PRIVACY AND DATA PROTECTION : INDONESIA LEGAL FRAMEWORK

(Final Version)

Thesis of Master Program in Law and Technology
Universiteit van Tilburg

by
Heppy Endah Palupy
138618

Supervisor :
Prof. J.E. Corien Prins

Tilburg
June 2011

Table of Contents

Abstract

The right to be left alone and the right to know what the personal data collect and to be maintenance could be consider as the one of importance human right in modern era. This right might be the one of right that influence by the development of new technology. In the western countries, the privacy and data protection becoming one of importance issues in relation with modern human life. They have more specific and complete regulation that describe and protect the privacy and personal data of the citizen. The protection in each countries are different. European Union has two importance policies in relation to Privacy and Data protection. The first is the council of *Europe's Convention on Data Protection* and the second is EU *Data Directive.* The U.S design differently with EU, there is no single laws that provide a comprehensive protection of privacy or data. There have been a number of law and executive orders dealing with specifically with privacy and data protection concept.

There are some international instrument related with privacy and personal data protection such as OECD guidelines 1980, APEC privacy framework, Council of Europe Convention 1981 and European Convention for the Protection of Human Right and Fundamental Freedom. This international instrument are contains some principles in privacy and data protection. This international instrument influences the regulation application on privacy and data protection in EU, US and Asia.

In Indonesia, the privacy right and data protection could be considered as a one of important regulation. It can be one of the issues in the latest community influencing by the way we communicate today and the faster development of technology. The growth of technology provide any chance to gather, analyses and disseminate the information in a ways and it is need legal protection of privacy to those legal certainty. But, as a developing country, Indonesia has a large community in technology and communication user. Indonesia do not have any specific regulation in privacy and data protection. Every legal protection of privacy and data protection are giving by existing law. The Urgency to address issues about privacy and data protection in enhancement of technology, because sometimes the existing law, cannot work properly in order to the technology development associate with privacy and data protection. This thesis intend to answer the problem that arise in concept of Privacy and Data Protection in Indonesia, To what extend Indonesia regulate the privacy data protection in associated with existing law and fast development of technology. The analysis is conducted by examining the regulatory framework used to safeguard this right to privacy and data protection.

List of Abbreviations

APEC : Asia-Pacific Economic Co-operation

BCR : Binding Corporate Rules

COPPA : The Children's Online Privacy Protection Act

ECHR : European Convention on Human Right

ECtHR : European Court of Human Right

ECPA : The Electronic Communications Privacy Act

EC : European Commission

EU : European Union

ETS 108 : The Convention for the Protection of Individuals with regard to establishing the Automatic Processing of Personal Data

EVRM : Verdrag tot Bescherming van de Rechten van de Mens

FCRA : The Fair Credit Reporting Act

FERPA : The Family Educational Rights and Privacy Act

FOIA : Freedom of Information Act

HIPAA : The Health Insurance Portability and Accountability Act

ICJ : European Court of Justice

OECD : Organization for Co-operation and Development

PIPA : The Personal Information Protection Act

PRC : The People's Republic of China

TBDF : Trans-border Data Flows

US : The United states of America

Chapter 1 – Introduction

1.1. Background

The rapid development of technology has had a significant impact upon social life. Throughout the world, technology offers many facilities that contribute to fast connectivity. At the same time, accessibility to technological advances raises questions about the right of individuals to retain the confidentiality for certain types of information. The easy and swift dissemination of information through technology creates threats to privacy by providing great opportunities for surveillance by persons who have access to personal information about others.

The concept of *the right to privacy* became popularly recognized in 1890 when Samuel Warren and Louis Brandeis wrote the essay titled, "The Right to Privacy," published by *Harvard Law Review.*[1] They proposed the recognition of an individual's "right to be let alone" and argued that this right should be protected by existing law, as a matter of human rights. Thus, the concept of a right to privacy is very well recognized but is still difficult to define. Privacy, as a part of human rights, identifies the protection of personal data as an important right. Data protection regulation is a key business and economic issue for information-intensive businesses in the modern era. Modern business practices often involve data manipulation such as segmentation of customer data, including data mining and data harvesting, creating customer profiles, consolidating global data processing, and other business processes.[2] Several countries have specific laws to protect the privacy and personal data of their citizens. This is particularly true in Europe and the United States, where there are specific regulations about privacy and data protection. The concepts of privacy that obtain in Europe and the US show differences in their characteristics, however. The US has no single regulation on privacy and data protection that can be narrowly applied. However, in the European Union, which is governed by supra-national policies, the concept is protected by the EU Data Protection Directive.

---

[1] See Samuel D, Warren, Louis D. Brandeis, "The Right To Privacy," 1890, *Harvard Law Review*, Vol IV No. 5.

[2] Data privacy protection across Asia –A regional perspective, Freshfields Bruckhaus Derringer LLP, October 2008, http://www.freshfields.com/publications/pdfs/2008/oct08/24238.pdf

Regulations concerning the right to privacy and data protection could be considered as one of the most important areas of need in Indonesia. It is one of the major issues in the modern community, which is being affected by the way we communicate today, the new way of business or commerce, and by the rapid development of technology. The growth of technology provides many opportunities to gather, analyze, and disseminate information in various ways and this certainly makes legal protection of privacy a necessity. As a developing country, Indonesia has a large community of users of technology and communication systems. However, Indonesia does not have any specific regulations to govern privacy and data protection. Any legal protection of privacy and data is provided by existing law. With the enhancement of technology, the urgency to address issues about privacy and data protection is increasing, because sometimes the existing laws cannot work effectively in light of rapid technology development and its implications for privacy and data protection. As a member of Asia-Pacific Economic Cooperation (APEC) and also as a country that, as a potential member of the Organization for Economic Co-operation and Development (OECD) Guidelines, Indonesia needs to address any regulation concerning privacy and data protection.

1.2. **Research Questions**

Based on the definition of the problem as outlined above, the main research question to be examined in this thesis is the following: *Considering the limitations of existing law and the fast development of technology, to what extent does Indonesia need to introduce regulations to ensure privacy and data protection?* In order to answer this main question, I will provide answers to the following related questions:

- *What is the nature of the current privacy and data protection regulations associated with Indonesia's legal system?*
- *Does the existing legal standard of privacy and data protection offer adequate protection to people in Indonesia?*
- *What is the influence of international standards and regulation of privacy and data protection for the Indonesian situation? And, how important is it for Indonesia to have specific regulations about privacy and data protection?*

1.3. Methodology

In order to answer the main question and address the subsidiary problems mentioned above, this paper will include a literature review and examination of case law. As the main source, I will review Indonesia's existing legal regulations as they pertain to privacy and data protection. I will review, in particular, regulations concerning technology, electronic transactions, telecommunications, and information systems. I will also analyze the literature concerning current regulations, in accordance with current Indonesian conditions, and compare its development in privacy and data protection with developments in the EU and the US as far as regulations in privacy and data protection are concerned.

1.4. Structure

This thesis is divided into five chapters. Chapter 2 will firstly give a description of privacy and data protection, an international instrument in Europe, the US, and Asia, and a brief overview of privacy and data protection in some countries of Asia. Then, this chapter will also explain what international privacy and data protection means for Indonesia. Chapter 3 will discuss the regulatory frameworks of privacy and data protection in Indonesia, along with the legislation enacted in relation with privacy and data protection in the country. Basically, in this chapter, we will further elaborate and provide more evidence on why those regulatory frameworks are lacking in full adequacy. Subsequently, Chapter 4 will analyze the evidence presented in Chapter 3, and then I will elaborate the extent and nature of the privacy and data protection legislation in Indonesia. Lastly, Chapter 5 will provide answers to the research question and draw conclusions.

Chapter 2 – Overview of Privacy and Data Protection in Countries Relevant to Indonesia

To give a good understanding of the issues addressed on the topic, in this chapter, we will present a brief overview of the nature of privacy and data protection, with a focus on the international instruments of privacy and data protection in Europe, the US, and Asia. This is followed by a description of the development of privacy and data protection in some countries of Asia. Then, this chapter will also explain the international privacy and data protection means for Indonesia, as well as provide the definition of privacy and data protection and explore the possibility of privacy and data protection legislation in Indonesia.

2.1. Basis of Privacy and personal Data Protection Needs

There is an international consensus that data protection laws are necessary to protect an individual's right to privacy[3] and should be considered as either a basic and inalienable human right or as a personal right or possession.[4] The catalysts for protection are: (1) technological and organizational development, (2) public fear of those developments, and (3) the nature of other legal rules, which form the normative basis for such laws.[5] Data protection and privacy rights

[3] See Tan, Johanna G, "A Comparative Study of the APEC Privacy Framework – A New Voice in the Data Protection Dialogue?" *Asian Journal of Comparative Law*, Volume 3, issue I, 2008, page 1, http://www.bepress.com/cgi/viewcontent.cgi?article=1071&context=asjcl. The need to protect personal data and the rationales for doing so are not new; they have been discussed since the 1960s. The European countries were the first to start enacting comprehensive legislation. This caused fears in an increasingly interconnected global economy that European countries with "higher" standards of data protection would enact "borders" and prevent the flow of information to other countries, which did not have equivalent standards of data protection.

[4] Rolf. H Weber, "Internet of Things – New Security and Privacy Challenge," *Computer Law & Security Review 26*, Elsevier Ltd, 2010

[5] Supra note 3, page 5. Johanna explained that it is arguably the third category that shapes the legislative response to the first and second categories. Without a compelling normative basis, it is difficult for a society to articulate what is actually at stake and there is little incentive for the legislature to act and address the problem. Johanna also illustrated that Europeans have experience in association with the uncontrolled use of personal information from their experiences under World War II-era fascist governments and post-War communist regimes where the disclosure of race, religion, or political affiliation led to arrests of otherwise law-abiding citizens.

are closely related. In other words, privacy is a fundamental human right and data protection is one way to protect it.[6]

2.1.1. Privacy

Concern about privacy is concern about the conditions of life.[7] Although privacy is recognized as a fundamental human right,[8] as a concept, it is very difficult to define and varies widely according to the context, nations, and cultures.[9] The concept of privacy is difficult to encapsulate in a universal definition.[10] As there is no accepted definition of the term "privacy" here, privacy will be used in a broad sense to refer to the protection of an individual's personal sphere. The concept of privacy figures prominently in discourse about the social and political threats posed by modern information and communications technology (ICT).[11] Privacy can be divided into concepts such as information privacy, bodily privacy, communication privacy, and territorial privacy.[12]

---

[6] See http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Legislation. Protection of personal data is a right that is separate, but closely linked to the right to privacy: The right to privacy may be described as a right, which prevents public authorities from measures that are privacy invasive, unless certain conditions have been met. The rights to data protection as a consequence of technical development aim to establish conditions under which it is legitimate and lawful to process personal data. Data protection legislation obliges those responsible to respect a set of rules and empowers the people concerned by granting them rights.

[7] Gross, Hayman, "The Concept of Privacy 42," *New York University Law Review 34, 1967*, page 36.

[8] See Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS 108), preamble.

[9] Supra note 7, page 36. The law does not determine what privacy is, but only what situation of privacy will be afforded legal protection.

[10] Makarim, Edmon, *Tanggung Jawab Hukum Penyelenggara Sistem Electronic*, Lembaga Kajian Hukum Technology, Fakultas Hukum UI, Rajawali Press, Jakarta, 2010.

[11] See Regan, P.M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill / London 1995.

[12] Information privacy can be described as the establishment of rules governing the collection and handling of personal data such as credit information and medical information. Bodily privacy describes protection against invasive procedures such as genetic tests, drug testing, and body cavity searches. Communication privacy is described as the protection for security and privacy in matters of communication. Territorial privacy is described as the setting of limits on intrusion into the domestic sphere and other environments such as the workplace or public space.

2.1.2 Data Protection

The development of computer systems and the Internet make information about almost anyone easy to find and share. The basic concept of personal data protection first arose in the 1960s.[13] In 1970, Germany was the first country to enact regulations about data protection; this was followed by a national law in Sweden in 1973 and the United States in 1974, and France in 1978.[14]

The concept of data protection is often treated as a part of privacy protection; such rules provide protection for personal data. The protection may be associated specifically with privacy, and the notion itself may be applied as a wider category of privacy. Seeing data protection as a part of privacy is consistent with the understanding of privacy as a form of secrecy, or a right against disclosure of concealed information, or a right to limit access to the self, or control of information pertaining to one's self.[15] However, there are important differentiations in terms of scope, goals, and content of privacy and data protection. Data protection explicitly protects values that are not the core of privacy such as the requirement of fair processing, consent, legitimacy, and non-discrimination.[16] The expression of data protection concepts is closely related with the right to respect for private and family life.

