THE EFFECTIVENESS OF THE MINISTER OF COMMUNICATION AND INFORMATICS REGULATION NUMBER 20 OF 2016 ON THE PROTECTION OF PERSONAL DATA IN ELECTRONIC SYSTEMS

Fadhilah Pijar Ash Shiddiq, Sinta Dewi Rosadi, Rika Ratna Permata
Faculty of Law, Universitas Padjadjaran
fadhilahpijar@gmail.com, sinta@unpad.ac.id

ABSTRACT

Privacy, as a part of Human Rights, is the right of freedom of private matters. The basic concept of privacy is "the right to be let alone" which state that every individual have the right to have his own solitude without intervention. One of the most important information which also can be associated with Information Privacy is Personal Data that shall be protected as a form of protection to the privacy itself. Some of the personal data has been used as the requirements of the SIM Card Registration, thus making new problems regarding its personal data protection since the comprehensive regulation still covered only by the Ministral Regulation. Research method used in this paper is Descriptive Analytic in which the writer analyze the research object by explaining the situation and the condition of the personal data protection obtained from literatures on the facts that can be associated with the implementation of SIM Card Registration Policy according to Indonesia's Positive Law and International Law. According to the result of the study, the Ministral Regulation already covered most of the basic data protection needed in the SIM card registration policy, however the protection provided by the Ministral Regulation still has not covered the third party involved. The Involvement of this third party is inevitable and should be protected immediatelyin order to prevent any abuse of personal data.

Keywords: Privacy, Personal Data Protection, SIM Card Registration

A. INTRODUCTION

Entering the era of information age, the demandof information and communication technology is growing rapidly. Almost all types of daily activities are now supported by information and communication technology. This phenomenon emerged due to thetransformation in the shape of society into an information society which also induces the increased development of rapid information technology that is sophisticated and able to meet the demands of all levels of society (Edmon Makarim, 2004: 27).

The demandof information is closely related to data requirements as its main composition. Amongst many types of data available in the world, personal data is very important but also vulnerable to abuse which can ultimately constitute violations of the privacy data owner in the event of being misused.

Personal data must be protected due to the matterof privacy, therefore it shall have governed by appropriate regulations, because certain parties can identify individuals specifically in a large set of data and make decisions on certain individuals based on an analysis of these data. Nowadays, the technology of information also enables companies and governments to monitor every conversation carried out, every commercial transaction conducted and every location visited. This ability may lead to negative effects on individuals, groups and even society due to its capability to restrict the movement and freedom of certain individuals or groups themselves.

Etymologically, privacy comes from the word *privauté* in an old French word which means secret or mystery. The word *privauté* itself began to emerge in the early 14th century which later developed into privatization until in 1814 it became well-known as the private term which is the basic word of privacy nowadays (Online Etymology Dictionary, https: //www.etymonline.com/word/privacy, accessed on September 3, 2018).

The concept of privacy was first developed by Warren and Brandeis which stated that: "Privacy is the right to enjoy life and the right to let alone and this development of law was inevitable and demanded of legal recognition." (Samuel Warren & Louis D. Brandeis, The Right To Privacy, Harvard Law Review, Volume 4, 1890: 1). Based on thedefinition stated by Warren and Brandeis, privacy becomes concern of the world with the initial concept of "the right to be let alone", this concern is related to individual freedom and restriction on the control of certain parties to individuals. Furthermore, privacy develops into rights that begin to be recognized and protected by international, regional and national law (Sinta Dewi Rosadi, 2015: 3).

