. The party conducting interception has declared to implement the procedures eavesdropping by adopting minimisation procedures, and the Attorney General has

[54] *Wiretap Act, op. cit.*, §2518(5).
[55] Thomas Wong, *op. cit.*, p. 29.
[56] *Pen/Trap Statute, op. cit.*, §3123(c).
[57] *Wiretap Act, op. cit.*, §2518(7)(a).
[58] Thomas Wong, *op. cit.*, p. 32 (According to *Pen/Trap Statute*, conspiracy threatening national security is not definable as an emergency to allow interception without a court warrant).
[59] *Wiretap Act, op. cit.*, §2518(7)(b).
[60] Thomas Wong, *op. cit.*, p. 29-30.

reported the minimisation procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence no later than 30 days after the procedure is effective.

In terms of supervision, the Wiretap Act, FISA, or the Pen/Trap Statute has provided specific provisions on this mechanism. Supervision of the implementation of interception of communications in the United States is conducted by both judicial and legislative institutions. To understand more about the regulations associated with the supervisory mechanisms, the following table is presented:

Regulation	Supervisor		Description
	Category	Authorised Agency	
Wiretap Act	Judiciary	Administrative Office of the US Courts	The judge giving approval/non-approval of the interception, and the Prosecutor performing the interception have to give reports to the Administrative Office on the implementation of the interception activities.[61]
	Legislative	Parliamentary Committee	Committee on the Judiciary and Intelligence; House Permanent Select Committee on Intelligence; and Senate Select Committee on Intelligence are three parliamentary committees with the authority to supervise interception of communications implemented by law enforcement and intelligence bodies.[62]
		Congress	The director of the Administrative Office has to report in April every year about the reports received by the Office from the agencies performing and giving approval of interceptions.[63]
FISA	Judiciary	Administrative Office of the US Courts	The Attorney General has to deliver annual reports to the Administrative Office, the contents of which are classified.[64]
	Legislative	Parliamentary Committee	On a semi-annual basis, the Attorney General has to deliver a report to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.[65]
		Congress	The Attorney General has to deliver an annual report to the Congress on the practices of interception done by the Prosecutor's Office.[66]

[61] *Wiretap Act, op. cit.*, §2519(1)-(2).
[62] Thomas Wong, *op. cit.*, p. 26.
[63] *Wiretap Act, op. cit.*, §2519(3).
[64] Thomas Wong, *op. cit.*, p. 30.
[65] *Ibid.*, p. 31.
[66] *Ibid.*

Pen/Trap Statute	Judiciary	Administrative Office of the US Courts	Agencies conducting interception through pen/trap has to deliver a report to the Administrative Office.[67]
	Legislative	Congress	The Attorney General has to deliver annual reports to the Congress in relation to practices of interception done by the Prosecutor's Office.[68]

In addition, regarding the remedy mechanism for parties who feel that their right to privacy has been violated with the implementation of interception of communications, the Wiretap Act has established that the parties can exercise their right to lodge a complaint on the basis of:[69]

a. The communications network has been intercepted unlawfully;
b. The court order approving the interception has been inadequate; and/or
c. The Interception has been not carried out in accordance with the court order.

2. Australia

Prior to 1960, there had been no legal regime prohibiting the practice of interception of communications in Australia. The regulations associated with the practice began to emerge since 1950 when the Australian Prime Minister issuing a Regulation governing wiretapping conducted by the executive power specifically for cases related to espionage, sabotage and subversion.[70]

It was not until 1960 that a law was enacted that gave certain limitations on the implementation of the communications interception named the Telephonic Communications (Interception) Act. This provision was later repealed and replaced by the Telecommunications (Interception and Access) Act (Interception Act)[71] in 1979, which created a "Commonwealth legal monopoly of telephone interception," a power structure delegating the powers of interception to the authority of the states.[72] The existence of the Interception Act later developed into a major legal framework for Australia in regulating the practice of interception of communications in the country.

Based on the Interception Act, interception of telecommunications can only be justified for two fundamental objectives, namely, (i) national security and (ii) law enforcement.[73] In the case of national security, the Commonwealth Attorney-General can issue orders to carry out interception of communications. In addition, communication interception warrant on the grounds of national security considerations can also be issued by the Director General of Security of the Australian Security Intelligence Organization (ASIO). Delegation of authority to the Director General of Security of ASIO is only applicable to specific situations such as:[74]

a. Attorney-General within three months rejects the warrant issued by the Director General of Security of ASIO; and

[67] *Ibid.*, p. 32.
[68] *Pen/Trap Statute, op. cit.*, §3126.
[69] *Wiretap Act, op. cit.*, §2518(10)(a).
[70] Thomas Wong, *op. cit.*, p. 36.
[71] *Telecommunications (Interception and Access) Act*, (1979) [*Interception Act*].
[72] Reda Manthovani, *Penyadapan vs. Privasi*, (Jakarta: Bhuana Ilmu Populer, 2015) p. 172.
[73] Thomas Wong, *op. cit.*, p. 38.
[74] *Interception Act, op. cit.*, §10(1).

b. Director General of Security of ASIO has been satisfied with the facts of the case based on the investigation that justified the issuance of a warrant of the Attorney General and waiting for the Attorney General's decision will endanger national security.

Meanwhile, for the purposes of law enforcement, interception of communications is only possible for the investigation of the offenses at the first and second levels.[75] Violations of the first level include murder, kidnapping, narcotics and terrorism;[76] while second level violations include loss of life, serious personal injury, arson, drug trafficking, serious fraud, bribery, corruption, money laundering, cybercrime, and so on.[77] In the context of law enforcement, interception of communications could only be done by the Australian Federal Police (AFP), the Australian Crime Commission (ACC), and the competent authorities of the states or the Northern Territory in connection with ministerial decrees in force, including the Independent Commission Against Corruption, New South Wales Crime Commission, Police Integrity Commission, Queensland Crime and Misconduct Commission, Western Australian Anti-Corruption Commission, Inspector of the Police Integrity Commission, and Royal Commission into the Western Australian Police Service.[78]

In terms of supervision of communications interception activities, the legal framework in Australia has delegated the oversight authority to a number of bodies,[79] as presented in the table below.

Supervisor		**Description**
Category	**Authorised Agency**	
Executive	Ombudsman	The Ombudsman has the authority to perform inspection, at least twice in a year, to records of AFP and ACC in the issuance of warrants and acts of interception.[80]
Legislative	Joint Statutory Committee on the ACC	This committee has the authority to perform examination of the ACC annual reports and to deliver Committee Report on the performance of the ACC in implementing its function to the Parliament of Australia.[81]
	Parliamentary Joint Committee on ASIO, Australian Secret Intelligence Service (ASIS) and Defence Signals Directorate (DSD)	The Joint Committee on ASIO, ASIS and DSD has the authority to evaluate issues related to the ASIO, ASIS and DSD, including interception of communications conducted by the three agencies.[82]
	Standing Committees on Legal and Constitutional Affairs	The Standing Committees are general investigation committees of the Parliament of Australia with the authority to execute orders derived from annual reports of related ministries, including those published by the Attorney

[75] Reda Manthovani, *op. cit.*, p. 178.
[76] *Interception Act*, *op. cit.*, §5(1).
[77] *Ibid.*, §5D.
[78] *Ibid.*, §§5,34,39.
[79] Thomas Wong, *op. cit.*, p. 44-46.
[80] *Interception Act*, *op. cit.*, Ch.4A.
[81] Thomas Wong, *op. cit.*, p. 45.
[82] *Intelligence Services Act*, (2001).