---

[13] Supra note 3, the need to protect personal data and the rationales for doing so are not new; they have been discussed since the 1960s. European countries were the first to start enacting comprehensive legislation. This caused fears in an increasingly interconnected global economy that European countries with "higher" standards of data protection would enact "borders" and prevent the flow of information to other countries, which did not have equivalent standards of data protection.

[14] Electronic Privacy Information Center (EPIC) and Privacy International (PI): "Privacy & Human Rights 2006" (P&HR 2006), Overview of Privacy, https://www.privacyinternational.org/article.shtml

[15] Purtova, Nadezhda, "Private Law Solution in European Data Protection Relationship to Privacy, and Waiver of Data Protection Rights," *Netherlands Quarterly of Human Rights, 2010*, *vol. 28*, nr. 2, pp. 179–19, page 3.

[16] Gutwith, S. & Hert, P. de, *Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action*, Poullet, Y.; Gutwith, S.; De Terwanghe, C.; Hert, P. de (Ed.) *Reinventing data protection?, Springer science, Dordrecht, 2009, 3–44, page 5.*

2.2. International Instruments of Privacy and Data Protection

2.2.1. OECD Guidelines 1980

The Organization for Economic and Co-operation Development (hereinafter OECD) is an international organization that has 30 member countries. OECD is the arena in which the first transatlantic conflicts over issues of protection took place.[17] The preamble of the OECD Guidelines 1980 stated that "member countries considered it necessary to develop guidelines which would help to harmonize national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data."[18] This guideline continues to represent the international consensus concerning the collection and management of personal information. The preface of the OECD Guidelines also reflects the highlighting of the differing attitudes toward privacy and the need to reconcile "fundamental but competing values such as privacy and the free flow of information" so as to "advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries."[19] By setting out core principles, the guidelines play a major role in assisting governments, business, and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to trans-border data flows, both online and offline. These guidelines were created to decrease the gap between the member countries in the implementation of privacy and data protection legislation.

These guidelines provide the principles for the protection of privacy and trans-border flows of personal data in national and international application. The basic principle of national application is the basis for several principles that have to be applicable in national legislation:[20]

---

[17] See Bennett, Colin. J & Raab, Charles. D, *The Governance of Privacy: Policy Instruments in Global Perspective,* Ashgate Public & Co, 2003, Chapter 4, Page 74–77.

[18] OECD, Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data adopted on 23 September 1980, Preface.

[19] Supra note 3, page 8.

[20] Supra note 18, Part 2.

1. **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle**: Personal data should be relevant to the purposes for which such are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.
3. **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of a change of purpose.
4. **Use Limitation Principle**: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

   a) with the consent of the data subject; or

   b) by the authority of law.
5. **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
6. **Openness Principle**: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle**: An individual should have the right:

   a) to obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to him;

   b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

8. **Accountability Principle**: A data controller should be accountable for complying with measures that give effect to the principles stated above.

The basic principles of member countries are reflected in the international basic principles. The international principles of the OECD guidelines 1980 are as follows:[21]

1. Member countries should consider the implications for other Member countries of domestic processing and re-export of personal data. Member countries should take all reasonable and appropriate steps to ensure that trans-border flows of personal data, including transit through a Member country, are uninterrupted and secure.
2. A Member country should refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations because of those data and for which the other Member country provides no equivalent protection.
3. Member countries should avoid developing laws, policies, and practices in the name of the protection of privacy and individual liberties, which would create obstacles to trans-border flows of personal data that would exceed requirements for such protection.

[21] Supra note 18, Part 3.

2.2.2. Council of Europe Convention 1981

The Council of Europe Convention 1981 was the first legally binding instrument in the data and protection fields.[22] This convention required the parties to take the necessary steps in their domestic legislation to apply the principles it laid down to ensure respect in their territory for the fundamental human rights of all individuals regarding the processing of personal data.[23] These principles concern fair and lawful collection and automatic processing of data, storage for specified legitimate purposes and not for use for ends incompatible with these purposes, or kept for longer than is necessary. They concern the quality of the data, in that they must be adequate, relevant, and not excessive (proportionality); accurate; confidential; contain information of the data subject; and provide right of access and rectification.[24]

The convention provides for the free flow of personal data between states party to the convention. This free flow may not be obstructed for personal data protection reasons unless parties derogate from this provision, which they may do in two specific cases: where protection of personal data in the other party is not "equivalent," or where the data are transferred to a third state, which is not party to the convention.[25]

In June 1999, the Council of Europe amended the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[26] and in 2001, the Council established an Additional Protocol to Convention ETS No. 108 on Supervisory Authorities and Trans-border Data Flows.[27] There are two substantive new provisions, one on the setting up of

[22] Supra note 8.

[23] Supra note 8.

[24] Supra note 8.

[25] Supra note 8.

[26] See Explanatory Amendment Explanatory Memorandum on the amendments to Convention 108 allowing the accession of the European Communities. It provides for the European Communities to express their consent to be bound by the Convention by way of accession. Accession shall be secured by the deposit of an instrument of accession with the Secretary General of the Council of Europe.

[27] This Protocol was open for signature in Strasbourg, on 8 November 2001, on the occasion of the 109th Session of the Committee of Ministers of the Council of Europe. The purpose of this protocol is to improve the application of the principles.

one or more supervisory authorities by each party, and one on trans-border flows of personal data to countries or organizations that are not parties to the Convention. This additional provision on trans-border flows of personal data explains to those recipients that are not subject to the jurisdiction of a Party that they are only indirectly concerned. The Country may derogate from the principle of the free circulation of data between its territory and a recipient that is not subject to the jurisdiction of a Party via another Party, in order to avoid such transfers resulting in the circumvention of the legislation of the Party of origin. There is therefore no specific provision on trans-border flows of data in respect of states or organizations that are not Parties to the Convention.[28]

2.2.3. European Convention for the Protection of Human Rights and Fundamental Freedom/EVRM

The European Convention for the Protection of Human Rights and Fundamental Freedom (hereinafter the Convention), was the impetus of the Convention for the Protection of Individuals with regard to establishing the Automatic Processing of Personal Data (ETS No. 108. In particular, Article 8 of this Convention states that "Everyone has the right to respect for his private and family life, his home and his correspondence."[29] This right can only be restricted by a public authority in accordance with domestic law and in so far as it is necessary, in a democratic society, for the defense of a number of legitimate aims.[30]

Article 8 can be used as guidelines for the European Court of Justice (ICJ)[31] to enforce the fundamental rights of the European community and for a self-contained system of human rights protection.[32] At Strasbourg, several issues in relation with Article 8 were given a more

[28] See Explanatory Report, Article 2, Trans-border flows of personal data to a recipient that is not subject to the jurisdiction of a Party to the Convention. http://conventions.coe.int/treaty/en/Reports/Html/181.htm

[29] See Article 8, Convention for the Protection of Human Rights and Fundamental Freedoms.

[30] Council of Europe, Data protection, History, http://www.coe.int/t/dghl/standardsetting/DataProtection/History_more_en.asp

[31] IJC referred to the Strasbourg Court of Human Right.

[32] De hert, Paul & Guthwirth, S, Data Protection in the Case Law of Strasbourg and Luxemburg Constitutionalisation in Action, in Gutwirth, S, Poullet, Y, De Hert, P., Nouwt, J & De Terwangne, C. (Eds),

specific definition or characteristic as regards data protection. The Court applies a broad definition for the notion of "private life." Private life is not only for the individual's private dwelling and the private sphere. De Hert and Gurtwith describe the notion of "private life" as embracing the development of interpersonal relationships and providing protection not only for the domestic sphere but also (data relating to) certain facts that occur in the public sphere. Strasbourg also brought the recognition of privacy protection to firm and business activities, and conferred rights of protection (optionally for Member states) not only for a natural person but also a legal person.[33]

Regarding Article 8, there is some recognition of the notion of private life, the information about a person belonging in the public domain,[34] the right of the individual to have control, to a certain extent, over the use and registration of their personal information, access claims to personal files,[35] claims regarding deletion of personal data from public files,[36] and claims for transsexuals for the right to have their official sexual data corrected.[37]

Reinventing Data Protection?, Springer Science, Dordrecht, 2009, page 11 (C. Riehle, Book Review of B Siemen, C.M.L.J., 2007, page 1193-1195).

[33] Ibid.

[34] ECtHR; Amann v. Switzerland, § 65 ; ECtHR, Rotaru v. Romania, §§ 43-44; ECtHR, P.G. and J.H. v. the United Kingdom, § 57-58; ECtHR, Segerstedt-Wiberg and others v. Sweden, Application no. 62332/00, Judgment of 6 June 2006, § 72. See E. Brouwer, o.c., 133 & 137 (De hert, Paul & Guthwirth, S, Data Protection in the Case Law of Strasbourg and Luxemburg Constitutionalisation, in Action, in Gutwirth S, Y Poullet, P. De Hert, J Nouwt & C. De Terwangne (Eds), reinventing Data Protection?, *Springer Science*, Dordrecht, 2009)

[35] ECtHR, Gaskin v. the United Kingdom, Application no. 10454/83, Judgment of 7 July 1989; ECtHR, Antony and Margaret McMichael v. United Kingdom, Application no. 16424/90, Judgment of 24 February 1995. ECtHR, Guerra v. Italy, Judgment of 19 February 1998, Reports, 1998-I; ECtHR, McGinley & Egan v. United Kingdom, Applications nos. 21825/93 and 23414/94, Judgment of 28 January 2000 (De hert, Paul & Guthwirth, S, Data Protection in the Case Law of Strasbourg and Luxemburg Constitutionalisation, in Action, in Gutwirth S, Y Poullet, P. De Hert, J Nouwt & C. De Terwangne (Eds), reinventing Data Protection?, *Springer Science*, Dordrecht, 2009)

[36] ECtHR, Leander v. Sweden, Application no. 9248/81, Judgment of 26 March 1987; ECtHR, Segerstedt-Wiberg and others v. Sweden, Application no. 62332/00, Judgment of 6 June 2006 (De hert, Paul & Guthwirth, S, Data Protection in the Case Law of Strasbourg and Luxemburg Constitutionalisation, in Action, in Gutwirth S, Y Poullet, P. De Hert, J Nouwt & C. De Terwangne (Eds), reinventing Data Protection?, Springer Science, Dordrecht, 2009)

[37] ECtHR, Rees v. UK, Judgment of 25 October 1986 Series A, No. 106; ECtHR, Cossey v. UK, Judgment of 27 September 1990, Series A, No. 184; ECtHR, B v. France, Judgment of 25 March 1992 Series A, No. 232-C; ECtHR,

2.2.4. APEC Privacy Framework

The Asia Pacific region cooperates on privacy issues with the Asia Pacific Economic Co-operation Privacy (APEC) Framework of 2004. The importance of protecting information privacy and data protection can be found in the preamble of the APEC[38] Privacy Framework 2004, which mentions that the potential of electronic commerce cannot be realized without government and business cooperation.[39] As an agency of international cooperation, APEC has been required from an early date to address privacy and data protection issues as they impinge on economic matters. To deal with these concerns, APEC has developed a principle-based approach that aims to align the law as much as possible with principles already developed internationally. Accordingly, APEC's privacy framework can serve as starting point it is consists of a single independent privacy enforcement body (or interagency body) as a point of contact for other economies and gives the enforcement body the power to cooperate with enforcement bodies in other economies.[40] The role of the APEC Privacy Framework 2004 is to balance and promote effective information privacy protection and the free flow of information.[41] The APEC privacy framework contains nine principles:[42]

1. **Preventing Harm**: A principle designed to prevent the misuse of information.

Christine Goodwin v. the United Kingdom, Application no. 28957/95, Judgment of 11 July 200 (De hert, Paul & Guthwirth, S, Data Protection in the Case Law of Strasbourg and Luxemburg Constitutionalisation in Action, in Gutwirth S, Y Poullet, P. De Hert, J Nouwt & C. De Terwangne (Eds), reinventing Data Protection?, Springer Science, Dordrecht, 2009)

[38] The members of the APEC are Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Republic of the Philippines, The Russian Federation, Singapore, Chinese Taipei, Thailand, United States of America, and Viet Nam.

[39] See APEC Privacy Framework 2004, Preamble, page 2.

[40] Crompton, Malcom, *Overview of Asian Privacy Law Lesson Learned and a Possible Way Forward*, Privacy Symposium Sponsored by the Institute of Law China Academy of Social Science, Role of Information Service Providers, 2006, page 9.

[41] Supra note 3, page 16

[42] Supra note 39, preamble, page 2.

2. **Notice**: Directed toward ensuring that individuals are able to know what information is collected about them and for what purpose.
3. **Collection Limitations**: The collection of personal information that is relevant to the purposes of collection.
4. **Uses of Personal Information**: Personal information should be used only to fulfill the purposes of collection and other compatible or related purposes.
5. **Choice**: This principle is to ensure that individuals are provided with choice in relation to the collection, use, transfer, and disclosure of their personal information.
6. **Integrity of Personal Information**: Personal information should be accurate, complete, and kept up to date to the extent necessary.
7. **Security safeguards**: This principle recognizes that individuals who entrust their information to another party are entitled to expect that their information be protected with reasonable security.
8. **Access and Correction**: Individuals have the ability to access and correct their personal information.
9. **Accountability:** Personal information should be accountable. The Parties holding the personal information should be accountable.