In 1960, William Prosser conducted a survey of more than three hundred cases regarding privacy that emerged after the publication of Warren and Brandeis articles (Daniel J. Solove, 2006: 14). He concluded that cases related to privacy could be categorized into four different things, namely: Solitude Interference (Intrusion Upon Seclusion) Disrupting the solitude of others in very offensive circumstances. Intrusion upon seclusion protects individuals from the actions of people who listen confidentially (*eavesdropping*) to conversations carried out in private aspect, especially stealthy entering home and (deceitful entry) and secretly capture photosof all activities inside someone's home,(Public Disclosure of Private Facts Facts) Publish personal information with offenseive means the person's consent, (False light) Publish a false impression of someone in a offensive means, and (Appropriation) Using another person's name or similarity of identity for personal benefit without the

person's permission (Adam Moore, Defining Privacy, Journal of Social Philosophy, Vol. 39 No. 3, 2008: 411-428).

In 1970, the use of computerized databases by government institutions and private institutions began to spread rapidly in the United States and Europe. The trend of using computerized databases raises new threats to privacy, such as data theft, data exploitation, and data publication without the consent of the data owner. The term data protection was created and developed in Europe to regulate matters relating to the protection of privacy, while in the United States the term data privacy is used more on the same thing.

Protection of privacy and personal data must be distinguished because privacy has a broader and abstract definition and context, while the protection of personal data is a very specific part of privacy aimed at protecting the collection, registration, storage, exploitation and dissemination of individual personal data (Lee A Bygrave, 2014: 1).

One important goal of the existence of the law regarding the protection of data privacy is to ensure that individuals are enable to monitor and access their personal information collected by other parties and to provide repairs if necessary. This is intended to ensure that each individual knows information about those who are on the other side, as well as to encourage data collectors to keep and protect the personal data they collect (Purwanto, 2007: 13). Keeping in mind that the technology of information has become a part of everyday life, the protection of personal data in the utilization of information technology becomes very important.

Mobile phone as one of the most popular information technologies began to enter Indonesia in 1984. The cellphone model that first entered Indonesia was still very large, so it was still quite difficult to carry around. In 1994, PT Satellite Palapa Indonesia ("Satelindo") operated as the first Global System for Mobile ("GSM") operator in Indonesia, by commencing its operations in Jakarta and around. GSM uses a Subscriber Identity Module ("SIM") card, making it safe from copying, tapping and excellent quality and wide reach (Ifan Anwar, https://tekno.kompas.com/read/2010/04/01/18352875/Tracing. Development. Mobile. Di. Indonesia, accessed on 12 April 2018).

SIM Card or better known as the Prime Card (Article 1 number 7 Minister Of Communication And Informatics Regulation Number 20 Of 2016 On Protection Of Personal Data In Electronic Systems) is used with two payment methods, namely the first is the payment made in advance and services are availed afterwardrecognizes as Prepaid, secondthe is payment method called the Postpaid connections which avail the services first and thereafter pay the price for it. In June 2017 there were around 392.78 million Prime Cards circulating in Indonesia, while the population in Indonesia was only around 262 million ((Kata Data, https://databoks.katadata.

co.id/datapublish/2017/10/12/berapa-jumlah-kartu-telepon-seluler-yang-beredar, accesed on 12 April 2018). This number is certainlycontradict with the population of Indonesia, especially since access to this cellphone is not owned by everyone. This contradiction is emerged by various things, starting from one person who uses more than one Prime Card, to people who use the Prime Card once to get a certain promo.

The using practiceof Prime Card in Indonesia has not reached orderly. Besides being used, in terms of registration, users are often not registered properly. Therefore, the Ministry of Communication and Information enacted the policy of re-registration of the Prime Card using the National Identity Card number ("KTP") and Family Card number ("KK") to fix the data on the Prime Card in Indonesia. The aim is to provide protection to consumers regarding abuse of cellphone numbers by irresponsible parties, such as fraud and hoaxes. In addition, there is also a National Single Identity interest launched by the government (Oik Yusuf, https://tekno.kompas.com/read/2017/11/01/20190067/7-hal-yang-wajib-diketahui-soal-registrasi-kartu -sim, accessed on April 17, 2018).