		General with the authority to issue surveillance warrants for the interests of national security.[83]
	House of Parliament	The Attorney General must deliver the annual report to the House of Parliament related to the practice of interception conducted by the Prosecutor's Office for the purposes of law enforcement.[84]

In terms of remedy for victims of interception, the aggrieved party can file a civil suit to court. This arrangement has been stated in the Interception Act.[85] Furthermore, offenders of unauthorised interception can be given criminal sanctions.[86]

3. The Philippines

The narration of communications interception as a form of intrusion to a person's right to privacy has been recognised by the Philippines. This is reflected in the Constitution, which declares:

> "*The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.*"[87]

In its development, stipulations related to the interception of communications have been comprehensively regulated in sectoral legislations,[88] such as the Anti-Wiretapping Law (AWL),[89] Human Security Act (HSA),[90] and the Cybercrime Prevention Act (CPA).[91]

In the Filipino national legal system, in essence interception of communications is prohibited, and those committing it can be given criminal sanctions, as declared in the Penal Code,[92] AWL,[93] HSA[94] and the Electronics Engineering Law.[95] However, Filipino law opens the possibility of lawful communications interception in the case of the following:[96]

a. Treason;
b. Espionage;
c. Provoking war and disloyalty in case of war;

---

[83] Reda Manthovani, *op. cit.*, p. 182-183.
[84] *Interception Act*, *op. cit.*, §§100-103A.
[85] *Ibid.*, §107A.
[86] *Ibid.*, §105(2).
[87] *Constitution of the Philippines*, (1987) Article III (2)(1).
[88] PI and FMA, *Stakeholder Report to the Universal Periodic Review 27th Session – Philippines: The Right to Privacy in the Philippines*, (2016) para. 13 [Philippine UPR].
[89] *An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for Other Purposes*, (1965) RA No. 4200 [*AWL*].
[90] *An Act to Secure the State and Protect Our People from Terrorism*, (2007) RA No. 9372 [*HSA*].
[91] *An Act Defining Cybercrime, providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes*, (2012) RA No. 10175 [*CPA*].
[92] *Revised Penal Code of the Philippines*, (1930) RA No. 3815, Pasal 290.
[93] AWL, *op. cit.*, §§1-2.
[94] HSA, *op. cit.*, §16.
[95] *An Act providing for a More Responsive and Comprehensive Regulation for the Registration, Licensing and Practice of Professional Electronics Engineers, Electronics Engineers and Electronics Technicians, Repealing Republic Act No. 5734, Otherwise Known as the "Electronics and Communications Engineering Act of the Philippines", and for Other Purposes*, (2004) RA No. 9292, §35.
[96] AWL, *op. cit.*, §3; HSA, *op. cit.*, §7.

d. Piracy;
e. Mutiny in the high seas;
f. Rebellion, in commission and incitement to rebellion;
g. Sedition;
h. Kidnapping as defined by the Penal Code;
i. Violations of Commonwealth Act No. 616; and
j. Terrorism.

In procedure, the law enforcement, in this case the *Philippine National Police* (PNP) and the *National Bureau of Investigation* (NBI),[97] can conduct interception of communications insofar they have requested and obtained permission from the courts based on the above.[98] In the implementation, interception can only be done for a period of 30 days (for HSA and CPA),[99] (99) while in AWL the time period allowed for interception is 60 days.[100]

In an effort to ensure the implementation of lawful communications interception, the PNP and NBI receive internal supervision of the Department of Justice of the Philippines (DOJ).[101] Especially for interception of communications in terrorism cases, the HSA provides the oversight mandate to the Grievance Committee, led by the Ombudsman and consisting of the Solicitor General and representatives of the DOJ.[102] In addition to the Grievance Committee, the HSA also provides the authority to conduct surveillance for the legislature by establishing a Joint Oversight Committee, which is composed of five senators and five MPs elected semi-annually.[103]

Although the Philippines already has a number of institutions authorised to carry out surveillance of communication interception authorities, especially law enforcement officers, the law in the Philippines has not been adequately transparent regarding supervision of interception of communications made by intelligence agencies, including the National Security Council (NSC), Office of the National Security Adviser (ONSA), National Intelligence Coordinating Agency (NICA), National Intelligence Committee (NIC), National Intelligence Board (NIB), and the Intelligence Service of the Armed Forces of the Philippines (ISAFP).[104]

To guarantee the recovery of the rights of victims of interception, Filipino law has confirmed that everyone conducting interception of communication may be liable to criminal sanctions. Not only that, perpetrators of communication interception also have the responsibility to provide remedy to the injured party.[105] The determination of the amount of compensation is decided by the courts.

4. United Kingdom

[97] CPA, *op. cit.*, §§10,15; *An Act Expanding Republic Act No. 9208, entitled "An Act to Institute Policies to Eliminate Trafficking in Persons especially Women and Children, establishing the Necessary Institutional Mechanisms for the Protection and Support of Trafficked Persons, providing Penalties for Its Violations and for Other Purposes"*, (2012) RA No. 10364, §16(g).
[98] AWL, *op. cit.*, §3; HSA, *op. cit.*, §8.
[99] HSA, *op. cit.*, §10; CPA, *op. cit.*, §15.
[100] AWL, *op. cit.*, §3.
[101] CPA, *op. cit.*, §11.
[102] HSA, *op. cit.*, §56.
[103] *Ibid.*, §59.
[104] Philippine UPR, *op. cit.*, paras. 19-23; F. Domingo, "Philippine Intelligence Community: A Case for Transparency", in ADMU, *Security Sector Reform: Modern Defense Force*, (2014).
[105] *Civil Code of the Philippines*, (1949) RA No. 386, Article 32.

The evolution of human rights promotion in Europe accompanied by the rapid developments of communications technology in the 20th century are two fundamental factors that drive the formation of the rule of law regarding interception of communications in the United Kingdom.[106] It begins with the decision of the European Court of Human Rights in 1984 in the *Malone* case[107] which holds that the law and practice in England and Wales, which allow police to conduct interception of communications to James Malone, as violations of Article 8 paragraph (2) of the European Convention on Human Rights, guaranteeing the right to privacy of a person, as the legal regulations in England and Wales did not provide clarity on the scope and procedures of interception of communications by public authorities.

The imperfection of the law indicated in *Malone*[108] pushed the UK Parliament to publish the Interception of Communications Act (Act 1985) in 1985. However, the rule did not last long. In 2000, this instrument has been replaced by the Regulation of Investigatory Powers Act (RIPA).[109] Act 1985 was repealed because the European Court of Human Rights in *Halford*[110] noted that the Act did not have comprehensive provisions regarding interception of communications. Act 1985 only regulated interception of public telecommunications network and contained provisions relating to the interception of the private telecommunications network.