APEC member are not obliged to implement domestically the APEC privacy Framework in any particular way**.**[43] Hence, there are different situations and conditions that apply in addressing privacy and data protection among APEC members. No harmonized regulations exist between the members of APEC.

[43] Australian Law Reform Commission Report 108, par. 31.35.

2.3. Privacy and Data Protection in the EU

2.3.1. General

There are two important supra-national policies in Europe in relation to data protection. The first is the Council of Europe's Convention on Data Protection and the second is the EU Data Directive.[44]

The Council of Europe was set up after the Second World War to help unite Europe by fostering closer relations between the states belonging to the community, ensuring economic and social progress by common action to eliminate the barriers that divide Europe and promoting democracy based on the fundamental rights recognized in the constitutions and laws of the Member States and in the European Convention for the Protection of Human Rights and fundamental freedom.[45] That Convention recognizes the right to privacy as one of the fundamental human rights. The Council's concern with the processing of personal information grew slowly with advances in information technology and the increase in the use of such data. In the late 1960s, the Council's Committee of Experts on Human Rights conducted a survey regarding human rights and modern scientific and technological developments. It concluded that existing laws did not provide adequate protection for individuals given the developments in these areas. Several other committees examined various aspects of the problem and came to similar conclusions. In 1976, the Council established a Committee of Experts on Data Protection that reported its findings in early 1979, and the result was the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS 108). The Council of Europe Convention sets forth the data subject's right to privacy, enumerates a series of basic principles for data, provides for trans-border data flows, and calls

[44] Stratford, Jean Slemmons & Stratford, Juri, Data Protection and Privacy in the United States and Europe, Paper presented at the IASSIST Conference, May 21, 1998, at Yale University, New Haven, Connecticut. Jean Slemmons Stratford, University of California, Davis, and Juri Stratford, University of California, Davis.

[45] Commission of the European Community. Communications on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security, Directive 95/46/EC, Article 3

for mutual assistance between parties to the treaty including the establishment of a consultative committee and a procedure for future amendments to the convention.[46]

The Commission of the European Community recommended that member states ratify the Council of Europe Convention and warned that it might introduce its own directive on the subject. When it did so, the primary purpose of the directive was to standardize protection across the Community. The EU Data Protection Directive reaffirms the principles outlined in the Council of Europe Convention.[47] The data protection directives were enacted to harmonize privacy and data protection legislation between European countries. Many countries in Europe had enacted legislation designed to balance the individual's right to data protection. This was undertaken at the national level long before the initiative was taken at the EU level in the early 1990s to ensure more harmonization on the basis of Convention 108.[48]

2.3.2 Rules on export of personal data

2.3.2.1. General

European countries recognize the export of personal data as a part of a privacy and data protection regime. The EU embraces the OECD Guidelines as an international consideration of protection on personal data transfers.[49] Following the OECD Guidelines, the Council of Europe enacted the Convention for the Protection of an Individual with Regard to Automatic Processing of Personal Data (ETS 108) as a legal basis of open transfer data among member states and for non-member states.[50] The additional protocol of ETS 108 introduced in 2001 provided that the

---

[46] Ellis, Sarah and Oppenheim, Charles, "Legal Issues for Information Professionals, Part III: Data protection and the Media – Background to the Data Protection Act 1984 and the EC Draft Directive on Data Protection," *Journal of Information Science 19*, 1993, page 85.

[47] Swire, Peter B. and Litan, Robert E., Avoiding a Showdown over EU Privacy Laws, Brookings Policy Brief, no. 29 (February 1998) (URL http://www.brook.edu/comm/ policy briefs/pb029/pb29.htm)

[48] Official website of European Data Protection Supervisor, The European Guardian of Personal data Protection, http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2

[49] Supra note 18, Part 3, Para 15–18

[50] Supra note 8, Article 12–13.

transfers are allowed if there is an adequate level of data protection.[51] This additional protocol is a legally binding source of privacy and personal data protection, which has a close relation with the transfer of personal data.

The EU also has a Directive[52] that protects the transfer of personal data among the Member States. Article 1 (2) of the Directive mentions that Member States shall neither restrict nor prohibit the free flow of personal data between Member States. This is based upon the assumption that following implementation of the Directive, all Member States will provide a basic level of data protection and therefore there will be no need to restrict the transfer of data flows because the privacy of citizens with respect to the processing of personal data will be protected throughout the Union.[53] The Directive provides for the regulation of data transfer on two levels: data transfer between Member States and data transfer between Member States and non-Member States. All transfers of personal data between Member States are to be lawful. This is also the aim of the Council of Europe Convention; however, the width of interpretation afforded to signatories when implementing the Convention has meant that there is still scope for controlling transfers between signatory states.

The EU Directive further prohibits the transfer of personal data to non-EU countries that do not meet the European "adequacy" standard for data protection**.** Directive 95/46/EC sets the minimum level of data protection for the Member States; provisions of the Directive are to be the basic criteria to evaluate contents data protection rules and procedural means for ensuring data users' compliance with the data protection rules in a third country. Basic principles to be included in data protection rules shall include the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle,

---

[51] Article 2 (1) of the Additional Protocol to the Convention for The Protection of Individuals with regard to Automatic processing of Personal Data, Regarding Supervisory Authorities and Trans-border Data Flows, Strasbourg 2001.

[52] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[53] White, Alison, "Control of Trans-border Data Flow: Reaction the Data Protection Directive," *International Journal of Law and Technology, Vol 5 No 2*, 2011 page

and the right of access, rectification, and opposition, and restrictions on onward transfers. Since there is no uniform legal enforcement pattern or model, the objectives of a data protection system are defined as: (a) to deliver a good level of compliance with the rules; (b) to provide support and help to individual data subjects; and (c) to provide appropriate redress to the injured party where rules are not complied with.[54] The Article 29 Data Protection Working Party has defined adequacy and proposed criteria of adequacy.

2.3.2.2. Binding Corporate Rules

Binding Corporate Rules (hereinafter BCRs) are a set of rules adopted within a particular company or corporate group that provide legally binding protection for data processing within the company or group.[55] BCRs were developed by EU Article 29 Working Party for use by multinational organizations or groups of companies as a mechanism for transferring personal data throughout the organization. BCRs need to be approved by every European data protection authority in whose jurisdiction a member of the group will rely on them,[56] but the advantage is that the approval process is simplified as an application is made to one national "lead" data protection supervisory authority in Europe and that authority liaises with all other authorities to seek approval. This mechanism prevents companies from sending personal data outside the EU except when the destination country has been pre-approved as having adequate

[54] Kong, Lingjie, "Data Protection and Trans-border Data flow in a Global Context," *The European Journal of International Law, Vol. 21 no. 2* © EJIL 2010, page 444, http://ejil.oxfordjournals.org/content/21/2/441.full.pdf+html

[55] International Chamber of Commerce, ICC Task Force on Privacy and Protection of Personal Data, ICC report on binding corporate rules for international transfers of personal data, report prepared by Christopher Kuner and Robert Bond. Paris. 2004. http://www.iccwbo.org/uploadedFiles/ICC/policy/ebusiness/pages/FINAL_ICC_BCRs_report_rev.pdf

[56] The company has to ask for the approval by the DPAs of the countries where the processing of data and cross border data transfers take place. See WP 107, Article 29 - Data Protection Working Party. Working Document Setting Forth a Cooperation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting from "Binding Corporate Rules." 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_en.pdf

data protection.[57] BCRs are tailor-made solutions for company-enforceable data protection that describes where the data will be exported and the purposes for those exports.

Article 29 Working Party believes that BCRs are the preferred solution for global data exports. BCRs offer multinationals transferring data regarding which countries do not have adequacy protection with the EU.[58] BCRs allow parties to have an ability to create their own, custom-built, data-flow policies that more accurately reflect the unique nature of their business and the ways in which they exploit data.[59]

BCR principles provide protection with the principles mentioned in EU directives such as notice, choice, use, security, correction, and enforcement. BCRs propose to be internally binding on group members and their employees and externally binding against the group, be effective and be transparent, detailing the personal data concerned, where personal data will be transferred and how and why it will be processed.[60]

2.4. Privacy and Data Protection in the US

2.4.1. General

There is no single law in the United States that provides a comprehensive treatment of data protection or privacy issues. Privacy provisions exist in common law, and in the federal and state constitutions, and in a variety of statutes addressing specific issues that have arisen in

[57] Supra note 52, article 25.

[58] Article 25 on the EU Directive 95/46/EC, it is prohibited to export the data to a third country outside of the EEA unless that country “ensures an adequate level of protection" for the exported data.

[59] Supra note 55.

[60] See WP 74, Article 29 Data Protection Working Party-Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 2003. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf

different sectors and jurisdictions.[61] As a result, this makes it hard to define the relevant privacy theories.[62]

Regarding the constitutional interpretations provided by the courts and the international agreements mentioned above, there are many laws and executive orders dealing specifically with privacy and data protection in the US. Avner and Nicholson compiled the Legislative Measures Affecting Privacy and Data Protection. They include the legislation primarily protecting privacy from the government, as well as legislation addressed primarily to the private sector.[63]

Legislation primarily protecting privacy from the Government is as follows:[64]

a. **The Privacy Act of 1974:** The Act obliges federal agencies to collect information to the greatest extent possible directly from the concerned individual, to retain only the relevant and necessary information, to maintain adequate and complete records, to provide individuals with rights of access to review and have their records corrected, and to establish safeguards to ensure the security of the information.
b. **The Electronic Communications Privacy Act of 1986 (ECPA):** The ECPA requires government officials who wish to intercept or obtain electronic communications—such as email or other information available electronically, such as Internet Service Providers' (ISP) logs and public library patron records—to seek and receive permission, known as a "Title III" order, from a federal judge. The ECPA has been amended by the USA PATRIOT Act.
c. **The Privacy Protection Act of 1980:** This act serves to protect free speech and First Amendment rights, not privacy in general. The act prohibits government from searching

---

[61] Levin, Avner and Nicholson, Mary Jo, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground." *University of Ottawa Law & Technology Journal, Vol. 2, No. 2*, pp. 357-395, 2005. Page 361, SSRN: http://ssrn.com/abstract=894079.

[62] Solove, Daniel J., "Conceptualizing Privacy." *California Law Review, Vol. 90*, p. 1087, 2002. SSRN: http://ssrn.com/abstract=313103

[63] Supra Note 61. Levin Avner.

[64] Protecting the citizen data collected by Government.

or seizing any work or materials held by a person intending to disseminate it to the public in some form of public communication (e.g., newspapers, books, broadcasts) without court authorization (e.g., a subpoena).

d. **The Family Educational Rights and Privacy Act (FERPA):** This act protects the privacy of student records at all educational institutions receiving federal funding (e.g., universities and colleges).
e. **The Driver's Privacy Protection Act:** This act prohibits the public disclosure of personal information contained in state department of motor vehicle records for marketing purposes, unless drivers expressly consent. Personal information can still be disclosed for many other purposes (e.g., private investigations, toll payment, identity confirmation) without consent, so the act, despite its title, only offers limited protection to drivers.
f. **The Right to Financial Privacy Act:** This act protects the confidentiality of personal financial records, but only from government.

Legislation protecting privacy in the private sector:

a. **The Fair Credit Reporting Act (FCRA):** The FCRA recognizes the consumer's right to privacy (e.g., the consumers have a right to access their records, albeit for a fee); the FCRA is primarily concerned with ensuring credit accuracy.
b. **The Financial Modernization Act:** The act requires that financial institutions have a privacy policy and that they bring it to their customers' attention. Although financial institutions are broadly defined (e.g., car dealerships offering leases are included), the legislation fails to set any principles for those policies. Customers are able to opt-out—that is, stipulate to their financial institutions that they do not want their personal information to be shared with other businesses in certain circumstances.
c. **The Identity Theft and Assumption Deterrence Act:** The act does not provide protective measures for privacy. Rather, it creates criminal sanctions for invasion of privacy in order to deter identity theft.
d. **The Cable Communications Policy Act:** This act regulates the cable industry in the U.S. generally, and incorporates several specific privacy measures. Cable companies are not

allowed to collect personal information without consent, or to disclose it to third parties, unless the information is necessary for service purposes.

e. **The Videotape Privacy Protection Act:** The act prohibits video stores from disclosing customer records without their consent. The act requires video stores to destroy personal information within a year of the date that it is no longer necessary for the purpose for which it was collected.
f. **The Telephone Consumer Protection Act:** Telemarketers are required under the act to maintain such a list and abide by the wishes of listed consumers not to be called.
g. **The Telecommunications Act of 1996: The** Communications Acts 1934, 33 are specific privacy measures designed to limit marketing on behalf of telephone companies, based on their ability to access their customers' calling patterns.
a. **The Health Insurance Portability and Accountability Act of 1996 (HIPAA):** To protect personal medical information traveling from healthcare providers and administrators to potential employers, HIPAA establishes privacy measures, which aim to be a minimal standard to which states can add. Personal health information cannot be disclosed without the patient's express consent, plus patients have a right to access and amend their information, and a right to know to whom the information has been provided
b. **The Children's Online Privacy Protection Act of 1998 (COPPA):** The purpose of this act is to protect children's personal information from collection and misuse by commercial websites.