Enactment of the Minister of Communication And Informatics Regulation Number 12 of 2016 *juncto* the Minister of Communication And Informatics Regulation Number 21 of 2017 concerning Customer Registration for Telecommunications Services is the beginning of a change in the procedure for registration of Prime Cards. The previous registration only requires the Population Registration Number ("NIK") of the KTP as stipulated in the Minister of Communication And Informatics Regulation Number 23 of 2005 concerning Telecommunications Services Customer Registration, presently it must be completed with KK Numbers and through the verification phase to prove the truth. After being verified then the Prime Card can be used.

The implementation of the new Prime Card registration policy involves several agencies, therefore, it is necessary to clarify the responsibilities of each agency in order to protect personal data in the registration process of this prime card.

B. PROBLEM STATEMENT

Based on the foregoing topic, this paper will address:

1. How is the effectiveness of personal data protection in the implementation of prime card registration carried out in Indonesia?
2. How is the effectiveness of resolving disputes against the protection of personal data?

C. RESEARCH METHOD

The research method used in this study is described as approach method, research specifications, data collection techniques, and data analysis methods. The approach

method used by the writer is normative juridical conducted by tracing and analyzing literatures and documents related to the substance of research (Soerjono Soekanto and Sri Mamudji, 2004: 14).

The research specification used by the writer is analytical descriptivedue to the intention of the reserach to provide a detailed, systematic, and comprehensive description of legislation and legal theories (Soemitro and Ronny Hanitijo, 1983: 10). The data collection technique that the writer does is Literature Studies, which collects data and conducts research on the literature and documents that are closely related to the protection of personal data and privacy.

The data analysis method used in this study is qualitative juridical analysis, which is an analysis that emphasizes more on the process of deductive and inductive conclusions and the analysis of the relationship of the phenomena faced by using scientific logic with the assitance of legal interpretation methods.

D. DISCUSSION AND RESEARCH RESULTS

1. Effectiveness of Personal Data Protection in the Implementation of Prime Card Registration Policy

The Minister of Communication and Informatics Regulation Number 12 of 2016 on the Telecommunications Services Customer Registration requires the existence of several personal data which are used as registration requirements, such as NIK and KK Number. Both data are personal data as referred to in Article 84 of the Population Administration Law. In addition, the law also stipulates that truth and confidentiality of personal data must be protected by the government (Article 85 paragraph (1) of Law Number 23 of 2006 on the Population Administration).

Nowadays, all large companies have used electronic systems as data storage media. Electronic Systems here are a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate Electronic Information (Article 1 number 5 of Law Number 11 of 2008 on the Electronic Information and Transactions). Usually this electronic system consists series of networks that connect several hardware devices such as computers. Therefore, all data entered into this electronic system will automatically become Electronic Information which is defined as one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or similar, letters, signs, numbers, access codes, symbols, or processed perforations that have meaning or can be understood by people who are able to understand (Article 1 point 1 Law - Law Number 11 of 2008 on the Electronic Information and Transactions).

Telecommunications Service Providers which are large providers have certainly used electronic systems to support their business activities. Personal data in the initial card registration process when it enters the electronic system of telecommunications service providers either through official outlets, partner outlets, short message services, or telecommunication service provider site services, then the personal data will automatically become Electronic Information henceupon all personal data of the telecommunication service customers, the provisions in Law Number 11 of 2008 on the Electronic Information and Transactions (ITE Law), Government Regulation Number 82 of 2012 on the the Implementation of Electronic Transaction Systems (Governement Regulation of PSTE)and the Minister of Communication and Informatics Regulation Number 20 of 2016 On Protection of Personal Data In Electronic Systems (Minister Regulationof Information and Communication Protection) may entry into force.

