Privacy: An Overview of Indonesia Statutes Governing Lawful Interception

Sinta Dewi

Abstract

The right to privacy is an issue that draws a lot of public attention, especially when associated with the frequent interceptions made by the state upon state citizen private communications in the course of legal enforcement. Yet, those state practices in the form of surveillance and interception of communications have disrupted citizen's privacy right indeed. In Indonesia, in the post-Constitutional Amendment, the right to privacy is recognized as one of the fundamental rights of citizens that must be protected. This protection is asserted in paragraph G of Article 28 (1) of the 1945 Constitution, states that every person has the right of self-protection (privacy), family, honour, dignity, and property (including personal data). The statement also affirmed in Article 32 of Law No. 39 the Year 1999 on Human Rights, which among other things stated that the independence and confidential communications by electronic means should not be disturbed except by order of a judge or other authority duly authorized by law.

Notwithstanding, the current situation in Indonesia shows that there is no single rule on procedures for an interception. Thus has created vulnerability towards interception of citizens' private communications, including in the use of internet communication, such as electronic mail and various social media tools. To date, Indonesia has at least twelve legislations regulating interceptions in different ways. Those confusing and overlapping regulations have threatened human rights, especially privacy rights. In Indonesia, the war against corruption and terrorism has somehow affected the practices of wiretapping and reduced the protection of privacy rights.

Sinta Dewi. Privacy: An Overview of Indonesia Statutes Governing Lawful Interception. *Central European Journal of International and Security Studies* 12, no.4: 586–597.

Keywords: privacy rights, legal interception, communications

Introduction

The major issue in information privacy law is a tension between privacy and security. In order to investigate the crime, the law enforcement must gather information by monitoring suspected individuals that have to pose substantial threats to privacy[1,2,3,4]. This situation is exacerbated by the advancement of new technologies and the internet that have provided new challenges to long-standing human rights norms. By facilitating increased State surveillance and intervention into individuals' private lives, the spread of digital technologies has created a serious need for States to update their understandings and regulations of surveillance and modify their practices to ensure that individuals' human rights are respected and protected.[5,6,7,8]

Privacy has been embraced in the Asian Region. There are two major factors that influenced the privacy protection development in Asia, specifically in Indonesia. Firstly, the influences of international law such as the *Universal Declaration of Human Rights* and Indonesia as a signatory to several international human rights convention. Privacy in Indonesia is considered as a part of fundamental human rights. Indonesia as a signatory to international instruments, such as the *Universal Declaration of Human Rights* and *International Covenant of Civil and Political Rights* 1966 and ratified with Law Number 12, 2005. Secondly, privacy awareness in Indonesia has increased due to the development of information technology with its capabilities to collect, analyze and disseminate information. This new development worldwide became an enabling factor in other sector industries, such as telecommunication, media, financial and has increased the level of information generated to individual[9,10,11,12]. Therefore privacy also stated in Electronic Information Technology Law, 2008. Privacy issues also raise in Indonesia relating to the growing concern of protection personal data in e-identity program, because the local government collecting personal data including biometrics data and also relating to the government legal enforcement power on wiretapping.

However, intervention practices on privacy, in the form of surveillance, communications interception and disruption of personal data is one of the major problems that arise in the utilization of information technology and communications, especially the internet. The UN special

rapporteur for freedom of opinion and expression, Daniel [1], has given particular attention to this matter, given the high practice of observation (surveillance), the interception of private communications of citizens, as well as the alienation of personal data arbitrarily. In his report, La Rue affirms the need for countries to have laws that clearly describe the conditions that the right to privacy of the individual can be limited under certain conditions, and actions to touch this right should be taken on the basis of a special decision. This decision was taken by state authorities clearly guaranteed by law to perform the act.[13]

The origins of wiretapping occur in two quite different practices: eavesdropping and letter opening. "Eavesdropping," restricted in meaning, has come to describe any attempt to overhear conversations without the knowledge of the participants. "Letter opening" takes in all acquisition, opening, reading, and copying of written messages, also without the knowledge of the sending and receiving parties. Telecommunication has unified and systematized these practices. Before the electronic era, a conversation could only be carried on by people located within earshot of each other, typically a few feet apart. Neither advanced planning nor great effort on the part of the participants was required to ensure a high degree of security.