Jean Slemmons Stratford and Juri Stratford describe the most important of the laws dealing exclusively with personal information as the Privacy Act of 1974.[65] This law is binding on the federal government and states it does not have any authority over the collection and use of personal information held by other private and public sector entities. The Privacy Act (PL 93-579) is a companion to an extension of the Freedom of Information Act (FOIA) of 1966. FOIA was primarily intended to provide access to government information. It did exempt the disclosure of personnel and medical files that would constitute "an unwarranted invasion of

[65] Stratford, Jean, Slemmons, Jean & Stratford, Juri, Data Protection and Privacy in the United States and Europe, presented at the IASSIST Conference, May 21, 1998, at Yale University, New Haven, Connecticut. Jean Slemmons Stratford, University of California, Davis, and Juri Stratford, University of California, Davis.

personal privacy."[66] This provision was initially used to deny access to people requesting their own records. Therefore, the Privacy Act was also adopted both to protect personal information in federal databases and to provide individuals with certain rights over information in those databases. The act has been characterized as "the centerpiece of U.S. privacy law affecting government recordkeeping."[67] The act was developed explicitly to address the problems posed by electronic technologies and personal records systems and covers most personal records systems maintained by the federal government. The act set forth some basic principles of "fair information practice" and provided individuals with the right of access to information about themselves and the right to challenge the contents of records. It states that personal information may only be disclosed with the individual's consent or for purposes announced in advance. The act also requires federal agencies to publish an annual list of systems maintained by the agency that contain personal information.

2.4.2. Safe Harbor Principles

The European Commission's Directive on Data Protection went into effect in October 1998 and prohibits the transfer of personal data to non-European Union countries that do not meet the EU "adequacy" standard for privacy protection.[68] While the US and the EU share the goal of enhancing privacy protection for their citizens, the IS takes a different approach to privacy from that taken by the EU. The US uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The EU, however, relies on comprehensive legislation that requires, among other things, the creation of independent government data protection agencies, registration of databases with those agencies, and in some instances, prior approval before personal data processing may begin. As a result of these different privacy approaches,

[66] Freedom of Information, Title 5 U.S.C. 552(b) (6), http://www.justice.gov/oip/amended-foia-redlined-2010.pdf

[67] Aldrich, Robert, Privacy Protection Law in the United States, (NTIA Report 82–98) in the U.S. Congress. House Committee on Government Operations. Oversight of the Privacy Act of 1974: Hearings. 98th Congress, 1st Session, 7-8 June 1983, 489 (Y4.G74/7:P93/11/974).

[68] See article 25 Data protection Directive 95/46/EC.

the directive may have significantly hampered the ability of U.S. organizations to engage in a range of trans-Atlantic transactions.[69]

In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the directive, the U.S. Department of Commerce, in consultation with the European Commission, developed a "safe harbor" framework and this website provides the information an organization should need to evaluate—and then join—the US-EU Safe Harbor program.[70] The European Commission has also made an adequacy finding regarding specific transfers to the Safe Harbor system.

To diminish the uncertainty and provide a more predictable framework for such data transfers, the Safe Harbor framework includes the principles that were developed in consultation with industry and the public to help trade and commerce between the U.S. and EU, such as:[71]

1. **Notice.** This principle says that a company or organization must inform an individual if they have a purpose for using or collecting their data. It explains the purpose and rules under which the organization or companies must provide contact information and disclose any information to third parties.
2. **Choice.** The individual has opportunities to choose what and how personal information is used by an organization or companies. The individual can choose the offering by an organization with enough information and has the choice to opt-out or opt-in.
3. **Onward transfer.** To disclose information to a third party, organizations or companies must apply the principles of notice and choice. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor privacy principles or is subject to the directive. As an alternative, the organization can execute a written agreement with a

[69] The adequacy decision of the European Commission was published at the *Official Journal of the European Communities*, volume 43. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF

[70] US-EU Safe Harbor official website, https://www.export.gov/safeharbor/eu/eg_main_018476.asp

[71] Supra note 70. US-EU Safe Harbor official website, https://www.export.gov/safeharbor/eu/eg_main_018476.asp

third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.[72]

4. **Security.** The organizations or companies must show that they have adequate security in maintaining, using, and disseminating the personal data. They must ensure that the personal information collected is secure from any misuse, from loss, unauthorized access, disclosure, alteration, and destruction.
5. **Data Integrity.** Personal information must be relevant to the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use and be accurate, complete, and current.
6. **Access.** Individuals must have access to personal information that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
7. **Enforcement.** To ensure compliance with Safe Harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each complaint and dispute can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make adhere to the Safe Harbor principles; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants and Safe Harbor benefits will no longer be assured.

Safe Harbor principles offer the same quality of protection for data transfer. So, the confidentiality of the data must be safe and secure when the data have to be transferred to another country. The Safe Harbor is a legal basis for cross-border data transfers, although it has limited applicability because it only applies to transfers between companies in the European

[72] *Supra* Note 70. US-EU Safe Harbor official website, https://www.export.gov/safeharbor/eu/eg_main_018476.asp

Economic Area and the specific companies in the U.S. that have joined the Safe Harbor Framework.[73]

2.5. Privacy and Data Protection in Asia

2.5.1. General

The development of privacy and data protection legislation in Asia is completely different. The main difference is that the regulations for privacy and data protection are not harmonized in Asia, unlike the regime in Europe, which is governed by the EU data protection directive. This often creates a problem for multinational businesses because they must comply with a raft of fragmented local laws and regulations that often lack transparency.[74] The differentiated level of protection on privacy and data between the countries in the Asian region make some inconsistencies in protection and make it more difficult for business and modern commerce.

The EU has already anticipated the problem caused by the fragmentation of law, and they have way to alleviate the legislation between the members but while still preserving respect for local circumstances and culture.[75] This is an appropriate response to the APEC way. More specifically, a system must to be found to ensure that when more than one jurisdiction is involved, the personal information does not lose some of the protection that it was given when it was first collected.[76] In other words, the protection between one legislation in one jurisdiction must be harmonized so that they are the same. A number of Asian economies are thinking about developing new or more comprehensive privacy laws. This is within the context

[73] The decision by U.S. organizations to enter the Safe Harbor is entirely voluntary. Organizations that decide to participate in the Safe Harbor must comply with the Safe Harbor's requirements and publicly declare that they do so. See U.S.-EU Safe Harbor Framework, The U.S.-EU Safe Harbor Guide to Self-Certification, U.S. Department of Commerce, page 10, http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_018879.pdf

[74] Freshfields Bruckhouse Delinger, *Privacy Protection Across Asia - A regional Perspective*, Freshfiel Bruckhouse Delinger LLP, 2008, http://www.freshfields.com/publications/pdfs/2008/oct08/24238.pdf

[75] See the EU regulatory initiative.

[76] See APEC Privacy principle 9, accountability follows the data – no more, no less.

of the privacy and data protection overview of some Asian countries. These countries have had a close relation with Indonesia in terms of economic or political measures in the last 10 years.[77]

2.5.2. China

China, as a new economic force in the world, is trying to develop privacy and data protection. Both the domestic social economic development and the international trade and economic exchange will eventually push China to observe international standards of privacy and personal data protection. Currently, China's privacy and personal data protection shows a mixed picture. On the one hand, it reflects the economic demand in an increasingly globalized marketplace; on the other, it shows the people's increasing privacy awareness.[78] Unfortunately, although the Chinese Constitution acknowledges the privacy of communications,[79] China does not address the protection of privacy or personal data generally.

The Chinese Constitution provides that no organization or individual may, on any ground, infringe on citizens' freedom of privacy of correspondence, with the exception that public security or prosecutorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law for the purpose of safeguarding State security or investigating crimes.[80] The General Principles of the Civil Law set out the legal basis for civil rights protection but do not stipulate privacy as an independent right. In addition to the general laws, a few specific laws, to a certain extent, address the issue of privacy protection:[81]

a. **The Law on the Protection of Minors (1991)** prohibits the disclosure of the personal secrets of minors and with regard to cases involving crimes committed by minors, the names, home addresses, and photos of such minors as well as other information that

[77] http://www2.bkpm.go.id/file_uploaded/public/5%20NEGARA%20PMA.pdf

[78] Hong Xue, Privacy and Personal Data Protection in China: An Update for the year-end 2009, Institute for the Internet Policy & Law, Beijing Normal University, PR China, Elsevier Ltd, 2010.

[79] Invasions of residence privacy and communication privacy are crimes under the 1997 Chinese Criminal Law. See Article 245–246.

[80] See Article 40 of the Chinese Constitution (1982)

[81] Supra note 78.

could be used to deduce who they are, may not be disclosed, before the judgment, in news reports, films, television programs, or in any other openly circulated publications.

b. **The Law on the Identity Card of Residents (2003**) stipulates that no organization or individual has the right to check or hold a citizen's identity card except for the police, who are required to keep confidential any personal data obtained from the identity cards.

c. **The Regulations on Publication of Governmental Information (2008)** prohibit any administrative organ from publishing governmental information that involves State secrets, trade secrets, or personal privacy.

d. **The Lottery Administration Regulations (2009)** provide that lottery issuance, sale, agent organizations, or any others who acquire from professions or businesses the personal information of the lottery winner shall keep the winner's personal information secret.

e. **The People's Republic of China (PRC) Constitution** recognizes some related protection, including:[82]

- Article 38 and Article 40 of the People's Republic of China (hereinafter PRC) Constitution, under which the personal dignity and the freedom and privacy of correspondence of citizens of the PRC are recognized and protected, although an express constitutional right to privacy is not established by these provisions.
- Article 120 of the General Principles of the PRC Civil Law recognizes the right to identity and the right to protection of a person's name, portrait, reputation, or honor.
- Article 253 of the PRC Criminal Law, which was amended by the Chinese legislature on 28 February 2009, to make working personnel of state agencies and organizations in finance, telecom, transportation, education, or healthcare potentially subject to criminal liability if they sell or illegally provide to others the personal information of citizens obtained during such organizations' performance of their official duties or provision of services.

[82] See by Yu Du, Matthew Murph, Privacy Protection in China – Latest Developments, 2010, http://www.mmlcgroup.com/sitebuildercontent/sitebuilderfiles/privacy270810.pdf

- Article 1 of the Interpretation of the Supreme People's Court on Issues Regarding the Ascertainment of Liability for Compensation for Psychological Damages in Civil Torts grants a person whose privacy has been infringed the right to claim for psychological damages.

As a new economic power, China occupies a strong bargaining position in the world. The Chinese authorities cooperate with Indonesia in a number of economic and investment areas. Indonesian imports from China are bound to rise as demand from the Indonesian manufacturing sector for raw materials and machinery remains strong. Excluding consumer goods, China is becoming a major supplier for many Indonesian industries.[83] China and Indonesia are APEC members and, from a privacy perspective, the spread of privacy protection legislation must be welcomed where it is having a material effect on improving individual privacy and facilitating trust in modern forms of commerce.