In order to measure the effectiveness of personal data protection, the writers take the principles of personal data protection contained in the Organization for Economic Co-operation and Development Guideline 1980 on Privacy Protection and Transborder Flows of Personal Data ("OECD Guideline 1980") as a data protection guideline which has been recognized internationally. These principles are as follows (OECD Privacy Principles, http://oecdprivacy.org, accessed on November 18, 2018):

a. The Principle of Collection Limitation must have a limit on the collection of personal data and the data must be obtained without being against the law and fair, or more accurately interpreted as with the knowledge or permission of the subject of the data.
b. The Principle of Data Quality, personal data must be relevant to the purpose of data usage, and for further purposes towards these objectives, personal data must be accurate, complete and always up-to-date.
c. The Principle of Purpose Specification, the purpose of collecting personal data must be determined when data collection and subsequent use must be limited to that purpose. If there is a use that is not in accordance with the objective, it must be determined the change of purpose at each opportunity
d. The Principle of Use Limitation, personal data may not be disclosed or used other than for the purpose of collecting data, except:
    1) permitter by the subject of the data; or
    2) permitted by legal authorities.
    e. The Principle of Security Safeguards, personal data must be protected by reasonable security of risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.

f. The Principle of Openness, there must be a general policy regarding the openness relating to the development, practices and policies relating to personal data. Imply thattheestablishment of existence and nature of personal data must ready to to available, the main purpose of its use, as well as the identity and usual residence of the data controller.

g. The Principle of individual participation, an individual must have the right:
   1) to get confirmation from the data controller whether the data controller has data associated with it or not.
   2) to conveye to the subject, data relating to:
      a) reasonable time;
      b) on costs, if any, that are not excessive;
      c) reasonable manner; and
      d) in a form that is easily understood bythe subject.
   3) to be given a reason if the request made under subparagraphs (a) and (b) is rejected, and to be able to submit an objection to the rejection; and
   4) to object to the data relating to and, if the objection is granted, the data must be deleted, corrected, completed or changed.

h. The Principles of Accountability, the data controller must be responsible for complying with the steps that have an effect on the foregoing principles.

The protection of personal data in the implementation of thePrime Card registration policy can be grouped based on the stages of personal data flow from the start when submitted by the customer as the subject of the data until the time when it must be destroyed by the telecommunications service provider. To facilitate analyzing the effectiveness of data protection in the implementation of the Prime Card registration, the writers describe it based on the stages of data flow, namely as follows:

a. Data collection

   Data collection conducted when prospective telecommunications service customers provide personal data to telecommunications service providers either through outlets owned by telecommunications service providers, partner outlets, or themselves through short message services and official sites of telecommunications operators.

   Based on the foregoing principles, in the process of collecting this data is protected by the Collection Limitation in the OECD Guideline 1980 where data collected at the time the prospective customer sends it to telecommunications service providers must be limited in ways that do not against the law, conducted in fair, and prospective customers who will later become the subject of data must give consent Article 9 of the The Minister

of Communication And Informatics Regulation Number 20 of 2016 On Protection of Personal Data In Electronic Systemsstates that the use of any information through electronic media relating to someone's personal data must be carried out with the consent of the person concerned. The owner of the personal data that permitted the use of the data can declare that the personal data is confidential.

Based on the Principle of the Use Limitation stated in the 1980 *OECD Guideline,*the personal data of the customers must be collected based on the certain purpose that must be explained prior to the collecting, and the data shall not used to any interest not relating to the Prime Card Registration. According to Minister of Communication and InformaticsNumber 12 of 2016 concerning Telecommunications Services Customer Registration,personal data may only be processed and analyzed according to the purpose which has clearly stated when obtaining and collecting it.

b. Data Storage

Every telecommunication service provider is required to note and/or record in detail the use of telecommunication services (Article 18 paragraph (1) of Law Number 36 of 1999 on the Telecommunications). Storage of these data is usually conducted in an electronic system which further referred to as a database. Based on the Principle of Data Quality in the OECD Guideline 1980,telecommunication service provider is obliged to keep the personal data to remain confidential, accurate, complete and up-to-date.