The enactment of RIPA in 2000 is regarded as a major step for the legal framework for the interception of communications in the UK, as well as an effort to uphold the European Convention on Human Rights at the national level after the publication of the Human Rights Act (HRA) in 1998. Unlike Act 1985, the scope of RIPA already extends to interception of the private telecommunication system.[111]

Procedurally, RIPA allows the interception of communications conducted with and without a warrant[112] from the Secretary of State, which consists of the Home Secretary and the Cabinet Secretary for Justice, as the competent authorities for issuing permits of interception of communications.[113] Particularly in the context of interception carried out with a warrant, the activity must consider the principle of proportionality[114] and necessity[115] to achieve the following legitimate objectives:[116]

a. The interests of national security;
b. Aiming to prevent or detect serious crime, both national and cross-border as well as closely associated with UK's obligations to MLAT provisions with other countries; or
c. Aiming to maintain the economic stability of the United Kingdom.

Specifically for interception carried out without a warrant from the Secretary of State, RIPA states that it is allowed as long as approval from the intercepted party has been obtained (provisions of Sections 3 and 4 of RIPA). Alternatively it is possible to carry out interception to

[106] Oxford Pro Bono Publico, *Legal Opinion on Intercept Communication*, (2006) p. 4.
[107] *Malone v. United Kingdom* (1984) 7 EHRR 14.
[108] D. Ormerod and S. McKay, "Telephone Intercepts and Their Admissibility", *Crim. L. Rev.* (2004) p. 19.
[109] *Regulation of Investigatory Powers Act* (2000) c.23 [RIPA].
[110] *Halford v. United Kingdom* (1997) 24 EHRR 523.
[111] RIPA, *op. cit.*, §1(2).
[112] *Ibid.*, §§1(5),5.
[113] *Ibid.*, §7(1)(a).
[114] *Ibid.*, §5(2)(b).
[115] *Ibid.*, §5(2)(a).
[116] *Ibid.*, §5(3).

obtain information or evidence as long as it conforms with the provisions of Schedule 1 Police and Criminal Evidence Act 1984.[117]

In the legal system in the United Kingdom, implementation of interception of communications can only be done by security agencies and intelligence services, and law enforcement officials.[118] The agencies in question can be seen in the following table.

APPROVED PARTIES TO IMPLEMENT INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM	
Intelligence Services and Security Agencies	**Law Enforcement**
Security Service (MI5)	Police of the Metropolis21
Secret Intelligence Service (MI6)	Police Service of Northern Ireland
Government Communications Headquarters (GCHQ)	Territorial Police Forces of Scotland based on Police (Scotland) Act 1967
National Criminal Intelligence Service (NCIS)	Her Majesty's Revenue and Customs (HMRC)
Defence Intelligence Staff (DIS) 2	

To ensure the protection of the right to privacy of every individual in the United Kingdom from all forms of interception of communications made by the agencies above, RIPA delegates supervision of the implementation of these activities to the Interception of Communications Commissioner (IOCC).[119] Not only is the IOCC, the mandate of oversight of interception of communications conducted by MI5, MI6 and GCHQ is held by the Intelligence and Security Committee (ISC), a parliamentary committee.[120] Furthermore, to ensure remedy to victims of interception, RIPA also authorised the Investigatory Powers Tribunal (IPT) to receive complaints from the public.[121]

Based on the description above, it is clearly seen that attempts to protect the right to privacy from the practice of communications interception have been made by the governments of the four countries. In order to more easily compare the practices in these countries, the following table shows the comparison of the regulations pertaining to communications interception in these four countries.

Country	Regulation	Lawful objectives	Procedure	Oversight	Remedy
United States	✓	✓	✓	✓	✓
Australia	✓	✓	✓	✓	✓
The Philippines	✓	✓	✓	✓	✓
United Kingdom	✓	✓	✓	✓	✓

Based on the summary, it is understood that these four countries already have laws that specifically mention interception of communications. In the legislations provided by each country, the objectives and procedures for lawful interception have also been described. Additionally, these countries also have determined rigid procedures on which parties are entitled to conduct interception of communication, and which parties oversee the

[117] *Ibid.*, §1(5).
[118] *Ibid.*, §6(2).
[119] *Ibid.*, §57.
[120] Thomas Wong, *op. cit.*, p. 11.
[121] RIPA, *op. cit.*, §§65-69.

implementation. In fact, some of these countries also provide specific rules related to the remedy mechanism for parties who feel aggrieved by a practice of communications interception.

CHAPTER IV
REGULATION OF COMMUNICATIONS INTERCEPTION IN INDONESIA

A. Privacy and Prohibition of Unlawful Interception of Communications

Indonesian law recognises and guarantees the protection for citizens' rights to privacy. This is enshrined in the Second Amendment to the 1945 Constitution, which took place in 2000. The recognition of the right to privacy as one of the constitutional rights of citizens is defined in the provisions of Article 28G (1) of the 1945 Constitution, which states:

> Every person shall have the right to protection of him/herself,[122] family, honour, dignity, and property, and shall have the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right.

In addition, the 1945 Constitution also provides guarantees for everyone to communicate, seek, obtain, possess, store, process and convey information by employing all available channels. The warranty is defined in the provisions of Article 28F of the 1945 Constitution. Thus, referring to the 1945 Constitution, communication and information, including the private lives of citizens, are protected rights, and should not be arbitrarily interfered with. It is also to ensure that everyone can freely express their expressions and opinions.

Prior to the Amendment, respect for the right to privacy of a person had actually appeared in a number of laws and regulations in Indonesia, even during the colonial period. This is seen in the Penal Code and the Civil Code. The provisions of Chapter XXVII of the Penal Code on Crimes of Position, Article 430 to Article 434 regulate the prohibition of unlawful interception of communication. The Civil Code regulates civil legal relationships between persons or entities, which allows for a lawsuit if the right to privacy is being violated by the other party.

The prohibition of unauthorised and arbitrary interception of communications (unlawful interception), which has close links with the safeguard of the right to privacy can also be found in a number of provisions of law, such as Law No. 5 of 1997 on Psychotropic Substances, Law No. 36 of 1999 on Telecommunications, Law No. 18 of 2003 on Advocates, Law No. 21 of 2007 on the Eradication of Trafficking in Persons, and Law No. 19 of 2016 on the amendment of Law No. 11 of 2008 on Information and Electronic Transactions (ITE). The ITE Law does not only regulate the prohibition of wiretapping/interception of communication against the law, but also prohibits (on a limited basis) the arbitrary transfer of personal data. It is stipulated in Article 43 paragraph (1) of ITE Law, which states that any investigation in the field of ITE shall be "made with due regard to privacy protection, secrecy, smooth running of public services, data integrity, or data entirety ...."

The guaranteed protection of the right to privacy in general, other than found in the provisions of the 1945 Constitution, has also been defined in the provisions of Law No. 39 of 1999 on Human Rights, in particular through the following articles:

[122] This article corresponds to the similar article in UDHR, but with 'privacy' translated as 'him/herself' and re-translated into English.

Article	Contents
Article 29 paragraph (1)	Everyone has the right to protection of the individual, his family, opinion, honour, dignity, and rights.
Article 30	Everyone has the right to security and protection against the threat of fear from any act or omission.
Article 31 paragraph (1)	No one shall be subject to arbitrary interference with his home.
Article 31 paragraph (2)	No one shall set foot in or enter the enclosure of a house or enter a house without the permission of the person who lives there, except for reasons provided for under prevailing legislation.
Article 32	No one shall be subject to arbitrary interference with his correspondence, including electronic communications, except upon the order of a court or other legitimate authority according to prevailing legislation.