2.5.3. Japan

Japanese privacy protection is not well developed. The Japanese decided to have privacy and data protection based on international demand.[84] In April 2005, the Act for Protection of Personal Data was enacted in Japan. Based on the idea that ICT could be a strategic technology in the 21st century, the Japanese government has adopted a policy to construct a "highly-networked information society" and is developing its infrastructure. The Japanese government followed a policy of self-regulation for the private sector, especially relating to electronic commerce, until 1999, when lawmakers started working on the Personal Information Protection Bill.[85] The Personal Information Protection Act 2003 Law No. 57 (PIPA) was passed and enacted on 23 May 2003 and came into effect for private sector entities on 1 April 2005.[86]

---

[83] Official website Indonesia – China cooperation, http://www.cic.mofcom.gov.cn/ciweb/cci/info/Article.jsp?a_no=257621&col_no=521

[84] Orito, K. and Kiyoshi, M., Privacy Protection in Japan: Cultural Influence on the Universal Value, 2002-2006 , http://bibliotecavirtual.clacso.org.ar/ar/libros/raec/ethicomp5/docs/pdf_papers/52Orito,%20Yohko.pdf

[85] Crompton Malcom mentions on the Privacy symposium sponsored by the Institute of Law China Academy of Social science in 2006 that the Bill was revised in 2002 after there was a debate including from the media, and revised again in response to public criticism that it would, among other concerns, violate freedom of the press. In response to criticism from opposition parties and the media, the ruling coalition dropped the contentious

PIPA is quite strongly based on requiring explicit consent from the individuals involved, especially for the use of personal information and its disclosure to third parties. The law does provide for some exceptions but these are narrowly framed and appear to have caused considerable confusion about how these work. Some entities have interpreted the law too narrowly. A growing number of businesses have refused to lawfully share personal information with public officials and others, for fear of violating PIPA. As a result, a number of socially beneficial uses of personal information have become unnecessarily restricted or discontinued since PIPA came into force. The press has reported that a number of Ministries needed to issue clarifying guidance about how the law operates in relation to school emergency contact lists and other normal school activities and also regarding disclosure of personal information for the recall of defective products. There also appeared to be a gap between consumer expectations of how the law should apply to marketing, and how it was actually applied. [87]

2.5.4. Singapore

There is no general data protection or privacy law in Singapore, but the protection is divided into the public sector, private sector, and common law. Singapore has both a strong common law tradition as well as appropriately structured statutory provisions to regulate the use of personal data. Under the general law, confidential information may be protected under a duty of confidence. Personal information is also protected under sector-specific laws such as the Banking Act, Statistics Act, the Official Secrets Act, and the Statutory Bodies and Government Companies (Protection of Secrecy) Act. There is, however, no overarching legislation for the protection of personal data in Singapore.[88]

"five basic principles" from the bill and provided exemption clauses for the press. Broadcasters, newspapers, news agencies, and other reporting organs, including individuals and writers, are exempted from the application of the clauses.

[86] Crompton, Malcom, Chapter 3: Overview of Asian Privacy Law Lesson Learned and Possible Way Forward, Privacy Symposium Sponsored by the Institute of Law China Academy of Social Science, Role of Information Service Providers, 2006.

[87] *Supra* note 86.

[88] Infocom Development Authority of Singapore, Policies and Regulation, http://www.ida.gov.sg/Policies%20and%20Regulation/20060627155443.aspx

However, there is a highlight on privacy and data protection in Singapore. *First,* after public consultations in 2002, the National Internet Advisory Committee (NIAC) issued the Model Data Protection Code for the Private Sector (Model Code), which is modeled on internationally recognized standards.[89] The Model Code is a generic code that is available for voluntary adoption by the entire private sector and sets out the minimum requirements for the protection of personal data based on the principles of EOCD Guidelines.[90] *Second*, protection for banking secrecy was established in the Banking Act, which prohibits any bank in Singapore or any of its officers from disclosing any customer information to any other person unless expressly permitted to do so in the Banking Act.[91] It is a sufficient protection for the costumer because the banks have an obligation to keep the confidentiality of their customer. Banks are expected to employ a level of encryption appropriate to the type and extent of risk present in its networks, systems, and operations.[92] *Third* is the Marketing and spam control. Singapore established the Spam Control Act in 2006. This Act regulates the sending of electronic messages. First, the Act prohibits the sending of messages to electronic addresses harvested or "guessed" through automation. Secondly, unsolicited electronic commercial messages sent in bulk will have to comply with several requirements.[93] Some of this highlights the concerns of other countries over the state of protection in Singapore and the development of privacy and data protection legislation in Asia.

Economic matters play a big role in the cooperation between Indonesia and Singapore. Both countries have agreed to strengthen cooperation and it is of great importance to include privacy and data protection as one of the important tools in this respect because economic cooperation also requires exploring the possibility of having privacy laws. The options for encouraging or enforcing privacy principles that are not based on law enforced by a public

---

[89] Bryan, Tan, , Data Protection Guide: Singapore, Keystone Law Corporation, 2010, http://www.keystonelawcorp.com/downloads/SingaporeKeystoneLaw20103C.pdf

[90] See the principles of OECD guidelines on the protection of privacy and trans-border flow of personal data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[91] See Banking Act Section 47.

[92] Supra note 89.

[93] Supra note 89.

authority are also being explored in a number of economies. The Singapore government, for example, has sponsored the establishment of an e-Merchant Trustmark regime called TrustSg (www.trustsg.com.sg), which includes a commitment to respect privacy and has encouraged businesses to subscribe to it.[94] The government of Singapore needs to feel similar constraints when they engage in cooperation with Indonesia,[95] which will be more easily achieved if Indonesian agencies and companies have adequate protection.

2.5.5. South Korea

South Korea is a member of the Organization for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. South Korea has adopted a data protection regime similar to that of the United States and Japan, with one act covering the public sector and sectoral legislation for the private sector.[96] The statute in the former category is the 1994 Act on the Protection of Personal Information Maintained by Public Agencies, which is generally applicable to the automated processing of personal data in the public sector, but not to manual records. This statute has a provision recommending that private entities respect the data protection principles in the statute, but it has no appropriate administrative or enforcement mechanism to that effect. As early as 1997, legislators and academics proposed a general privacy law for the private sector. However, the government proposed and later adopted a narrower alternative that targeted only the information and telecommunications industries.

The Act on Promotion of Information and Communications Network Utilization and Data Protection, modeled after the German Online Service Data Protection Act of 1997,[97] came into

[94] Supra note 89

[95] There are a number of ways that regulators could enforce privacy laws across borders. These include being able to enforce their own laws via investigations they carry out themselves in respect of violations in other jurisdictions and/or the ability to cooperate with investigators in other jurisdictions, for example through the sharing of information.

[96] Chung, C. and Shin, I., On-Line Data Protection and Cyberlaws in Korea, *27 Korean J. of Int'l and Comp. L. 21*, 1999.

[97] The Act adopts common "fair information principles" and rules for the collection, use, and disclosure of personal data by "providers of information and communications services," such as common carriers, Internet service providers and other intermediaries, particularly content providers. The Act also covers specific off-line service

effect in 2000.[98] In November 2006, members of the Futures Forum for Korea in the Korean National Assembly attempted to arrive at an agreement on a proposal for a comprehensive privacy law.

South Korea has one of the world's highest concentrations of mobile-phone users,[99] while Indonesia has the largest community in Facebook.[100] Similarly, in Korea there is rising concern about possible privacy abuses, for example, of individuals having their photo taken without prior consent. As regards Facebook, individuals face possible privacy abuse by the ability of others to put one's information on the website without prior consent. In November 2003, South Korea introduced regulations to protect against the surreptitious taking of photos in public areas such as locker rooms and swimming pools. Starting in 2004, mobile phone manufacturers are required to design camera-enabled mobile phones to make "camera shutter" sounds, of at least 64 decibels, when a picture is taken. *The Korea Times* reported that the government was drafting a new bill to prohibit individuals from taking photographs of others using camera phones without prior consent. This can be one of the examples that Indonesia can use as a comparative model. Indonesia can learn how the privacy and data protection is enacted in this country but Indonesia still needs to adjust the protection for the

---

providers such as travel agencies, airlines, hotels, and educational institutes. The Act requires that "data users" seek consent from "data subjects" for the collection, use, and disclosure of data to a third party "beyond the notification as prescribed in the Act or the limit specified in a standardized contract for the utilization of the information and communication services." The Act allows the data subject to withdraw consent for the collection, use, and disclosure of data at any time and requires the data user to comply unless the preservation of such personal information is required by another Act. Further, every data subject has a right to access and correct his or her personal information. The Act prohibits one from sending unsolicited commercial e-mail contrary to an addressee's explicit refusal of such mails. All unsolicited commercial e-mails must contain the word "Advertisement" in the subject line of each and every message and must contain opt-out instructions and contact information for the sender. Additionally, several direct marketers established the Association for the Improvement of the E-Mail Environment in early 2002 to help cope with the increasing number of unsolicited commercial e-mails problem in Korea.

[98] Privacy international overview of the Republic of South Korea, 2007, https://www.privacyinternational.org/article/phr2006-republic-south-korea

[99] *JoongAng Daily*, Phone Camera Makers Are Told to Use 'Click' to Protect Privacy, November 12, 2003, https://www.privacyinternational.org/article/phr2006-republic-south-korea#[77]

[100] http://tekno.kompas.com/read/2010/06/01/22190833/Indonesia.Pengguna.Facebook.Terbesar.di.Asia-12

condition of Indonesia. South Korea is the one of the leading countries in Asia and has a big chance to gather joint cooperation with Indonesia in the economic sphere.

2.6. What do the international frameworks mean for Indonesia?

International instrument have an importance role to Indonesia. Indonesia as a part of international community, use international instrument as a one source of law in regulating relation or cooperation between the countries. Trough international agreement, each country organize various activities or resolve various problem that occur between the countries. No single country that doesn't have agreement with other countries because it is importance to have political or economic position in the community. One of the effort to encourage the trade, investment and market access are conducting an ambitious attempt to enact privacy and personal data protection.

European Union is one of the leading countries with strong privacy and personal data protection are restrict any transfer data of their citizen to the country with non equal protection. So, if Indonesia want to have good cooperation with European countries, Indonesia have to prepare adequate protection. It will be the good reason for Indonesia to build strong protection in a future. And also with U.S, they have strong protection to their citizen, so if Indonesia want to have a strong cooperation with U.S, it is better for Indonesia to have privacy and data protection in Indonesia legal system.

Related with privacy and data protection, Indonesia doesn't take a part in any privacy and data protection international instrument. The Asian countries like Japan, Singapore, South Korea and China are the leading country in Privacy and personal data protection with good relation with Indonesia. As the emerging power from Asia, Indonesia need to consider their role in protecting their citizen.

Chapter 3 – Building the Privacy and Data Protection Concept: Indonesia's Legal Framework

In this chapter, we discuss the regulatory frameworks of privacy and data protection in Indonesia, describing the legislation enacted in relation with privacy and data protection. Basically, in this chapter we will further elaborate and provide more evidence why those regulatory frameworks are lacking in adequacy.

3.1. Privacy and data protection national instrument overview, the nature of privacy and data protection in Indonesia

The Indonesian legal system is based on civil law mixed with customary law and religious law.[101] In this legal system, the enforceable right to privacy and personal data protection does not exist. The initiative to give protection to privacy and personal data comes from the international demand of partners of Indonesia in economic cooperation. Indonesia has a strategic position on international trade,[102] including electronic commerce. In order to

[101] There are three kinds of laws enacted regarding citizens of Indonesia. Law, Customary Law, for example, the citizens of Indonesia still use their custom to live in their society, Civil Law, with an influence from Dutch colonialization, for example, Commercial law, which is based on Commercial Code 1847 (Kitab Undang-Undang Hukum Dagang or Wetboek van Koophandel), and Islamic law, for example, the Islamic marriage institution for Muslims. Based on Sudargo Gautama and Robert N. Hoick (1983): From the earliest days of Dutch colonization, inhabitants of the Indonesian archipelago have been divided for legal purposes into various "population groups" (golongan rakyat, bevolkingsgroupen), based primarily on racial origin. Although other group distinctions were also made, for example, between Dutch subjects and foreigners, between residents and non-residents, between Dutchmen and several categories of non-Dutchmen – no distinction was more important or more pervasive than the division into population groups. What kinds of contracts one might enter into and in what form, whether one could own land and where, from whom one could inherit wealth and in what ways – matters such as these depended almost entirely on which population group one belonged to. This was so because distinct rules of contract law, of property law, of inheritance law existed for each group. Each group, that is to say, had what amounted to its own legal system – separate regulations administered by separate government officials and enforced in separate courts of law. Although transactions between members of regulations were sometimes made, the basic division was never overcome. Distinct, and very different, systems of law have thrived side by side in Indonesia for centuries. See Ali, Ahmad, *Law and Development in Changing Indonesia*, IDE Asian Law Series No. 8 Law and Development in Asian Countries, Institute of Developing Economies (IDE), JETRO, 2001.

[102] Indonesia as a big population is a potential market, with 237,641,326 citizens (2010) and national import 2011 is about US$14.89 Billion, http://www.bps.go.id/

accommodate cooperation, Indonesia has to provide adequate regulation to enhance protection in accordance with international norms.

Nowadays, because of the international instruments that Indonesia has ratified and signed, Indonesia has the legal basis to make the law applicable at the national level.

Indonesia signed the OECD guidelines in 2004, and followed the guidelines to enforce the applicability of privacy and data protection regulation. Also, as a member of APEC, Indonesia follow the APEC Privacy Framework 2004, which clearly mentions in the foreword, "*the potential of electronic commerce cannot be realized without government and business co-operation to develop and implement technologies and policies which … address issues including privacy.*" This membership stimulated national legislation to recognize the privacy protection to balance and promote effective information in order to promote economic cooperation especially in electronic commerce between the members.

The EU is a very attractive market for Indonesia because it is the biggest market for non -oil and gas exports and also European investors have proven to be among the most stable and reliable partners of Indonesia.[103] So, it is important to Indonesia to solve the challenge and obstacles that they are facing when doing cross-border business. In other words, it is important to Indonesia to fill the requirement on EU level standards on privacy and data protection.