Every provider of electronic systems must operate an electronic system that meets the minimum requirements where one of the minimum requirements is that an electronic system must protect the availability, integrity, authenticity, confidentiality and accessibility of electronic information (Article 16 paragraph (1) of Law No. 11 of 2008 on the Electronic Information and Transactions). Article 15 of The Minister of Communication And Informatics Regulation Number 20 Of 2016 On Protection of Personal Data In Electronic Systemsstipulates that personal data stored in this electronic system must be in the form of encrypted data. If the owner of personal data is no longer a user, the electronic system operator must keep the personal data in accordance with the last time it identified a user.

At this stage of data storage, there is an undeniable threat to data breach, therefore, based on the Principle of Security Safeguards, telecommunication service providershall prepare data security measures that can guarantee the confidentiality and integrity of the customers personal data. Article 18 paragraph (1) requires that storage may be carried out in accordance with

the provisions concerning procedures and means of securing electronic systems. The security measures began with electronic system certification and the availability of internal regulations for the personal data protectionby telecommunication service provider.

Observing at various cases related to data security in the stages of data storage that occur throughout the world, it is only natural that telecommunication service providers are required to prepare themselves in the event of the worst possibility of data breach. Therefore, all telecommunications service providers must prepare a recovery mechanism in the event of failure to protect personal data.

The Principle of Openness in the OECD Guideline 1980 requires the notification of general policies regarding openness related to developments, practices and policies relating to the protection of personal data, including if there is a failure in such protection to the customers

A good intention to immediately notify the customer of telecommunications services as the owner of personal data in addressing any failure to protect personal data by the telecommunications service provider is an obligation that is regulated in the Minister of Communication and Informatics Regulation Number 20 Of 2016 On Protection of Personal Data In Electronic Systems. This notification must be carried out with the reasons or causes of the failure to protect personal data no later than 14 (fourteen) days after the failure of personal data protection as stipulated in Article 28 of the Minister of Communication and Informatics Regulation Number 20 of 2016 On Protection Of Personal Data In Electronic Systems. This is also considered as a form of responsibility for telecommunications service providers based on the Principles of Accountability in the 1980 OECD Guidelines.

c. Data Destruction

After passing the storage deadline, which is 5 years as stated in the the Minister of Communication and Informatics Regulation Number 20 Of 2016 On Protection of Personal Data In Electronic Systems, then personal data that is no longer used must be immediately destroyed by the telecommunication service provider. Telecommunication service customers can also request the removal of their personal data to telecommunication service providers (Article 20 PM Kominfo Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems the Minister of Communication and Informatics Regulation Number 20 Of 2016 On Protection of Personal Data In Electronic Systems). This destruction is not only valid for electronic data, but also applies to the related non-electronic personal data.

The Minister of Communication and Informatics Regulation Number 20 Of 2016 On Protection of Personal Data In Electronic Systemshas been sufficiently effective to regulate the protection of personal data which is fundamental in the implementation of Prime Card registration policies, however because this regulation is a derivative from the of Governement Regulation of PSTE as an implementing regulation of the ITE Law, the scope is only limited to System Administrators Electronics which are defined as each person, state administrators, business entities, and communities that provide, manage and/or operate Electronic Systems individually or jointly to Users of Electronic Systems for their own needs and/or the needs of other parties (Article 1 paragraph 6 of the Minister of Communication and Informatics Regulation Number 20 Of 2016 On Protection of Personal Data). Implies that if the data is not being input into the electronic system or processed by another party that is not an electronic system provider, then the Minister Regulationis disabled to protect the data of the user.

Concretely, one matter that has not been protected with certainty is if the registration is conducted through partner outlets or also called the pulse counter, which is one way of registration as stated in the Minister Regulationconcerning Telecommunications Services Customer Card Registration. This partner outlet can store customer's personal data in a separate database in which usually only in the form of printed or written records. Then the nature of partner outlets not an electronic system provider, which in this case is the telecommunications service provider, the partner outlets are not bound to the Minister Regulations, therefore the misuse of personal data by partner outlets is still difficult to prevent and overcome even though this regulation has properly regulated variety of issues that are in line with the Principle of Protecting Personal Data.