Written communications were more vulnerable, but intercepting one was still a hit-or-miss affair. Messages travelled by a variety of postal services, couriers, travellers, and merchants. Politically sensitive messages, in particular, could not be counted on to go by predictable channels, so special couriers were sometimes employed. And written messages enjoyed another sort of protection. Regardless of a spy's skill with flaps and seals, there was no guarantee that, if a letter was intercepted, opened, and read, the victim would not notice the intrusion. Since spying typically has to be done covertly in order to succeed, the chance of detection is a substantial deterrent.

Electronic communication has changed all of this in three fundamental ways: it has made telecommunication too convenient to avoid; it has, despite appearances, reduced the diversity of channels by which written messages once travelled; and it has made the act of interception invisible to the target.

Conversation by telephone has achieved an almost equal footing with face-to-face conversation. It is impossible today to run a successful business without the telephone, and eccentric even to attempt to do without the telephone in private life. The telephone provides a means

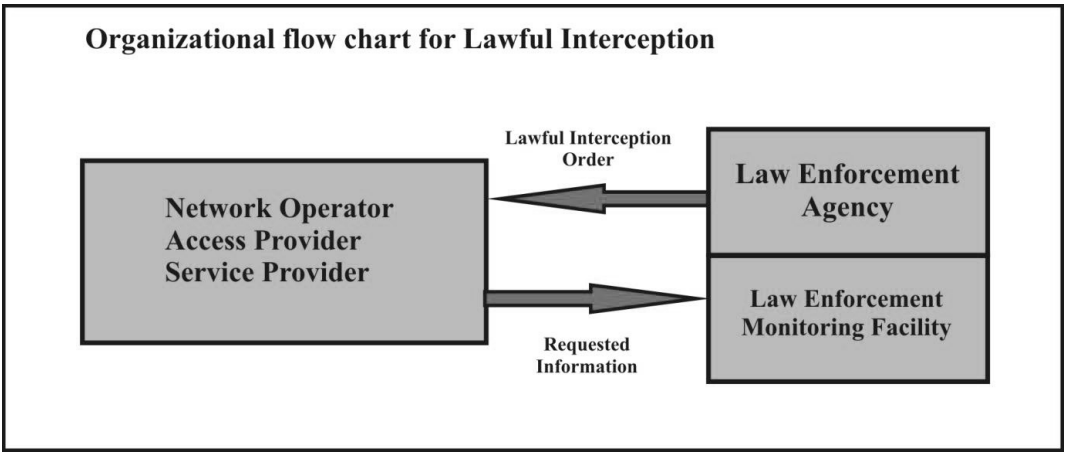
of communication so effective and convenient that even people who are aware of the danger of being overheard routinely put aside their caution and use it to convey sensitive information.

As the number of channels of communication has increased (there are now hundreds of communication companies, with myriad fibres, satellites, and microwave links), the diversity of communication paths has diminished. Today, telecommunications carriers must be registered with national and local regulatory bodies and are well known to trade associations and industry watch groups. Thus, interception has become more systematic. Spies, no longer faced with a patchwork of ad hoc couriers, know better where to look for what they seek.[14]

Interception of a communication in the course of its transmission involves the modification, interference or the monitoring of the system while the communication is actually being transmitted. Lawful interception is the terminology used to describe the means by which law enforcement agencies are authorised to intercept telecommunication sessions as prescribed by law. The advancement of technology has led to the need for law enforcement agencies to curb criminal and terrorist activities.