Not only for economic reasons, the privacy policy has to be introduced as part of the law concerning human rights. Privacy is a part of human rights and personal data protection is one way to respect this right. In Indonesia, there is an anxiety about protection for privacy and data protection because there is still no clear and ambiguous legislation. Therefore, privacy and personal data protection issues have become an urgent agenda. Many countries have established laws due to these issues, but no Indonesian law has been established with strong, specific regulations. The increase and the development of science and technology, the globalization, and the power of the media have urgently strengthened the need for privacy and personal data protection.

The barriers to privacy and data protection regulation come from Indonesia's own history. As an Asian country, Indonesia finds it very difficult to define and regulate privacy. Most

[103] Official website of European Union, Trade, http://eeas.europa.eu/delegations/indonesia/eu_indonesia/trade_relation/index_en.htm

Asian countries have no idea about privacy.[104] Privacy has not been seen as a "serious" issue in Asia, including Indonesia. Most Asians traditionally lived in communal societies, which did not pay much attention to privacy.[105] The term privacy as a human right comes from the West[106] and is becoming important in the era of information and communication technology (ICT). Hence, the legal basis for privacy and data protection in Indonesia can be derived from a variety of sources.

3.1.1 Privacy and data protection in the constitution

The Indonesian constitution, known as UUD 1945, does not explicitly mention privacy and personal data protection, but UUD 1945 strongly recommends protecting human rights. The preamble of the Indonesian constitution states that human rights are the ideals of the Indonesian nation as well as the national goal. The national goal is to protect the people of Indonesia and the entire country and promote the general welfare and the intellectual life of the nation and implement a world order based on freedom, social justice, and world peace.

Hereinafter, the concept of privacy and data protection can be found in amendment UUD 1945 articles 28F and 28G for data protection.[107] These articles do not directly mention

---

[104] Makoto Nakada's detailed presentation examined the assumption that Asian cultures lack the recognition of privacy as something intrinsically good. See Malcouronne, Peter, Report on the First Regional Conference for the Asia and Pacific Region on the Ethical Dimensions of the Information Society, Hanoi, 2008, page 13, portal.unesco.org/...**Conference**.../Final_Report_Hanoi_**Conference**.doc

[105] In this report, Soraj Hongladarom contended privacy has not been seen as a serious issue in Asia (or in Thailand, either). Most Asian people lived/live within communal societies – indeed, many languages in Asia lack a specific word for the term. See Malcouronne, Peter, Report on the First Regional Conference for the Asia and Pacific Region on the Ethical Dimensions of the Information Society, Hanoi, 2008, page 13, portal.unesco.org/...**Conference**.../Final_Report_Hanoi_**Conference**.doc

[106] Electronic Privacy Information Center (EPIC) and Privacy International (PI): "Privacy & Human Rights 2006" (P&HR 2006), Overview of Privacy, https://www.privacyinternational.org/article.shtml?

[107] Article 28F UUD 1945 mentions the following: "*Every person shall have the right to communicate and to obtain information for the purpose of the development of his/herself and social environment, and shall have the right to seek, obtain, possess, store, process, and convey information by employing all available types of channels."* Article 28G states the following*: "(1) Every person shall have the right to protection of his/herself, 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. (2) Every person shall have the right to be free from torture or inhumane and degrading treatment, and shall have the right to obtain political asylum from another country."* See http://www.wipo.int/wipolex/en/text.jsp?file_id=200129

privacy and data protection but can be considered an umbrella law for the specific regulation. However, this article has not been applied directly in any regulation in Indonesia. This is usually mentioned explicitly in the statute. But there is no doubt that these articles are concerned with human dignity as a human right.[108]

3.1.2. Privacy and data protection in human rights law

Privacy is a fundamental right. In many countries, privacy has become a different part of human rights, but they are still connected. In Indonesia, the Constitution is a first legal source, but detailed regulations will be set out in a specific law.[109] The Constitution is an umbrella for this specific regulation.[110] Human rights legislation in Indonesia was formally established in 1999 with Law Number 39 Year 1999. In Law no. 39/1999, several articles give some protection that refers to privacy. This legislation provides legal standards with regard to human rights issues.[111] These provide protection, such as: rights to several freedoms (e.g., freedom of speech, conscience, religion, assembly, and association); equality rights (equality before the law and equal protection of the law, protection against discrimination on the grounds of sex, race, color, religion, ethnic, or social origin, etc.). Other rights are political rights (right to vote, equal access to public service, freedom to form a political party, right to petition, etc.); rights of economic life (right to own property, freedom of movement, right to work and free choice of

[108] Literally, this article contains protection for the right to protect him/herself, his/her family, honor, dignity and property under his/her control; the right to feel secure and be protected from the threat of fear to do, or not to do something; the right to be free from torture or treatments degrading of human dignity; this right mentioned in article 28 refers to human rights protection. See Harjono, The Indonesia Constitutional Court, http://www.ccourt.go.kr/home/history/world/pdf/05.pdf

[109] Based on article 7 (1) Indonesia Constitution 1945, this is the legal basis of all legislation in Indonesia. See Law Number 10 year 2004 on the Establishment of Regulation.

[110] The Constitution of Indonesia has clearly provided provisions of human rights protection under Chapter XA as the fundamental rights of citizens. The legal system of Indonesia is based on the basic premise of the supremacy of the Constitution whereby the Constitution is given the highest authority. Consequently, the protection of human rights becomes imperative as a prerequisite for development.

[111] See article 1 (1) Law Number 39 year 1999: *Human rights mean a set of rights bestowed by God Almighty in the essence and being of humans as creations of God which must be respected, held in the highest esteem and protected by the state, law, Government, and all people in order to protect human dignity and worth*.

employment, freedom of provided services); collective rights (the right of people to self-determination, protection of minorities and indigenous peoples, rights to development, etc.); procedural rights (especially for administration of criminal justice); and specific rights for children, the elderly, the sick, the disabled, aliens, and asylum seekers as well as for other vulnerable groups.[112]

Referring to privacy and data protection, this human right law provides Article 12, which states:

> *Everyone has the right to protection of his self-development, to obtain an education, to educate himself, and to improve the quality of his life to become responsible, content, and prosperous people, in accordance with his human rights.*

In this article, Indonesia trying to protect human rights, and there is no special mention of protection regarding privacy and data protection. Protection while getting information and communicating describes the closest relationship between human rights and privacy and data protection in general.

Article 14[113] states:

> *(1) Everyone has the right to communicate and obtain information they need to develop themselves as individuals and to develop their social environment.*
> *(2) Everyone has the right to seek, obtain, own, store, process, and impart information using all available facilities.*

In Article 21, the human rights law, the regulator tries to enact the principle of "notice" of the 2004 APAEC privacy framework. Article 21[114] states:

> *Everyone has the right to integrity of the individual, both spiritual and physical, and as such shall not become the object of any research without his approval.*

Article 29[115] states:

---

[112] Faiz, Pan Mohamad, Human Rights Protection and Constitutional Review: A Basic Foundation of Sustainable Development in Indonesia, paper presented on International Students' Scientific Meeting 2008, The Institute for Science and Technology Studies (ISTECS) and Indonesian Student Association of Nederlands, Delft University of Technology, Delft, The Netherlands on 13-15 May 2008.

[113] Translation by http://hrli.alrc.net/mainfile.php/indonleg/133/

[114] Translation by http://hrli.alrc.net/mainfile.php/indonleg/133/

[115] Translation by http://hrli.alrc.net/mainfile.php/indonleg/133/

(1) Everyone has the right to protection of the individual, his family, opinion, honor, dignity, and rights. (2) Everyone has the right to recognition everywhere as a person before the law.

This article can be defined as the realization of privacy rights in Indonesia, but there is still a loophole here. For example, in the Ahmadiyya[116] case: the controversy is related to the right to individual and spiritual integrity.[117] The government faces two contradictions in policing this case because of reasons concerning human rights. Civilians have the right to practice their beliefs without intrusion but the other Muslim community[118] asked the government to dissolve Ahmadiyya because this branch has different beliefs. The Muslim community in Indonesia thinks that Ahmadiyya is ruining Islamic beliefs. Human rights organizations have tried to stop the dissolution of Ahmadiyya because doing so would violate the group's human rights, but the rest of the Muslim community still hopes the government will dissolve Ahmadiyya. This controversy remains a big issue in Indonesia in accordance with human rights, especially the right to spiritual privacy.

3.1.3. Privacy and data protection in law of criminal procedure Number 8 Year 1981

Article 47 Law Number 8 year 1981 authorizes the police to open personal mail delivered through the post office and other sources of telecommunication, with a special permit from the head of the national court, while Article 49 gives details that an investigator is required to keep

[116] Ahmadiyya is a branch of the Islamic religious movement founded in India and is considered controversial by other Muslim branches because of the way of their thinking, praying, and beliefs, which are different from other Muslim communities in common.

[117] As the Ahmadiyya Movement, the organization has been known in Indonesia since 1924. In 1980, the Indonesian Ulema Council (MUI) for the first time decided to ban Ahmadiyah. MUI declared Ahmadiyah is a forbidden and misleading group. See Suryawan, M.A, *Bukan Sekedar Hitam Putih*, Azzahra Publishing Ed I, 2006.

[118] See MUI Won't Back Down on Ahmadiyya Fatwa, http://www.thejakartaglobe.com/home/mui-wont-back-down-on-ahmadiyah-fatwa/423342. See MUI urges government to ban Ahmadiyya http://www.thejakartapost.com/news/2011/03/08/mui-urges-government-ban-ahmadiyah.html. See In the case of interception of a suspect's communications by the anti-corruption commission, Indonesia faces dualism core, http://www.antaranews.com/en/news/68319/muhammadiyah-avoids-movement-backing-ahmadiyah-dissolution

the contents of the mail secret, under the power bestowed upon him.[119] Article 47 Law Number 8 year 1981[120] states:

1) *Investigators are entitled to open, inspect and seize any letter through the post office, communication or transportation service office if they suspect with strong reason related to a crime under review, with special permission from the judge of the district court.*
2) *For the purposes of the investigation, the investigator has to submit a letter of request to the head of the post or telecommunication office, head office, or corporation in the communication area, and the investigator will receive a receipt letter if they receive approval to investigate the letter.*
3) *As referred to in paragraph (1) and paragraph (2) of this article, the investigation can be done at all levels of the court.*

This article represents privacy protection for correspondence, especially correspondence by mail. Under this law, an investigator can open any mail to the suspect, but with regard to respecting human rights, the investigator cannot open any mail without a judge's permission. If the investigator does not have permission but still attempts to open mail, then the suspect can sue the investigator.

3.1.4. Privacy and data protection in the telecommunication law

Basically, this regulation describes the government's protection of civil rights in the communication area. However, protection with regard to privacy and human rights can be found in articles 38-42 Law Number 36 year 1999 on Telecommunications.[121] In this telecommunications law, privacy, and data protection are specifically mentioned in Article 38:[122]

> *Every person is prohibited from taking actions, which may cause physical and electromagnetic disturbances to telecommunications operations.*

---

[119] See Law Number 8 Year 1981 on: kepustakaan-presiden.pnri.go.id/uploaded_files/.../**UU_8_1981**.pdf. See also legislasi.mahkamahagung.go.id/.../**UU**/**1981**/UU%20NO%208%20TH%20**1981**.pdf

[120] No official translation. Free translation by the author.

[121] See Law Number 36 Year 1999, http://www.postel.go.id/content/EN/regulasi/telecommunication/uu/law36-1999.pdf

[122] Official translation by the Ministry of Communication and Information Technology, http://www.postel.go.id/content/EN/regulasi/telecommunication/uu/law36-1999.pdf

Article 40 states:

All persons are prohibited from eavesdropping in any form whatsoever on information channeled through telecommunications networks.

Article 42 states:

(1) The telecommunications services operator is obligated to keep confidential the information transmitted and/or received by a telecommunications services subscriber through the telecommunications networks and/or telecommunications services that it is providing.

(2) For the purposes of criminal prosecution, the telecommunications services operator may record the information transmitted and/or received by the telecommunication services operator and may provide the information required on the basis of:

a. a written request from the Attorney General and/or the Chief of Police of the Republic of Indonesia for certain criminal offenses;

b. the request of an investigator for certain criminal offenses in accordance with prevailing laws.

(3) Provisions concerning the procedures for requests and submission of the recorded information referred to in paragraph (2) shall be regulated by Government Regulation.

The government is trying to enact regulations regarding telecommunications to ensure that the right and the obligation of the parties can be held correctly. The telecommunications area is developing very fast, and the government needs to regulate this area because it is very important. The regulations protect the parties from any misuse of telecommunications. However, these regulations allow the government to intercept or tap any communications with the suspect with government regulation.[123] This article means that civilians' right to privacy is decreased by the government because the government regulation has a lower standard than the law. An adequate level of protection of privacy rights is needed to ensure the enforcement of this right.