In the elucidation of Article 31 of Human Rights Law, the definition of arbitrary interference has been clearly outlined with reference to the private life (privacy) in one's place. This explanation confirms the residence of individuals as an area whose protection is guaranteed as part of a personal life. However, there is no further reference to whether the definition of 'home' refers to domicile, or in a more factual sense, referring to a place where the individual is located. Protection in the Human Rights Law is further strengthened by the ratification of the International Covenant on Civil and Political Rights into Indonesian national law, through Law No. 12 of 2005.

Relying on the provisions of the protection above, the entire practice of surveillance in Indonesia, as part of the restrictions on the right to privacy, must be based on the principles of limitation, either regulated by national law, or by international instruments of human rights that have been ratified. The main reference of restrictions on human rights in the 1945 Constitution is stipulated in the provisions of Article 28J paragraph (2) of the 1945 Constitution, which states:

> In exercising his/her rights and freedoms, every person shall have the duty to accept the restrictions established by law for the sole purposes of guaranteeing the recognition and respect of the rights and freedoms of others and of satisfying just demands based upon considerations of morality, religious values, security and public order in a democratic society.

Formulations with similar emphasis also appear in Article 70 and Article 73 of the Human Rights Law. Later, the Constitutional Court through its decision asserted that the practice of eavesdropping/interception of communications, to be categorised as lawful, must be regulated in a special law to protect the right to privacy of citizens.[123] Citing expert opinion in Case No. 5/PUU-VIII/2010, the Constitutional Court said that legislation concerning the procedures for the interception of communications should at least regulate: (i) the authority to perform, instruct or request the interception of communications, (ii) the specific purpose of interception of communications, (iii) categories of legal subjects that are authorised to intercept communications, (iv) consent of superiors or permission of judges before the interception of communications, (v) procedures for the interception of communications, (vii) supervision of the interception of communications, and (viii) use of the results of the interception of communications. Furthermore, the Court said that the interception is permitted only when

[123] See Decision of the Constitutional Court No. 5/PUU-VIII/2010, dated 24 February 2011.

fulfilling the following prerequisites: (i) a statutory authority designated by law to give permission to the interception of communications (usually the Chairman of the Court), (ii) the guarantee of a definitive period in the interception of communications, (iii) limitations on the handling of materials resulting from interception of communications, and (iv) restrictions regarding who can access the interception of communications.

Thus, in general, the Indonesian legal framework and constitution have guaranteed protection of the right to privacy of its citizens. This includes a number of activities regarding restrictions or limitations on the enjoyment of these rights, such as the practice of interception of communications, insofar the concepts, rules and practices do not violate the principles of human rights.

B. Interception of Communications in Various Legislations

In many countries, conceptually and practically, interception of communications or surveillance activities can only be done for either of the two following interests: national security, implemented in the intelligence function; and law enforcement. However, in Indonesian law, in general, the practice of communication interception or wiretapping is allowed by various laws for law enforcement, state intelligence, and enforcement of judges' code of ethics.

Procedurally, each of the legislations giving the authority for interception of communications for different state agencies also has different procedures. As a result, there is no unity of law, resulting in lack of legal certainty in the practice of communications interception in Indonesia. This situation has the potential of threatening the protection of civil rights of citizens, especially in their personal communications. The different regulations on interception of communications can be seen in the following legislations:

1. Law No. 8 of 1981 on the Criminal Procedural Code (KUHAP)

Based on Article 47 of the Criminal Procedure Code, the investigator has the authority to access one's personal letter sent through the post office or telecommunications, department or communications or transport company, if the object is suspected on reasonable grounds to have a relationship with a criminal case being examined. The authority is dependent on a procedure granting special permission from the Chairman of the Court.

In Article 48, if after opening and examination, it turns out that the letter is connected with the case under review, the letter is attached to the case file. Whereas, if there is no connection with the case, the letter is to be re-sealed and immediately handed back to the post office and telecommunications, department or communications or other transport company, and stamped stating that the letter "has been opened by an investigator" with the date, signature and the identity of the investigator. In addition, investigators and officials at all levels of checks in the judicial process must keep confidential on the strength of the oath of office regarding the contents of the returned letter.

2. Law No. 5 of 1997 on Psychotropic (Psychotropic Law)

Essentially the Psychotropic Law is intended to complement the provisions of Article 47 of the Criminal Procedural Code, and at the same time provide specialised law in the legal procedures of the crime of psychotropic substances. In Article 55, it is stated that investigating police officials can tap telephone conversations and/or other electronic telecommunication devices carried by persons suspected or strongly believed to discuss issues relating to the crime of

psychotropic substances. The tapping is to last for a maximum period of 30 (thirty) days. Furthermore in the elucidation, it is stated that tapping a telephone conversation and/or other electronic communications tools can only be done on the written instruction of the Head of Indonesian Police or an appointed official.

3. Law No. 31 of 1999 on the Eradication of the Crime of Corruption (Anti-Corruption Law)

The provisions of Article 26 of the Anti-Corruption Law state that in the process of investigation, prosecution, and examination of corruption cases, the investigator has the authority for interception (wiretapping). In addition to wiretapping, the provisions of Article 30 also provides authority for investigators to open, inspect and confiscate letters and packages sent by mail or other communication devices belonging to the suspect. Wiretapping can be done if investigators have enough evidence, and only conducted against information related to the suspected case of corruption in question. Obtaining evidence by way of interception is possible if there is a suspicion based on a report that a crime of corruption has happened or will happen, and its validity is determined by judges, consisting of career and ad hoc judges in the trial process.

4. Law No. 36 of 1999 on Telecommunications (Telecommunications Law)

The Telecommunications Law sets legal protection of the civil liberties of citizens' telecommunication activities from unlawful interception practices. The provisions contained in Article 40 and Article 42 paragraph (1) expressly prohibit any form of tapping on information transmitted over telecommunications networks, and require telecommunications service providers to maintain the confidentiality of information telecommunication users.

The provisions also contain exceptions, that tapping can be done in the interests of criminal proceedings upon written request to the Attorney General and/or the Chief of Police, as well as authorised investigators.[124] The Telecommunications Law also includes criminal sanctions against eavesdropping practices that exceed the allowed provisions with the minimum penalty of two years or a maximum of up to 15 years in prison and/or paying a fine of two hundred million rupiahs.

5. Law No. 30 of 2002 on the Commission for the Eradication of Corruption (Anti-Corruption Commission Law)

In the comprehensive efforts to eradicate corruption, particularly in the conduct of the inquiry, investigation, and prosecution, the Law gives authority to the Commission to undertake a number of actions that can interfere with a person's right to privacy. In Article 12 of the Law, in particular points (a), (c) and (f), it is stated that the Commission has the authority to conduct wiretaps and record conversations, inquire about the finances of the suspect or the accused and request property and taxation data from banks or financial and related institutions.

Similarly to the Anti-Corruption Law, the Anti-Corruption Commission Law also does not provide further guidance on the mechanism of the authority of tapping and management of the data obtained by the Commission through the intervention measures. In fact, under Article 47,

[124] See the technical mechanism in Articles 87-Pasal 89 of Governmental Regulation No. 52 of 2000 on the Implementation of Telecommunications Services.