For interception to be lawful, it must be conducted in accordance with national law, following due process after receiving proper authorization from competent authorities. Typically, a national law enforcement agency issues an order for intercepts to a specific network operator, access provider, or network service provider, which is obliged by law to deliver the requested information to a law enforcement monitoring facility.

In order to prevent investigations from being compromised, the national law usually requires that lawful interception systems hide the interception data or content from operators and providers concerned. Whilst the detailed requirements for lawful interception differ from one jurisdiction to another, the general requirements are similar. The lawful interception system must provide transparent interception of specified traffic only, and the intercept subject must not be aware of the interception. Additionally, the service provided to other uninvolved users must not be affected during the interception. The term target, as used here, can refer to one person, a group of persons, or equipment acting on behalf of persons, whose telecommunications are to be intercepted. Lawful interception also implies that the target benefits from domestic legal protection. However, protections are complicated by cross-border interception.



Source: Adapted from ETSI TS 101 331, Definition of interception.
See www.pda.etsi.org/pda.

Interception of communications can take place in a number of ways: Wire Tap: this involves the installation of a transmitting device on a telephone line for the purpose of intercepting and usually recording telephone conversation and telephonic communications.

Location Tracker: This involves using devices to identify through the telecommunication system the location of an individual.

Pen registers and trap and trace devices: A pen register records only the numbers of outgoing telephone calls. While a trap and trace device is used to capture the numbers of incoming telephone calls.

The intentional interception of communications on public and private telecommunication systems without lawful authority is an offence. Lawful interception plays a crucial role in helping law enforcement agencies to combat criminal activity. Lawful interception involves the collaboration between law enforcement agencies and communication service providers. As such while there are laws dealing with the procedural and authorisation activities required for law enforcement agencies, likewise there are laws relating to the obligations of telecommunications operators and service providers. On the practical level, interception is very vulnerable to violation of privacy rights. It is recommended that government in any state should regulate interception through the act of legislation. Several countries including developed countries such as US, UK, and other European countries also

govern interception in a specific legislations that guarantee a balance protection of the rights of user, providers and public interest.

International Law Perspectives

The Role of international law to protect privacy against surveillance and interception have contributed significantly through international society consists of states, Civil Society Organizations, International Organization on Human Rights and business people is since the interception practices have violated the privacy rights of the public. So, they express their opinions in international forums organized either by Civil Society such as Privacy International, Electronic Frontier Foundation and other organizations. As in June 2013, they issue *International Principles on the Applications of Human Rights to Communications Surveillance,* which must be taken into account by all countries as it is based upon basic principles of the protection of human rights set out in international human rights law.

This instrument attempts to clarify how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to Communications Surveillance technologies and techniques. These principles can provide civil society groups, industry, States, and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights [2].

Another important role also is done by the United Nations (UN) through its Special Rapporteur on Human Rights in December 2013, when the UN General Assembly issued Resolution Number 68/167 on *The Right to Privacy in the Digital Age, which among others include [3]:*

1. To respect and protect the right to privacy, including in the context of digital communication;
2. To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;
3. To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

4. To maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.

Interception and Privacy in Indonesia

The debates regarding the interception of a communication in Indonesia are getting more intensified lately, this because the interception of communication today is usually used by law enforcement agencies as to expose the crimes, particularly organized and transnational crimes. This is even getting more intensified after the enactment of Act Number 17 the Year 2011 on State Intelligence and Act Number 18 the Year 2011 on Amendment to Act Number 18 the Year 2004 on Judicial Commission. The discourse to make new regulation regarding the interception of communication increasingly stronger, particularly after the Constitutional Court gave the verdict on the case of Article 31 paragraph (4) Act No. 11 the Year 2008 on Information and Electronic Transactions.

An interception by law enforcement agencies or official institutions remains controversial because it can consider as an invasion of the privacy rights of the citizens, which includes the privacy of private life, family life and correspondence. On the other hand, the interception is also effective as a method of investigation in the disclosure of criminal cases. Interception is a useful alternative to develop the method of prevention, detection and investigation of crimes.