In the case of interception of a suspect's communications by the anti-corruption commission, Indonesia faces dualism highlight. The interception of a suspect's communications is considered to be an example of problem solving due to an investigation by the anti-

[123] Article 31 of the telecommunication law mentions that the provision and interception procedure as intended in this article should be regulated by the government.

corruption organization, but human rights organizations resist this interception because Indonesia still does not have adequate regulations for intercepting communications. The inadequate regulations regarding interception will increase the new problem of human rights because misuse of the interception regulation is likely to occur.

This article provides protection for consumers' personal telecommunications. However, in early 2011, the Telecommunication Regulation of Indonesia Bureau and the Indonesian Parliament discussed the dissemination and disclosure of consumers' telecommunication data.[124] The authorities found an advertisement in a newspaper stating that PT Bumi Kharisma Lininusa could provide personal data about 25 million consumers throughout Indonesia.[125] If PT Bumi Kharisma Lininusa provides data without consumers consent, then the company is obviously violating Article 42 of this law.

3.1.5. Privacy and data protection of medical reports

Privacy and data protection are also given to citizens under Health Law Number 36 year 2009 Article 57:

> *Everyone is entitled to personal confidential health conditions that have been advanced to health care providers.*[126]

And article 47 (2) Law Number 29 year 2004 concerning medical Practices states:

> *Medical reports referred to paragraph (1)*[127] *must be stored and maintained confidential by the physician or dentist and head of service facilities health.*[128]

---

[124] See official website of Indonesia Parliament, http://www.dpr.go.id/complorgans/commission/commission1/risalah/K1_risalah_MP_III_TS_10-11_Risalah_RDP&RDPU_Kom_I_dg_BRTI,_ID-SIRTII,_Operator_Telekomunikasi.pdf

[125] See official website of Ministry of Communication and Information Technology, http://www.postel.go.id/update/id/baca_info.asp?id_info=1636

[126] No official translation. See http://depkes.go.id/downloads/UU_No._36_Th_2009_ttg_Kesehatan.pdf

[127] Article 47 (1) mentions: Medical record documents referred to Article 46 are owned by physicians, dentists, or health care facilities, while the contents medical records belong to patients. See the official website of www.depkes go.id and http://www.ropeg-depkes.or.id/documents/uu_29_2004.pdf

[128] No official translation. See http://www.ropeg-depkes.or.id/documents/uu_29_2004.pdf

In the Indonesian legal system, protection is given by the government to citizens to protect their health privacy history from disclosure by health care providers. An individual's health history is part of human dignity and cannot be disclosed without the patient's consent. In other words, health care providers are restricted from disclosing any information about the patient to a third party.

3.1.6. Privacy and data protection on the Information and Electronic Transaction Law

Privacy and personal data protection can be marked as a progress of concerns regarding technology and communication development in Indonesia. The specific term of privacy and data protection can be found in Article 26 Law Number 11 year 2008 concerning Information and Electronic Transaction:[129]

> *(1) Unless provided otherwise by Laws and Regulations, use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned.*
> *(2) Any Person whose rights are infringed as intended by section (1) may lodge a claim for damages incurred under this Law.*

Legal protection of privacy and personal data provided by article 26 is very common, though it does not provide wide enough coverage. This article only mentions the right to enjoy personal life free from any invasion by others, the right to have communication with others without any surveillance, and the right to access the information about the personal life of and data on individuals. But this article gives a chance to the aggrieved person for the use of personal data of the people concerned.[130]

In general, own privacy policies are used by the online trading websites such as eBay and Amazon. They already provide protection for the privacy and personal data of their users and keep it secure and safe from any misuse. They provide adequate information about what personal data is collected, and guarantee the confidentiality of sensitive data like credit card

[129] Ali Budihardjo, Nugroho, Reksodiputro translation. http://www.pranata.lipi.go.id/wpcontent/uploads/2009/01/UUTIE.pdf

[130] See Article 26 Section 2 Law Number 11 year 2008.

numbers. But, in fact, many website in Indonesia do not provide any protection for personal data, and do not include the privacy policies to websites that collect personal data.

3.1.7. Privacy and data protection disclosing certain consumer information to banks

Protection of banking consumers is provided by Law Number 10 Year 1998 on Banking and Government Regulation Number 7/6/PBI/2005 concerning the Transparency of Information to Banking Product and Consumer personal Data Use. Protection is specifically mentioned in:

Article 40 (1) Law number 10 year 1998,[131] which states that:

Banks are required to keep confidential all information about customers, except in the case referred to article 41, 42, 43, 44 and 44A.

This article will apply to any banking case except the case referred in article 41, 42, 43, 44 and 44A that mention about the possibilities of Bank to disclose consumer information in a special condition.

Article 9 Government Regulation number 7/^/PBI/2005[132] states that:

1) *Banks are required to request written approval from the customer if the Bank discloses and distributes any of the consumer's personal data to other parties for commercial purposes, unless it is stipulated by laws and other applicable laws.*
2) *In the written approval request referred in Paragraph (1), the Bank shall explain the purpose and consequences of the provision and dissemination of personal consumer data to the other parties.*

The implementation of This article in fact is very difficult to apply. Consumer protection and consumers' rights as mentioned above are very difficult to enforce. In Indonesia, there are many problems in this area. Credit card holders or consumer databases are bought freely. The banks argue that they cannot do anything because the seller and buyer of consumer databases

[131] No official translation. Free translation by the author. See http://www.bi.go.id/NR/rdonlyres/C7402D01-A030-454A-BC75-9858774DF852/13313/uu_bi_1099.pdf

[132] No official translation. Free translation by the author. See http://www.bi.go.id/NR/rdonlyres/2C5737BD-5BE2-4B69-BD81-2F1CBD9C042B/11844/pbi7605.pdf

are not bank employees and banks are not legally required to avoid these transactions.[133] This is a big problem in privacy and data protection; the government has to solve this problem and ensure that citizens' rights to privacy are protected properly.

3.2. Privacy and Personal Data Protection, the national and the international regime

Based on the analysis of the legislation, the statutes regarding privacy and data protection in Indonesia are too general. The privacy policy only puts in some provisions in the statutory with a minor explanation about this, such as a privacy law that exists in the Banking Law, Telecommunication Law, or Human Rights Law. This model ensures that the privacy legislation is less comprehensive and lacking in implementation. In addition, the privacy and personal data protection enforcement still relies on the institutions that recognize these policies as an issue, such as privacy issues on the Banking Law; if there's a case, the Bank and Bank Indonesia as the highest levels in banking will assume responsibility. The privacy issues that arise in a human rights area will be addressed by the National Commission on Human Rights. Unfortunately, this model ensures the privacy and personal data protection enforcement will lack in consistency.

This can be a problem if Indonesia wants to have a close relation with a country with a high level of privacy and personal data protection, in particular with EU member states.[134] The Directive is intended to protect the citizen not only in the member states but also in other jurisdictions. Article 25 of the EU Directive 1995 requires that if personal information is going to

[133] BI Tak Bisa Berbuat Banyak Kasus Kebocoran Data Nasabah Bank, March 30 2011, ttp://www.vibiznews.com/news/banking_insurance/2011/03/30/bi-tak-bisa-berbuat-banyak-kasus-penjualan-data-nasabah/10,http://besteasyseo.com/sms-spam-kartu-kredit-jual-beli-data-nasabah-kasus-kebocoran-data-bi-bank-indonesia/1568

[134] "Under UE 1995, EU member states must be restricted in access to data and limit the purposes for its use, as data may only be used for the purpose for which it is collected, minimize the period of retention, ensure that individuals have access to the data that is held on them, ensure that individuals have legal recourse, and ensure that the data is protected adequately. See Directive 95/46/EC of the European parliament and of the Council on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data." In the *Official Journal of the European Communities*, 281/31, 1995; Preamble paragraph 3.

be sent to other jurisdictions that are not covered by EU laws, these other jurisdictions must have adequate privacy laws.[135]

To establish an agreement with the Indonesian government, to allow this transfer of data, an adequacy assessment is generally required. According to the Directive, the adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures that are complied with in that country.[136]

Indonesia and privacy and personal data protection international overview:

Issue	**International Instrument**	**Generally protection by Indonesia**
Preventing harm	OECD, APEC Privacy Framework, Article 6 Directive 95/46/EC	No definite legislation
Notice	OECD, APEC Privacy Framework, Article 18 Directive 95/46/EC	Article 21 Human Rights Law, Article, Government Regulation Number 7/6/PBI/2005 concerning the Transparency of Information to Banking Product and Consumer personal Data Use, 26 Law Number 11 year 2008 concerning Information and Electronic Transaction
Collection limitation	OECD, APEC Privacy Framework, Article 6 Directive 95/46/EC	No definite regulation
Uses of personal information	OECD, APEC Privacy Framework, Article 6 Directive 95/46/EC	Article 49 Law Number 8 year 1981

[135] "The transfer of personal data to a third country that does not ensure an adequate level of protection must be prohibited." See "Directive 95/46/EC of the European parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data." In the *Official Journal of the European Communities*, 281/31, 1995. Preamble paragraphs 56-57.

[136] See Article 25 Directive 95/46/EC of the European parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data. In the *Official Journal of the European Communities*, 281/31, 1995.

choices	APEC privacy Framework, Section V Article 12 Directive 95/E46/EC	No definite regulation
Integrity and personal information	OECD, APEC Privacy Framework, Article 6 Directive 95/46/EC,	No definite regulation
Purposes specification	OECD, APEC Privacy Framework, Article 6 Directive 95/46/EC	Article 49 Law Number 8 Year 1981
Security safeguard	OECD, APEC Privacy Framework, Article 6 Directive 95/46/EC	Article 42 Law Number 36 year 1999 on Telecommunication, Health Law Number 36 year 2009 Article 57, 26 Law Number 11 year 2008 concerning Information and Electronic Transaction, article 47 law number 29 year 2004 on medical practice, article 40 (1) law number 10 year 1998
Access and Correction	OECD, APEC Privacy Framework, Section V article 12 Directive 95/E46/EC	Article 28 F Indonesia Constitution
Accountability	OECD, APEC Privacy Framework, Article 6 Directive 95/46/EC	Article 49 Law Number 8 Year 1981,
openness	OECD, APEC Privacy Framework, Directive Article 6 Directive 95/46/EC	No definite regulation
Individual participation	OECD, APEC Privacy Framework, Article 15 Directive 95/46/EC	No definite regulation

The problem for Indonesia is that under the 1995 EU Data Protection Directive, EU member states require that there must be a requirement such as restricted access to data, and the purposes for its use be limited, as data may only be used for the purpose it is collected, minimize the period of retention, ensure that individuals have access to the data that are held on them, ensure that individuals have legal recourse, and ensure that the data are protected adequately.[137] Based on the table mentioned above, there are some principles in international instruments that cannot be found in Indonesian legislation.

[137] The first report Towards an International Infrastructure for Surveillance of Movement, Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection, Privacy International in co-operation with European Digital Rights Initiative, the Foundation for Information Policy Research, and Statewatch, 2004

In relation to the notion of adequacy, the European Commission's expert group established grounds on the Article 29 Working Party.[138]

1. Content Principles:
   - Purpose limitations: where data can only be collected and processed for a limited number of purposes;
   - data quality and proportionality: the data is accurate and its integrity is maintained;
   - transparent: individuals are provided with information regarding the processing;
   - security: data is secure and protected from arbitrary access;
   - rights of access, rectification, and opposition: individuals may gain access to the information held on them, challenge and rectify errors, and challenge its collection and block the onwards transfers to other third countries.
2. Particular attention is required to:
   - Sensitive data: additional safeguards, such as explicit consent, are required for such data, defined by Article 8, "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."
   - Automated Individual decision-making: Where the purpose of data transfer is the taking of an automated decision, individuals should have the right to know the logic involved in this decision, and other measures should be taken.
3. Procedural/Enforcement Mechanisms:
   - Good level of compliance: high degree of awareness among data controllers of data protection rights and obligations
   - Provide support and help to individual data subjects in their exercise of rights
   - Appropriate redress mechanisms for individuals

[138] Article 29, Working Party. First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy. Brussels: European Commission, 1997, XV D/5020/97-ENfinal WP4. 26 June. https://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf

Based on the requirements mentioned above, the Indonesian legal regime would certainly not protect the personal data of EU citizens adequately. The protections given by the Indonesian regulations are too general and do not cover all aspects of privacy as mentioned in some international instruments. Thus, as a result, this information cannot be transferred out of the EU to Indonesia and there will a problem with this condition.