KPK investigators are allowed to conduct expropriation without permission from the chairman of the District Court if they have enough initial evidence.

6. Law No. 15 of 2003 on the Eradication of the Crime of Terrorism (Anti-Terror Law)

The Anti-Terror Law is the endorsement of Government Regulation in Lieu of Law No. 1 of 2002, which was passed shortly after the Bali bombing in October 2002. The provisions of Article 31 of the Anti-Terror Law mentions that with sufficient preliminary evidence, investigators have the right to access personal data such as letters, and to install a wiretap on a telephone conversation or other communication tools. The activity of tapping can only be done on the orders of the Chairman of the District Court with a validity period of 1 year. Those responsible for the investigating authority is the superior of the investigators referred to in Article 31 paragraph (3). The tapping mechanism provisions in the Anti-Terrorism can be said to be quite comprehensive, explaining the procedures and oversight of the tapping authority, including the duration of the wiretapping that is limited to one year.

7. Law No. 21 o f2007 on the Eradication of the Crime of Trafficking in Persons (Anti-Trafficking Law)

The Anti-Trafficking Law provides authority for investigators to intrude on someone's privacy in order to combat the crime of trafficking in persons in Indonesia. Included in the authority is one to conduct wiretapping and accessing personal data of suspects or those who allegedly committed the crime.

In the case of wiretapping, Article 31 of the Anti-Trafficking Law mentions that investigators can conduct wiretaps by telephone or other communication tools, which must be based on sufficient preliminary evidence. In addition, paragraph (2) mentions that the tapping procedure must go through the written permission of the Chairman of the Court, with a maximum validity period of one year.

It shows this Law has regulated a number of procedures and oversight, as well as limitations related to wiretapping authority committed by law enforcement. However, the Anti-Trafficking Law does not explain the limit on the extension of the time period for wiretapping. In addition, this legislation does not have provisions about remedy, if in the implementation, the wiretapping activities have been prejudicial to the rights of privacy of a third person who was not involved in the crime.

8. Law No. 35 of 2009 on Narcotics (Narcotics Law)

In an effort to eradicate narcotics crimes in Indonesia, this law gives authority to the National Narcotics Agency (BNN) to conduct a series of activities that reduce a person's enjoyment of the right of privacy. One of these activities is conducting wiretaps on activities related to abuse, illicit trafficking and drug precursors committed by suspects as stipulated in Article 75 point (i) of Narcotics Law.

In practice, the tapping mechanism for the crime of drug abuse is regulated under Article 77, which states that tapping can be done after investigators obtain sufficient preliminary evidence, with a period of 3 months after receiving the permit. The permit letter is obtained from the Chairman of the Court permit referred to in paragraph (2). In paragraph (3) it is explained that wiretapping can be extended once, for the same time period, with no set limit on how many times the extension can be granted.

Under Article 78, the investigator is allowed to conduct wiretaps without written permission of the Chairman of the Court. In paragraph (2), it is stated that within a twenty-four hours period, the investigator is required to request permission in writing to the Chairman of the Court.

9. Law No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering (Money Laundering Law)

Referring to the provisions of Article 44 point h of the Money Laundering Law, one of the authorities of PPATK (Financial Transaction Analysis Reporting Centre) is to give recommendations to the law enforcement agencies about the importance of interception or eavesdropping on electronic information and/or electronic documents in accordance with the provisions of the legislation. Further provisions on the implementation of this authority are not regulated in detail by this law.

10. Law No. 17 of 2011 on State Intelligence (State Intelligence Law)

Under the terms of Article 30 of State Intelligence Law, in carrying out its duties and functions, the State Intelligence Agency is equipped with the authority to conduct wiretaps, checking the flow of funds, and extracting information on targets related to: a. activities that threaten national security interests including ideological, political, economic, social, cultural, defence and security matters, and other sectors of public life, including food, energy, natural resources and the environment; and/or b. acts of terrorism, separatism, espionage, and sabotage that threaten the safety, security, and national sovereignty, including those that are undergoing the process of law.

Furthermore, Article 31 stipulates that the intercepts on targets that have indications referred to are implemented as follows: a. for the implementation of intelligence functions; b. on the order of the Head of State Intelligence Agency; and c. the period of validity of a maximum of six months and may be extended according to needs (paragraph (2)). Wiretapping against targets that already have adequate preliminary evidence is validated by a determination of the Chairman of the District Court (paragraph (3)).

Besides, the State Intelligence Act also stipulates that any person aggrieved as a result of the implementation of the intelligence functions of the state can apply for rehabilitation, compensation and restitution. However, what is meant by "adversely affected by the implementation of intelligence functions" is not described in detail, including the procedure of filing the petition.

11. Law No. 18 of 2011 on the Judicial Commission (Judicial Commission Law)

The existence of the Judicial Commission in the Indonesian legal system is aimed at establishing an independent judicial authority in carrying out justice and law enforcement in Indonesia. To that effect, the Judicial Commission is then given a number of specific authorities, including conducting wiretaps. Article 20 states that the Commission may request law enforcement agencies to conduct wiretaps and record conversations the judge, if there are alleged violations of judicial ethics code.

In addition, to conduct surveillance, the Judicial Commission can request information or data to Courts and/or Judge and through the Supreme Court as provided for in Article 22. The data in question are information relating to the judicial process and the alleged violation of the code

of conduct. This law does not explain the extent of the procedures granting the authority, including lack of arrangements regarding surveillance, limitation and recovery procedures for aggrieved parties due to the implementation of this authority. Further, authorisation of wiretaps for the Judicial Commission is also conceptually and paradigmatically problematic, because internationally, rules and practice do not authorise the use of tapping for reasons of enforcement of code of conduct.

12. Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 on Electronic and Transaction (EIT Law)

As well as the Telecommunications Law, EIT Law also provides confirmation concerning the prohibition of unlawful communication interception or wiretapping. This action is only possible in the context of law enforcement at the request of the police, prosecution, or other institutions whose authorities are determined by law (paragraph (3)). Besides, EIT Law also mandates the establishment of laws concerning the procedures for interception, to further regulate the procedures of interception of communications.

In addition to legislations, provisions on communication interception or wiretapping are also regulated by a number of implementing regulations, of which the following are still valid, Government Regulation No. 52 of 2000 on the Provision of Telecommunications Services; Minister of Information and Communication Regulation No. 11 of 2006 on Technical Regulations on Information Interception; and Police Regulation of Interception Procedures in the Police Monitoring Centre.