Briefly, quite a lot of perpetrators on the serious crimes can be brought to justice because of the interception. As an example, without an interception, Corruption Eradication Commission of the Republic of Indonesia may not be able to detect the perpetrators of corruption and also against him in court. Without interception. It would be difficult for the Densus 88 [4] to reveal numerous cases of terrorism, as well as for the National Narcotics Board in the case of psychotropic drugs abuse.

However, an interception as a method to deterrence and detection of crimes also tend to violate human rights, especially when this activity must deal with lack of regulation and lack of control from the government. Interception tends to be abused, particularly when the national legislation incompatible with human rights. Moreover, there is a tendency from the law enforcement officers, to make interception

transcription as a primary evidence in combating crime without trying to use another instrument as evidence in criminal matters.

The obscurity condition regarding the interception regulation in Indonesia appears from the number of statutory regulations. The regulations provide authorization to the government institutions to commit an interception, while the restrictions between one provision with other provisions are often different. The regulations regarding the interception activity can be found in a number of statutory provisions as follows:

An Overview of Indonesia Statutes Governing Lawful Interception

1. Chapter XXVII Indonesia Criminal Law Code on the Malfeasance, article 430 up to article 434; [6]
2. Act Number 5 the Year 1997 on Psychotropic; [7]
3. Act Number 31 the Year 1999 on Corruption Eradication; [8]
4. Act Number 36 the Year 1999 on Telecommunication;
5. Act Number 30 the Year 2002 on Corruption Eradication Commission;
6. Government Regulation Number 1 the Year 2002 on Terrorism Eradication
7. Act Number 18 the Year 2003 on Advocate; [10]
8. Act Number 21 the Year 2007 on Combating Trafficking Persons; [11]
9. Act Number 11 the Year 2008 on Information and Electronic Transaction;
10. Act Number 35 the Year 2009 on Narcotics; [12]
11. Act Number 18 the Year 2011 on Amendment to Act Number 22 the Year 2004 on Judicial Commission;
12. Government Regulation Number 19 the Year 2000 on Corruption Eradication Joint Team;
13. Government Regulation Number 52 the Year 2000 on Operation of Telecommunications Service;
14. Ministry Information and Communication Regulation Number 11 the Year 2006 on Technical Interception of Communication; and
15. Ministry Information and Communication Regulation Number 1 the Year 2008 on Information Recording for Security and Defence.

As mentioned earlier, unfortunately, the variety of acts and regulations governing the interception contain fundamental weaknesses, as one regulation is very often found contradictory or inconsistent with

another. The procedure to get an authorization for communication interception in one Act is different from another Act. The absence of a single regulation regarding the interception procedural in Indonesia has made the rights to privacy of Indonesian citizens are threatened. This situation appears because state officials can easily use various methods to intervene against the privacy rights of its citizen's Another constraint related to the interception of a communication in Indonesia is due to the fact that there is no single authority to provide the authorization or permission for intercepts. To get the authorization, regulations regarding the interception as mentioned above designate different institutions. For example, Act on Psychotropic allows phone tapping and recording with the permission from the Chief of the Indonesian National Police. The act of Narcotics allows the National Narcotics Agency to intercept the communication based on the permit of the Head of Municipal Court. However, under urgent circumstances, the intercepts can also be done without authorization. Act on Terrorism Eradication also allows investigators to intercept phone communications and make recording only with the permission from the Head of Municipal Court. The Corruption Eradication Commission is allowed to intercept phones communications and make a recording in order to reveal allegations of corruptions based upon their own decision. Act on Information and Electronic Transactions allow a request for interception from any investigation institution established under regulation, similarly with the Telecommunications Act. Act on State Intelligence allows the interception based on the command of the Chief of the State Intelligence Agency, as well as through the establishment decision of the Head of Municipal Court.