Therefore, it is necessary to immediately enact a Personal Data Protection Bill Draft commensurate with the Law that regulates the protection of personal data in Indonesia thereafter the protection of personal data scope is not limited to electronic system providers and telecommunications service providers but can reach all other data processing mediaas well as able to regulate various other parties involved in implementing this Prime Card registration policy.

2. Effectiveness of Dispute Settlement on Failure to Protect Personal Data in the Implementation of Prime Card Registration Policies

The Ministry of Communication and Informatics organizes the functions of formulating, stipulating, and implementing policies in the field of communication

and informatics. One of them is the Prime Card registration policy. This policy is included into the telecommunications field which is handled by the Directorate General of Post and Information Technology as an implementing element which is under and responsible to the Minister of Communication and Informatics.

The Directorate General of Post and InformaticsOperation (DG PPI) has the task of formulating and implementing policies and technical standardization in the field of organizing post and information technology.

The Ministry of Communication and Informatics through the Directorate General of PPI has the responsibility for telecommunications development purposed to improve telecommunications operations which includes the establishment of policies, regulations, supervision and control (Article 4 paragraph (2) of Law Number 36 of 1999 concerning Telecommunications). Conducting or arranging a Prime Card registration policy is a naturally purposed to build telecommunications, especially the use of telecommunications services in Indonesia.

The Minister of Communication and Informatics through the Director General of PPI has the responsibility to resolve disputes that occur. Telecommunication service customers can submit complaints to the Minister for the failure to protect the confidentiality of Personal Data. The complaint is intended as an effort to resolve dispute by deliberation or through other alternative settlement, however this complaint may only submitted by reason of not having written notice of failure to protect the confidentiality of personal data by telecommunication service providers to potential or non-potential telecommunication service customers. loss or loss for telecommunication service customers related to the failure to protect the confidentiality of personal data, even though written notification has been made of the failure of confidential protection of personal data but the time of notification is late (Article 29 of The Minister of Communication And Informatics Regulation Number 20 of 2016 on Protection of Personal Data In Electronic Systems).

The complaint must be submitted no later than 30 (thirty) working days from current time when the telecommunication service customer knowing information about the written personal data failure protection equipped with supporting evidence.

After receiving a complaint from a telecommunication service customer, the Director General of PPI can form a special panel for resolving personal data disputes ("Panels"). The panel must respond to complaints no later than 14 (fourteen) working days after the complaint is received. Settlement of disputes on the basis of complaints is carried out by deliberation or through other alternative settlement. On the proof of the failure to protect the confidentiality of personal

data, the panel that handles complaints can provide recommendations to the Minister for administrative sanctions imposed on telecommunication service provider even though complaints can or cannot be resolved by deliberation or through efforts to resolve other alternatives as mentioned in Article 33 of The Minister of Communication And Informatics Regulation Number 20 Of 2016 On Protection of Personal Data In Electronic Systems.

The mechanism of the dispute will require a long time considering the report is addressed to the Minister and then the Minister delegates the authority to settle the dispute to the Directorate General of PPI. Considering that protection failures can occur individually, certainly direct reporting to the Minister is very difficult to immediately being processed. It shall bepreferable if the DG PPI has a special sub unit which given authority in handling disputes over personal data protection, to ensure that each individual complaint can be resolved immediately.

In addition, this complaints mechanism also does not include violations that occur by third party electronic system providers, which in this case are partners of telecommunication service providers, even though the partners have clearly been involved in the registration process as a mean in Regulation of Minister of Communication and Information Services Telecommunications Services Customer Registration Card. Therefore, the regulation regarding settlement of the dispute is still not effective.