Law	Objective	Institution	Permission required	Time limited	Oversight	Remedy
Criminal Procedural Code	Law enforcement	Investigators	√	-	-	√
Psychotropic Law	Law enforcement	Investigators	√	√	-	-
Anti-Corruption Law	Law enforcement	Investigators	-	-	-	-
Telecommunications Law	Law enforcement	Prosecutors, Police	-	-	-	-
Anti-Corruption Commission Law	Law enforcement	ACC	-	-	-	-
Anti-Terror Law	Law enforcement	Investigators	√	√	-	√
Anti-Trafficking Law	Law enforcement	Investigators	√	√	-	-
Narcotics Law	Law enforcement	BNN	√	√	-	-
Money Laundering Law	Law enforcement	PPATK	-	-	-	-
State Intelligence Law	National security	State Intelligence Agency	√	√	√	√
Judicial Commission Law	Ethics enforcement	Judicial Commission	-	-	-	-
EIT Law	Law enforcement	Police, Prosecutors, Other institutions	-	-	-	-

From the variety of laws that regulate the authority of interception of communications, one can observe procedural differences, which would give rise to a state of legal uncertainty, which would have an negative impact on the protection of civil liberties of citizens. These procedural

differences are as follows: *First*, the extent of which a communications interception decision can be made by an institution. The Psychotropic Law allows phone tapping and recording of conversations with the permission of Chief of Police (Article 55). The Narcotics Law allows BNN to conduct wiretapping with the permission of the Chairman of the Court, but in urgent circumstances, interception can also be done without a permit (Article 77 paragraph (2) of Narcotics Law). Similarly, the Anti-Terror Law also allows investigators to wiretap phones and record conversations only with the permission of the Chairman of the Court (Article 31 paragraph (2) of the Anti-Terror Law). The State Intelligence Law allows tapping as a function of state intelligence, based on the order of the chief of BIN, and must go through the determination of the Chairman of the District Court (Article 32 paragraphs (2) and (3)), if the wiretapping is to be used as evidence in court. In contrast, KPK investigators only require the decision of the Head of the Commission to be able to conduct phone tapping and recording of conversations in corruption cases, without permission of the Chairman of the Court (Article 12 paragraph (1) of the Anti-Corruption Commission Law). Tapping can also be done through a written request from the Attorney General (Article 87 letter a of GR 52/2000).[125]

Second, observing the time period allowed for the interception, the various laws in Indonesia mention differing time periods between a maximum of three months to indefinite. This situation occurs because the laws regulate the maximum time periods differently between each other. In the Narcotics Law, for example, wiretapping is permissible for a period of three months and can be extended for the next three months. The State Intelligence Law allows interception for a 6-month period, which can be extended as needed. That is, there is no definite time limit for the state intelligence in conducting wiretapping. This rule obviously potentially violates the protection of citizens' rights to privacy, because it allows intelligence organisers to conduct wiretapping all the time. The Anti-Terror Law allows the implementation of wiretapping for a maximum period of one year, while the Anti-Corruption Commission Law allows wiretapping to be conducted without a specific time period.[126]

[125] See Wahyudi Djafar and Miftah Fadhli, *op. cit.*
[126] *Ibid.*

CHAPTER V
PROPOSAL FOR CHANGE: FORMULATION OF A LAW ON COMMUNICATIONS INTERCEPTION WITH A HUMAN RIGHTS PERSPECTIVE

Taking into consideration the fact that currently there is no single legislation that specifically regulates interception of communications, the writers are outlining their ideas on the issue of amending the policies on interception of communications based on the perspective of international human rights law.

The use of the human rights perspective as the basis for consideration of the establishment of a policy on interception of communication is important, considering a rights-based approach is the conceptual framework for the process of human development that normatively refers to international human rights standards, whose operationalisation is directed to promote and protect human rights.[127] In a rights-based approach, plans, policies and processes of development must be based on a system of rights and obligations set out in international law. It is relevant, consistent and congruent with Indonesia's obligations under a number of international human rights treaties, particularly the International Covenant on Civil and Political Rights (ICCPR), to provide regulations based on the provisions contained in the ICCPR and other international human rights treaties binding for Indonesia.[128]

In outlining their proposal related to the proposed change in Indonesian policy of interception of communications, the authors fully take into account the principles set out in the International Principles on the Application of Human Rights to Communications Surveillance. Based on these international principles, there are at least six fundamental issues that need to be considered in formulating a single renewable rule associated with interception of communications in Indonesia, namely:

A. Form of the legal regulation;
B. Legitimate purpose in carrying out interception of communications;
C. Procedures for the implementation of interception of communications;
D. Agencies with the authority to carry out interception of communications;
E. Monitoring mechanisms of interception of communications; and
F. Effective remedy mechanisms for injured parties from the practice of interception of communications.

A. Legal Regulation Form Related to Interception of Communications

Before describing the appropriate form of legal regulation on interception of communications in Indonesia, it should be understood that legal regulations in force in Indonesia consist of various forms, inter alia, Legislation/Law, Government Regulation in Lieu of Law, Government Regulation, and Presidential Decree.[129]

Of these, the Indonesian Constitutional Court has determined that the context of interception of communications is appropriately regulated in a Law. This is reflected in Constitutional Court

[127] OHCHR, *Frequently Asked Questions on a Human Rights-Based Approach to Development Cooperation*, (2006) p. 15.
[128] *International Covenant on Civil and Political Rights*, (1966) Article 2(3)(b) [*ICCPR*].
[129] Law No. 12 of 2011 on Formulation of Legal Regulations, Article 7 para. (1).

Decision No. 5/PUU-VIII/2010 on Judicial Review of Law Number 11 of 2008 on Electronic Information and Transactions to the Constitution of the Republic of Indonesia of 1945, which reads:

> "*Considering that the Court deems necessary a specific Law that regulates wiretapping in general to the procedure of tapping for each of the competent institution. This Law is urgently needed because currently there are no synchronised regulations on wiretapping, which could potentially harm the constitutional rights of citizens in general;*
>
> *That a government regulation cannot set restrictions on human rights. A government regulation is only an administrative arrangement, and does not have the authority to accommodate the limitations on human rights*."[130]

Furthermore, the Constitutional Court also confirms that a Law on interception of communications must at least be capable of governing (i) the authority to perform, instruct or request interception; (ii) specific objectives of interception; (iii) the category of legal subjects that are authorised to conduct interception; (iv) permission of superiors or permission of judges prior to the interception; (v) procedures for interception; supervision of interception; and (vi) the use of the results from interception.[131]

Based on this consideration, the legal reform of interception of communications law in Indonesia must be arranged in the form of Legislation. To that end, the Government of Indonesia together with the House of Representatives have an obligation to immediately formulate a draft Law that specifically regulates wiretapping activities in the country in order to attain the guaranteed protection of the right to privacy of all those who may be limited by the practice of interception.

B. Objectives of Communications Interception

Based on the objectives, international human rights law recognises only two legitimate purposes in conducting interception of communications, namely, (i) interests of national security and (ii) interests of law enforcement.[132] In implementation, both reasons are oft used as rationales for the lawful practice of interception of communications in a number of countries, including the United States, Australia, the Philippines and the United Kingdom. In fact, in the context of law enforcement, practices in the United States, Australia and the Philippines have described in detail which criminal acts are eligible to be intercepted, which parties may conduct, and supervision of the act.

Considerations of national security and law enforcement are also recognised in a number of sectoral laws in Indonesia,[133] which authorise interception of communications. It is prominent in the State Intelligence Law, Criminal Procedural Code, Narcotics Law, Anti-Terror Law, and the Anti-Trafficking Law. However, an anomaly occurs in Indonesian law, in which the interest of enforcement of judges' codes of ethics provides authorisation to the Judicial Commission to conduct interception of communications. Although the exercise of powers is done by asking the help of law enforcement officers, paradigmatically, the awarding of the authority and the purpose for the interception of communications are problematic. Therefore, specifically for the purpose of enforcement of the code of conduct, there should be a review.