The above condition shows that the institutions providing authorization for communication interception in Indonesia are varied and depending on the intercept target. Generally, in other countries, permit for intercept solely owned by one institution. Some countries use the model where the permit granted by the government (executive authorization), while some others use the model to obtain the permission from the court (judicial authorization), and the other model is that the intercept is allowed by the judge commissioner (investigating magistrate).

Indonesia embraced all models, and as the consequence, there is no monitoring mechanism nor a uniform control to the institutions that conduct intercepts. This condition will also raise the opportunities for

claims based on the interests of each institution, and as the result, human rights to the privacy which includes privacy of private life, family life and correspondence become vulnerable violated.

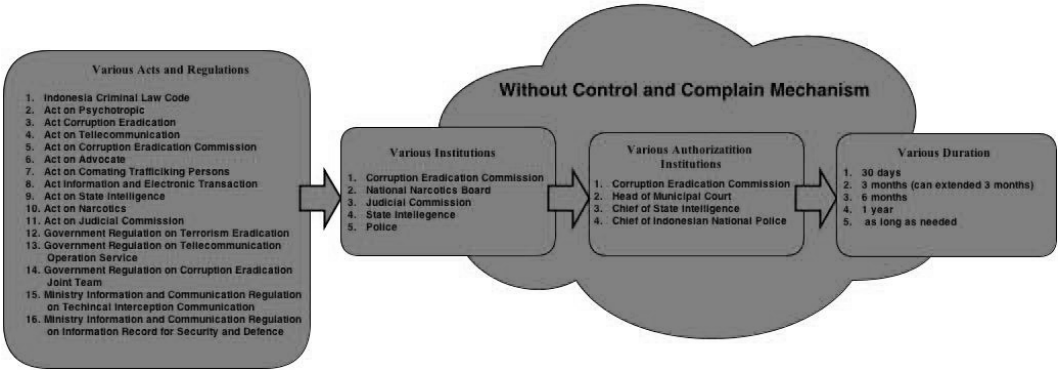
Moreover, an obstacle in regulating interception is due to the differences in the length of interception period or duration. Act on Psychotropic allows the interception communication conducted during 30 days. Act on Narcotics allows the communication interception within a period of 3 months and can be extended by another 3 months. Act on State Intelligence allows state intelligence officers to conduct interception for a period of 6 months and can be extended as needed. This means that there is no definite time limit for the state intelligence officers to intercept the target. Act on State Intelligence would potentially violate the rights of privacy protection of the citizens, as it allows state intelligence officers to take interception in long duration. Furthermore, the Act on Terrorism Eradication allows the communication interception within one year and Act on Corruption Eradication allows the communication interception conducted without any specific time limit. These differences in interceptions durations certainly susceptible towards violation of the rights of citizens, particularly if there is no monitoring and control on to the institutions.

The absence of rules regarding the use of the material results will also lead to the abuse of interception. The regulation setting related to the using of the interception results usually consists of :

1. restrictions on who can access the wiretapping and interception results;
2. interception procedures;
3. regulation on the relevant material of the interception;
4. procedures to bring the intercepts results as evidence to the court; and

The lack of rules regarding the use of the materials resulted from interception makes the resulting material can be accessed by any person. Furthermore, the interception's material results can also be heard or quoted in the media without prior selection. Certainly, this condition will also vulnerable to abusing the interception material.

The most important thing related to the interception of a communication in Indonesia is there is no specific complaints mechanism from citizens, particularly if the interception conducted with arbitrarily. The absence of this mechanism will make interception practices will potentially violate human rights.



Indonesian Obstacles Related to the Interception Regulation

Conclusion

Privacy is a fundamental human right and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights and is both recognised under national and international human rights law. Communications Surveillance interferes with the right to privacy among a number of other human rights. As a result, it may only be justified when it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued. In recent decades, due to the advancement of information technology that facilitates State surveillance of communications, States are failing to ensure that laws, regulations, activities, powers, and authorities related to Communications Surveillance adhere to international human rights law and standards. and have decreased to apply legal principles in new technological contexts that have become unclear.