E. CLOSING

According to the foregoing discussion, this research arrived at the following conclusions:

1. The regulation of personal data protection in Indonesian positive law has been sufficiently effective, because it has met the Principles of protecting personal data contained in the OECD Guideline 1980 on Privacy Protection and Transborder Flows of Personal Data as an internationally recognized data protection guideline. However, the arrangement of comprehensive data protection still at the level of Ministerial Regulation which has many gaps, especially the protection of data on partner outlets that have not yet become the scope of its protection.
2. The arrangement for settling disputes on the personal data protection in the Minister of Communication and Informatics Regulation of Personal Data Protection is not yet effective, because the procedure involves the Minister directly, it will cause difficulties if there are complaints submitted by individuals, besides this complaint will be difficult if the pulse counter as the third party has not been covered by the regulation of personal data protection.

BIBLIOGRAPHY:

Books:

Solove, D. J., 2006,*A Brief History Of Information Privacy Law In Proskauer On Privacy,* George Washington University.

Edmon Makarim, 2004,*Kompilasi Hukum Telematika* (Compilation of Telematicsa Law), Jakarta: PT Raja Grafindo Persada.

Purwanto, 2007,*Penelitian Tentang Perlindungan Hukum Data Digital* (Research on Digital Data Legal Protection)*,* Jakarta: Badan Pembinaan Hukum Nasional.

Sinta Dewi Rosadi, 2015,*Cyber Law Aspek Data Privasi Menurut Hukum Internasional* (Privacy Data Aspects According to International Law)*, Regional, dan Nasional*, PT Refika Aditama: Bandung.

Soerjono Soekanto dan Sri Mamudji, 2004,*Penelitian Hukum Normatif Suatu Tinjauan Singkat,* cet.8 (Normative Legal Research: A Brief Review, Publishing 8), Jakarta: PT. Raja Grafindo Persada.

Soemitro dan Ronny Hanitijo, 1983, *Metodologi Penelitian Hukum dan Jurimetri* (Legal Research and Jurimetry Methodology)*,* Jakarta: Ghalia Indonesia.

Journals:

Warren, S., Brandeis, L., D.,"The Right To Privacy", *Harvard Law Review*, Volume 4, 1890.

Moore, A.,"Defining Privacy", *Journal Of Social Philosophy,* Volume 39 Number 3, 2008

Websites:

Andiana Librianty, "Resmi Dibentuk, Ini Tugas Panja Perlindungan Data Pelanggan Seluler", 2018, https://www.liputan6.com/tekno/read/3412126/resmi-dibentuk-ini-tugas-panja-perlindungan-data-pelanggan-seluler, accessed on 25 November 2018.

Ifan Anwar*,* "Menelusuri Perkembangan Ponsel Di Indonesia", 2010, https://tekno.kompas.com/read/2010/04/01/18352875/Menelusuri.Perkembangan.Ponsel.di.Indonesia, accessed on 12 April 2018.

Indotelko.Com, "Kisruh Registrasi, Komisi I DPR Bentuk Panja Perlindungan Data Pelanggan Seluler", 2018, Https://www.Indotelko.Com/Kanal?C=Id&It=Komisi-I-Panja-Perlindungan, accessed on 24 November 2018.

Kata Data, "BerapaJumlah Kartu Telepon Seluler yang Beredar?", 2017, https://databoks.katadata.co.id/datapublish/2017/10/12/berapa-jumlah-kartu-telepon-seluler-yang-beredar, accessed on 12 April 2018.

OECD Privacy Principles, http://oecdprivacy.org, accessed on 18 November 2018.

Oik Yusuf, "7 Hal yang Wajib Diketahui soal Registrasi Kartu SIM", 2017, https://tekno.kompas.com/read/2017/11/01/20190067/7-hal-yang-wajib-diketahui-soal-registrasi-kartu-sim, accessed on 17 November 2018.

Online Etymology Dictionary, "Privacy", https://www.etymonline.com/word/privacy, accessed on 03 September 2018.