---

[130] Decision of the Constitutional Court No. 5/PUU-VIII/2010, para. 3.23.
[131] Wahyudi Djafar and Miftah Fadhli, *op. cit.*, p. 16.
[132] See further in Chapter III section B.
[133] Description about the twenty legislations can be seen in Wahyudi Djafar and Miftah Fadhli, *op. cit.*, p. 17.

In essence, in order to ensure the protection of civil liberties of citizens, intrusion on their life in the form of interception of communications, should be possible only in the interests of national security (intelligence) and law enforcement. In addition, to ensure legal certainty of the practice of interception of communications, the Law to be formulated by policymakers should be able to mention in detail the boundaries of national security and law enforcement agencies in question, which justify the implementation of interception of communications in Indonesia. In other words, the policy to be drafted must be able to provide a list of criminal acts or legal actions that ought to be intercepted. It is important, considering that Indonesia is a state of law in accordance with the mandate in Article 1 (3) of the 1945 Constitution.

C. Procedures for the Implementation of Communications Interception

In accordance with the opinion of the Constitutional Court in Decision No. 5/PUU-VIII/2010, communications interception procedures are valid upon the following prerequisites:

1. A statutory authority designated by law to give permission (order) of the wiretapping;
2. A guarantee of a definitive period in wiretapping;
3. A restriction on the materials resulting from the interception; and
4. A restriction on who can access the wiretap, which will be described in more detail below.

In connection with the opinion of the Constitutional Court, and with regard to best practices in several countries as described in Chapter III, the authors are going to present their views in association with the procedures of authorised interception of communications.

First, the Law to be drafted should contain specific provisions on statutory authority that has the authority to issue permits to conduct wiretaps, in this case the chairman of the court. In urgent circumstances, interception of communication can be carried out without prior approval of the chairman of the court, but shall be reported to the chairman of the court within 48 hours after the interception was implemented. The chairman of the court is entitled to assess whether the interception carried out without the warrant is lawful or not, for the objectives to be achieved.

Second, the Law to be drafted must also contain specific provisions relating to the time allowed for intercepting communications. The time period for interception for the purpose of law enforcement and national security can be dissimilar, bearing in mind the impacts that may be caused.

Third, the Law to be drafted must also contain specific provisions on the handling of the materials resulting from the interception. That is, data obtained from an interception of communications are not to be used arbitrarily, but limited to purposes that are permitted by the licensor.

Fourth, another procedural aspect that needs to be considered in the implementation of the interception of communications is the limits about what parties can have access to interception. That is, only the law enforcement and intelligence institutions should be given the authority to carry out interception of communications.

In the absence of these four elements, the practice of interception of communications can be a threat to the enjoyment of the right to privacy in Indonesia. In addition to these, another issue

that needs to be given attention associated with the procedures regarding interception of communication is the procedure for interception of communications across state borders.

The practice of interception of communications made from countries abroad into Indonesia, and vice versa, is actually increasing nowadays, along with the rise of transnational organised crime practices. Therefore, the new Law is expected to provide a legal framework specifically for the practice of cross-border interception of communications.

D. Agencies Authorised to Conduct Interception of Communications

Given the legitimate purpose in the interception of communication is limited to the purposes of national security and law enforcement, then the parties that have the authority to carry out interception of communications should be those who have the mandate to safeguard national security (intelligence agencies) and to carry out the functions of law enforcement (law enforcement agencies). The parties in question are shown below.

AGENCIES CONDUCTING INTERCEPTION OF COMMUNICATIONS	
NATIONAL SECURITY AGENCIES	**LAW ENFORCEMENT AGENCIES**
State Intelligence Agency (BIN)	Attorney General's Office
Strategic Intelligence Agency of the Indonesian Military (BAIS)	Indonesian National Police
Police Intelligence Agency (BIK)	Corruption Eradication Commission
Intelligence of the Attorney General's Office	National Narcotics Agency
Intelligence of Ministries/Agencies	Police investigators
	Military prosecutors

However, there is a problem regarding the exercise of the powers of interception of communications in institutions holding dual roles as both state intelligence and law enforcement agencies. These include police intelligence, intelligence of the Attorney General's office, or semi-judicial agencies such as the Directorate General of Immigration of the Ministry of Justice and Human Rights, and the Directorate General of Customs of the Ministry of Finance. If they conduct interception of communications for intelligence or national security purposes, there is a need to have clear boundaries delineating the purpose from the law enforcement function. In addition, restrictions and transfer procedures must be given when an act of interception of communications originally performed for national security objectives is changed into interception of communications for law enforcement purposes. The terms and procedures between the two are clearly different, including concerning the authorisation of the court.

E. Agencies Supervising the Conduct of Interception of Communications

Another important aspect to be regulated in the policy package on interception of communications in Indonesia is the mechanism to monitor the conduct of interception of communication. This is considered necessary to prevent abuses carried out by agencies authorised to conduct interception of communications, which can threaten a person's right to privacy.

In essence, the supervisory authority should be given to a separate entity that is independent and free from any kind of interference or influence from the government.[134] It is affirmed in UN

[134] Wahyudi Djafar, et al., *Perlindungan Data Pribadi di Indonesia: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia*, (2016) p. 27.

General Assembly Resolution 68/167 in 2014.[135] The independent body can be created from scratch, or by using existing independent institutions, with an extension of the mandate and the structure of the agency concerned, to perform the oversight function. Considering the exercise of powers of interception of communications has a number of special characteristics, the supervision should also have special characteristics as well.

Different countries have different practices: several countries create new agencies for oversight, such as the UK with the establishment of the Commissioner of the Interception of Communications, while others optimise existing entities, such as the Ombudsman in Australia. There are also countries establishing oversight committees in the parliament, such as Australia or the United States.

Indonesia certainly can choose from several models of supervision; a new independent body is ideal, though. The agency's composition should represent a wide range of actors and stakeholders. The agency should be given a special mandate to carry out the oversight function, to the entire exercise of powers of interception of communication conducted by intelligence and law enforcement agencies, including receiving complaints from the public in case of infringement, and provide redress.

Another alternative is the establishment of a joint committee in the parliament, which is to be given a specific mandate to oversee the implementation of the authorised interception of communications. The Joint Committee can consist of 5 to 9 persons, including members of House Commission I overseeing intelligence, and members of Commission III overseeing law and human rights. These commission members are to be chosen in particular based on their ability, capacity, as well as integrity to conduct oversight of interception of communications. This is important in view of confidentiality of every action and data gathered from communications interception activities. Therefore, besides other than being sworn in as members of Parliament in general, they also need a special oath to carry out the oversight function. To support the performance of the joint committee, it is also necessary to gain support from the secretariat of the Parliament, through a special secretariat or a special committee secretariat.

However, the formation of a joint committee of the House is only possible if the laws that regulate the institutional structure of the Parliament are amended. The rules that guide the formation of the structure and complementary agencies of the House must provide the space and accommodate the formation of this committee, including its relationship with other agencies in the House, particularly the leadership of the House, including those relating to the rights of finance and budget.