Until today, the regulations related to the interception in Indonesia randomly develop based upon sectoral interests. This condition leads to some problems *inter alia* overlapping regulations, overlapping institutions and causing legal uncertainty to the citizens. The condition also potentially contains human rights abuse, particularly the right of privacy. Therefore, Indonesia must harmonize all regulations related to the interception activity, otherwise, the main objective of the interception as to enforce the law, conversely become unlawful and resulting in the abuse of power committed by the government institution.

The needs of each country to have its own laws which should clearly describe the conditions that the rights for individual privacy may be

limited under certain terms, and measurements on this rights should be taken based on a special decision. This decision should be taken by the state authorities guaranteed by law as to perform the act.

Notes

1 Daniel J. Solove and Marc Rotenberg (2003), ***Information Privacy Law,*** Aspen Publishers, New York.
2 Yoo J, Lee MK and Lee WS (2016), 'Asymmetrical Corporate Responses To Economic Information: Applying The Firm Size Effect,' ***Journal of Administrative and Business Studies*** 2(1), p. 29-34.
3 Hashim H, Salam S and Mahfuzah Mohamad SN (2017), 'Investigating Learning Styles For Adaptive Massaive Open Online Cource (MOOC) Learning,' ***Journal of Advances in Humanities and Social Sciences*** 3(5), p. 282-292
4 Uğur Naciye Güliz and Barutçu Merve Türkmen (2018), 'Investigating Social Media Activities: A Study on Celebrity Posts,' ***Journal of Advances in Humanities and Social Sciences*** 4(2), p. 84-92
5 Sinta Dewi (2011), Balancing Privacy Rights and Legal Enforcement: Indonesia Practices, In *Sylvivia Mercado Kierkegaard* (Ed.), ***Law Across Nations,Governance, Policy and Statutes.***
6 Basoglu B (2017), 'Youtube Or Writing Tube: A Technology-Mediated Learning Tool For TESOL,' ***International Journal of Humanities, Arts and Social Sciences*** 3(3), p. 98-105.
7 Wang H Y (2015), 'Needs Analysis Of Sophomore-Year Students In A Technology University In Taiwan,' ***International Journal of Humanities, Arts and Social Sciences*** 1(2), p. 101-107.
8 Kongmanus K (2016), 'Development Of Project-Based Learning Model To Enhance Educational Media Business Ability For Undergraduate Students In Educational Technology And Communications Program,' **Journal of Advances in Humanities and Social Sciences** 2(5), p. 287-296.
9 Wahyudi Djaffar (2010), 'Memastikan Perlindungan Hak Privasi dalam Pertahanan Siber (Ensure Protection of Privacy Rights in Cyber Defense),'
10 Purba CS and Martono D (2017), 'Local Act Draft Model On Development, Control, And Telecommunication Tower Supervision,' ***International Journal of Humanities, Arts and Social Sciences*** 3(5), p. 231-240.
11 Polat F, Subay ÖÖ and Ulutürk AS (2018), 'Hate Speech In Turkish Media: The Example Of Charlie Hebdo Attack's,' ***Journal of Advanced Research in Social Sciences and Humanities*** 3(2), p. 68-75
12 El-Den J, Adikhari P and Adikhari P (2017), 'Social Media In The Service Of Social Entrepreneurship: Identifying Factors For Better Services,' ***Journal of Advances in Humanities and Social Sciences*** 3(2), p. 105-114.
13 Final Version, 'International Principles on the Applications of Human Rights to Communications Surveillance,' available at: https://en.necessaryandproportionate.org/text.
14 Privacy International Report (2018), 'The International Principles on the Application of Human Rights to Communicate,' available at: https://www.privacyinternational.org/reports/the-international-principles-on-the-application-of-human-rights-to-communications