In addition to the special supervision of an independent body established either outside or inside the parliament, other forms of supervision in the implementation of the interception of communications should also be conducted. These include internal supervision of heads of agencies/institutions, financial supervision of the Audit Board, periodic supervision through forums of working meetings in the House of Representatives, supervision by independent institutions, such as the National Human Rights Commission, the Ombudsman, the Corruption Eradication Commission, the Prosecutorial Commission, Police Commission, as well as supervision performed by the public. Specifically in the implementation of the state intelligence functions, the Parliament has established the State Intelligence Oversight Team, in House

[135] *The right to privacy in the digital age*, United Nations General Assembly Resolution 68/167, UN Doc. A/RES/68/167 (2014) para. 4(d).

Commission I, which is mandated by the State Intelligence Law. Therefore, the existence of the monitoring team also needs to be optimised in the oversight of the performance of state intelligence, including the exercise of powers of interception of communications.

F. Remedy for Parties Harmed by Interception of Communications

As a state party to the ICCPR, Indonesia must also ensure the provision of an effective remedy mechanism to the victims of interception, whose rights were violated by the act of communications interception.[136]

Effective remedies for violations of the right to privacy of due to a communications interception practice can be obtained by judicial and non-judicial pathway mechanisms (either administrative or legislative ones). In this regard, the UN Special Rapporteur has emphasised that effective remedy mechanisms should be able to meet the following four basic characteristics, namely:[137]

1. The remedy must be known and accessible to all those who feel that their rights have been violated;
2. Effective remedy has to pass a swift, thorough and impartial investigative process;
3. The remedy mechanism should be able to end on-going violations; and
4. When human rights violations escalate into serious violations of human rights, non-judicial remedy mechanisms cannot be used, and criminal prosecution must absolutely be implemented.

In the Indonesian context, at least there are several options that can be used to achieve effective remedy for those who feel that their right to privacy has been violated due to interception of communications, namely by filing a civil lawsuit to the court or applying to the Ombudsman. Meanwhile, those who conduct unlawful interception of communications can be criminalised under the provisions of legislations in force.

In addition to these options, a number of existing laws have regulated complaints and remedies in case of infringements in the implementation of the legislation in question. These can be found in the Criminal Procedural Code provisions governing compensation and rehabilitation (Articles 95- 101), the Anti-Terror Law, and the State Intelligence Law. However, to reinforce the remedy mechanism in case of errors or violations in an act of interception of communications, the Law on Interception of Communications will also need to specifically prescribe remedy mechanisms of an act of interception of communications, if the procedure or target is found to be in error.

[136] ICCPR, *op. cit.*, Article 2(3)(b).
[137] UN Doc. A/HRC/27/37 (2014) para. 40-41.

CHAPTER VI
CONCLUSION

The continued development of information and communication technology does not positively correspond with increasing protection of a person's right to privacy; in fact the privacy of a person is becoming more vulnerable to interference, and personal information more easily transferable, due to increasingly innovative technologies. Significant developments of information and communication technologies have created many new techniques in interception of communications into the private spaces of individual communications. Vulnerability to the potential exposure of one's personal communication becomes increasingly large with the increasing number of Internet and mobile phone users. Therefore, the state must plan to implement both paradigmatic and legal reforms in response to the new challenges, in order to ensure protection of the privacy of every citizen.

Moreover, with a large number of Internet and mobile phones users, Indonesia has a vast potential of intervention against the privacy of its citizens. This situation is further exacerbated by the lack of regulation specifically intended to ensure the protection of the right to privacy of citizens, particularly, protection from the practice of monitoring, interception of communications and arbitrary transfer of personal data. Not to mention, lack of awareness of citizens to protect their privacy adds to the dismal condition of the protection of this right.

The UN Human Rights Council Resolution has reminded all countries to respect and protect the right to privacy of all citizens, including in the context of digital communications, to be conducted among other things: (i) taking steps to ensure that relevant national legislations correspond to their obligations under international human rights law; (ii) reviewing any procedures, practices and rules regarding scanning, interception of communications and personal data collection, with a view to upholding the right to privacy by ensuring full and effective implementation of all their obligations under international human rights law; and (iii) establishing or maintaining independent and effective domestic mechanisms to monitor the practice of scanning, interception of communications and personal data collection, to ensure transparency and accountability.

It is therefore important for the government and parliament in Indonesia to take heed of the following recommendations:

1. There is a need for a law specifically intended to regulate procedures for interception of communications, which in detail formulate the following: (i) the categories of situations in which the act is done; (ii) authorisation or permits to the action; (iii) supervision by an agency/body/independent authority; and (iii) legal protection relating to the nature, scope, duration of action, reason for action, competent authority to authorise and implement, as well as recovery provided;
2. The prohibition for any act of unlawful and arbitrary interception of communications, including those conducted by individuals, government officials and private parties. This prohibition should also be accompanied with penalties for violators;
3. These legislative measures can be done through amending a number of existing laws and regulations, such as the amendment of the Penal Code relating to the prohibition of unauthorised interception practices, revision of the Criminal Procedural Code, which specifically regulates the procedures for interception of communications, as well as

enactment of special legislation regarding interception of communications, as mandated by the EIT Law and the Decision of the Constitutional Court;

4. The need for transparency and accountability on the use of powers and scope of communication interception techniques. This form of transparency and accountability can be done by regularly publishing aggregated information relating to the interception of communication whose permit requests have been accepted or rejected, and the objectives of the act;
5. The need for improved public access to information, understanding and awareness of the threat to privacy. This can be done by providing adequate information about the potential for invasion of privacy. Also, by increasing public awareness of the use of information and communication technologies, so as to understand the risks of any decision on the use of these facilities.

***

ORGANISATIONAL PROFILES

The Institute for Policy Research and Advocacy (Lembaga Studi dan Advokasi Masyarakat, ELSAM) is a policy advocacy organisation in the form of an institute, founded in August 1993 in Jakarta. Its purpose is to participate in the attempts to grow, advance and protect civil and political rights, and human rights in general – as mandated by the 1945 Constitution and the 1948 Universal Declaration of Human Rights. Since its inception, the spirit of ELSAM is to develop a democratic political order in Indonesia through empowerment of the civil society through advocacy and promotion of human rights.

ELSAM's main activities are (1) research of policies and laws impacting human rights; (2) advocacy of human rights in various forms; (3) human rights education and training; and (4) publication and dissemination of human rights information.

ELSAM's working programs are: (1) integrating the principles and norms of human rights in state policies and laws; (2) integrating the principles and norms of human rights in policies of corporate operations related to indigenous societies; and (3) capacity building of the civil society in advancing human rights.

Address:

Jl. Siaga II No.31, Pejaten Barat, Pasar Minggu
Jakarta-INDONESIA 12510
Tel. +62 21 7972662, 79192564, Fax. +62 21 79192519
E-mail: office@elsam.or.id, Web site: www.elsam.or.id,
Twitter: @elsamnews - @ElsamLibrary



Privacy International is committed to fighting for the right to privacy across the world.

We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.

To ensure that this right is universally respected, we strengthen the capacity of our partners in developing countries and work with international organisations to protect the most vulnerable.

Privacy International envisions a world in which the right to privacy is protected, respected, and fulfilled. Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right.

Privacy International, a registered UK charity (No. 1147471), was founded in 1990 and was the first organisation to campaign at an international level on privacy issues.

Privacy International is located at:

62 Britton Street, London
EC1M 5UY United Kingdom