CHAPTER 4 – How the Legislation protects privacy and personal data

4.1. The function of privacy and personal data protection

We have discussed the Indonesian legal framework of privacy and data protection in Chapter 3. From those discussions, there is evidence that privacy and data protection is covered in some legislation in Indonesia and therefore it can be seen that there is no single regime of privacy and data protection that is enacted to protect the citizen. From this discussion in Chapter 3, we can go further to the analysis with this lack of adequacy in protection on privacy and data protection, how Indonesian legislation protects the citizens, and this chapter also provides examples for a possible framework in privacy and data protection in Indonesia.

The partial policies for privacy and data protection given by Indonesian legislation provide no single and unified policy. This means that various legislations can be used to protect privacy and disclosure of data. Legal protection of privacy and data protection can be derived from a variety of sources. However, in many cases, this legislation is not enough to protect citizens from the misuse of data and protection. There are just too many loopholes in policing privacy and data protection regulations in Indonesia.

Recently, privacy and data protection is not a big issue in the public sphere. This is greatly different from European or the U.S., the various public entities of which believe that privacy and personal data are important parts of human rights. Indonesia is a communal society and concerned with issues of mutual interest between the members. These characteristics indicate that the public sphere will defeat an individual sphere. In Indonesia, there is no absolute ownership. Personal property or belongings are instruments for the pursuit of social values.[139] Properties are viewed a bundle of rights and analyzed for their effect as incentives. Property rights are efficient when they create incentives to maximize the nation's wealth.[140] As a country with communal characteristics, sometimes Indonesian authorities use public sentiment as a basis to create new legislation. The public sentiment of society is usually influenced by religion or cultural factors. The urgency to create new regulation always comes

[139] Makarim, Edmon, *Tanggung Jawab Hukum Penyelenggara system Electronic*, 1st edition, Jakarta, Rajawali Pers, 2010, page 278.

[140] Richard A. Posner, *Economic Analysis of Law*, 5th edition, New York, Aspen Publisher, 1998, page 12.

from public value. For example, Indonesia promulgated an anti-pornography law because it is appropriate with the country's religion. The community assumes that pornography violates decency and restricts it based on the values of their religion.

The conception of public interest may seem to be inappropriate in regards to matters of economic justification or sometimes it is against the concept of international human rights. In this area, based on the wide cultural and religious standards of the citizenry, privacy and personal data are not viewed as an important interest of society because the citizens are not familiar with the concept of privacy.

To address the function of privacy and personal data protection, we can look back into the theories from Alan Westin, who asserts that privacy is a claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[141] The function of privacy is mentioned as a personal economy, emotional release, self-evaluation, and limited and protected communication.[142] We can look to how these considerations are implemented into legislation to assess how the Indonesian legal system protects individual privacy and personal data.

4.2 The Influence of International instruments of privacy and protection in Indonesia

Indonesia has recognized international instruments as a source of law. International agreements can be the source of law as established by Article 11 of the Indonesian 145 Constitution, Law Number 37 Year 1999 concerning Foreign Relations and Law No. 24 of 2000 concerning International Treaties. Under Indonesian law, every treaty or agreement with other states or international entities shall be guided by national interest based on the principles of equality and mutual benefit and taking into account the prevailing national and international law.[143] Here, I will refer back to the role of international instruments in Indonesia.

---

[141] Alan F. Westin *Privacy and Freedom*. London, Sydney, Toronto: the Bodley Head, 1967, page 7.

[142] Supra Note 141

[143] See Article 4 (2) Law Number 24 Year 2000 concerning International Treaties; no official translation. See http://www.deptan.go.id/kln/daftar_phln/UU%202000%20No%2024%20ttg%20Perjanjian%20Internasional.pdf

Today, Indonesia is not a member of the OECD, but has an enhanced engagement with the OECD. The OECD offered this enhanced engagement as a process to be a member of the OECD. While enhanced engagement is distinct from accession to the OECD, it has the potential in the future to lead to membership. The accession procedure is complex and can be long, as it involves a series of examinations to assess a country's ability to meet the OECD standards in a wide range of policy areas.[144] The OECD does not give a strong impulse to Indonesia to enact privacy and data protection because of the position of Indonesia as not being a member, but it is still important to Indonesia to provide good legislation for a number of economic reasons. The inadequate protection will bring Indonesia into a difficult position when making trade agreements with others.

In contrast with the situation with the OECD, Indonesia was one of the founders of APEC in 1989.[145] APEC is committed to create economic cooperation and trade. APEC is a consultative, not a negotiating forum. All commitments made by APEC member economies are voluntary, and depend on what an economy is willing to give on the basis of its economic status. The association operates by consensus.

In 2007, APEC considered the APEC Data Privacy Pathfinder, the international implementation of the APEC Privacy Framework.[146] it was recognized that new and flexible approaches to accountability and compliance would be needed. The economies involved agreed to begin consideration of international implementation mechanisms by looking at how the use of cross-border privacy rules (CBPRs) can facilitate flexible cross-border information flows within a system that ensures credible oversight and enforcement of CBPRs. The Pathfinder implements this commitment to develop a system that provides for the use of CBPRs by business. The Pathfinder projects will build a system that allows businesses to create their

[144] See http://www.oecd.org/pages/0,3417,en_36734052_36761800_1_1_1_1_1,00.html

[145] See http://www.apec.org/en/About-Us/About-APEC/History.aspx

[146] See APEC Data Privacy Pathfinder Projects Implementation Work Plan – Revised, presented in First technical assistance seminar on the implementation of the APEC Data Privacy Pathfinder Singapore, 22-23 February 2009.

own CBPRs and consumers to rely upon "accountability agents," as well as regulators, in the APEC region to make sure businesses are held accountable for their privacy promises.

Economies are encouraged to consider participating in as many projects as possible, recognizing that economies may be interested in some projects, but choose to take a less active role. Indonesia, however, did not take part in this action, though it has had an influence on the implementation of privacy and data protection in Indonesia. There is no regulation that comprehensively governs privacy and data protection. But, Indonesia has to prepare the protection soon, because of the development of the international activity in privacy and personal data protection and also the development of international trade. This development requires rules concerning the protection of privacy and personal data that are consistent with the principles developed in the international level be arranged immediately. This area needs a good initiative from the Indonesian government because it can be a trade barrier to global trade transaction.

This anxiety is very reasonable because Indonesia still does not have strong legal tools to protect privacy and personal data. In international scales, legislation enacting privacy and personal data protection have become compulsory in EU countries. These EU Directives can be a barrier for Indonesia to make new international or bilateral trade cooperation with EU member states.[147] The EU countries will reject any cooperation without adequate protection for privacy and personal data.

4.3. The nature of Indonesian Privacy and Personal Data Protection

An important issue in need of clarification is whether privacy and data protection law should be considered to be "private law," "public law," or a combination.[148] Kurner makes the point that the distinction between public and private law has been much criticized, but it can be use as a tool to formulate the correct legislation in privacy and personal data protection in Indonesia. In

[147] See the Directive 195/46/EC Article 24.

[148] Kurner, Christopher, Internet Jurisdiction and Data Protection Law, http://www.justice.gov.il/NR/rdonlyres/0C7218F7-8B6D-4A62-9E45-7BFB80621E32/26405/ConflictKuner_article.pdf. See Christopher Kurner's thoughts about the nature of privacy and personal data protection. He made an analysis about the nature of privacy and data protection law.

fact, privacy and data protection law cannot be categorized solely within either private law or public law, since it derives from various legal areas, such as human rights law, telecommunication law, criminal law, and others.

Privacy and data protection are two different but related things. Privacy is clearly stated as a human rights law,[149] but personal data is about access or process of individual data. Privacy is a human rights law and personal data protection is one way to respect human rights.[150] Personal data protection typically contains provisions of a public law nature**,** relating to an authority and its duties and decisions and also often includes civil law provisions, typically on liability for data protection violations.[151]

Indonesia has no singular and unified act for privacy and data protection. Instead, protection is provide with a variety of sectoral laws. However, some regulations indicate that personal data has been protected by the civil law. The paradigm of privacy is known as common value, but there are different values in some common perceptions about privacy. Privacy is also a public value in that it is concerned not just with the individual as an individual or with individuals in common but also with the democratic system. A public value of privacy derives not only from its protection of the individual as an individual but also from its usefulness as a restraint on the government or the use of power.[152]

Privacy can ensure the protection of the citizen from risk of injustice and of personal control and respect for human rights (risk to dignity). In Indonesia, there is a restriction for every right. The public interest is more important than individual rights. For example, in Article 28J (1) of the Indonesian Constitution, every citizen is guaranteed the "freedom of speech, expression including publication." That is, each citizen is given the right to communicate their

---

[149] See Indonesia Constitution 1945 and see Electronic Privacy Information Center (EPIC) and Privacy International (PI): "Privacy & Human Rights 2006" (P&HR 2006), Overview of Privacy, https://www.privacyinternational.org/article.shtml?

[150] Supra note 149

[151] See Jon Bing, "Data Protection, Jurisdiction and the Choice of Law," paper delivered at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong 14 September 1999, http://www.pcpd.org.hk/english/infocentre/files/bing-paper.doc

[152] Marshoof, Altahf, *The Right to privacy in the Information era: A South Asian perspective*, Scripted, Volume 5, Issue 3, 2008.

ideas and experiences to others. But, in relation with privacy, nevertheless there are restrictions. Article 28J (2) also mentions that "every implementation of rights and freedoms, everyone shall be subject to restriction set by law solely for the purpose of ensuring the recognition and respect for the right of freedoms of others and to meet the demands of justice in accordance with moral consideration, values, religion, security and public order in a democratic society."

Privacy, though not an absolute right, must not be treated as immaterial. The right balance must be found and the right to one's privacy should always be respected. Whenever the right to privacy is taken away or restricted, it must be done so for valid and good reasons and not otherwise. The privacy protection is given by the Constitution and the law is restricted with concerns for the public interest on the application. The public sphere will always be the one that leads the society. In other words, the protection for citizens is derived from many sources of law, such as the protection on expressing their ideas and protected by the Constitution and also the law but it is likewise restricted by other laws. These are complementary and support each other.

4.4. Example of possible frameworks and rules for Indonesia

As mentioned above, Indonesia has no singular and unified law that covers privacy and data protection. Rather, protection is provided with sectoral laws. But some regulations indicate that personal data has been protected by the law. The paradigm of privacy is known as common value in that all individuals value some degree of privacy and have some common perceptions about privacy. Privacy is also a public value in that it is not just for the individual as an individual or for the individual in common but also in regards to the democratic system. A public value of privacy derives not only from its protection of the individual as an individual but also from its usefulness as a restraint on the government or the use of power.[153]

Based on the Indonesian model, it might be necessary to build a single and unified regulation as is done within the European regime because of the lack of privacy and data protection concept in the national legislation. The single and unified model is of greater

[153] Supra note 152.

importance because Indonesia first needs to formulate the terms of privacy before enacting privacy laws into national legislation. This step is aimed to encourage Indonesia to adopt a single and comprehensive perspective in the areas of privacy and personal data, as well as help the country to focus more on the issues of privacy and data protection.

Then, the single and unified regulation will help Indonesia to promote the legal certainty of privacy and personal data protection. Also, Indonesia needs to provide adequate[154] protection in order to fulfill the requirements of the international regime but also to fulfill these rights for its own citizens. If Indonesia is obliged to enact the legislation for privacy and data protection because of the need to respect human rights and cooperate economically with other countries, it is better to include international principles in privacy and data protection through national legislation. For example, data privacy protection can be assured through the actions of alternative institutions, be they legislatures, regulatory bodies, courts, or markets. This approach will steadily create stability in privacy and data protection enforcement, thus a good climate will occur and it will help Indonesia to have more cooperation with other countries, in particular with those of Europe, which have a high level of protection in regards to privacy and personal data.

[154] Referred to Article 29 Working Party. First orientations on Transfers of Personal Data to Third Countries -- Possible Ways Forward in Assessing Adequacy. Brussels: European Commission, 1997, XV D/5020/97-ENfinal WP4. 26 June. https://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf

Chapter 5 – Concluding Remarks

This chapter comprises conclusions and recommendations. The conclusions endeavor to answer the research and main research questions, while the recommendation anticipates the drawbacks mentioned in the conclusions.

5.1. Conclusion

1. *What is the nature of privacy and data protection in association with the Indonesian legal system?*

The term privacy cannot be found in any legal text of Indonesia. However, the protection of privacy and data can be found in some legislation. Indonesia gives protection to the privacy and personal data through some legislation, but without providing a single and unified regulation. The protection of privacy and data is based both on human rights and economic realities. The human rights basis refers to the protection of human life, the freedom of expression, and the protection of the citizens' dignity by protecting their personal data from any misuse and inappropriate disclosure. The economic basis refers to protection of individual property such as personal data especially for the electronic commerce and international demand on personal data transfer. Privacy and personal data protection typically contain provisions of a public law nature, but in Indonesia, there are still "private law," "public law," or a combination because the protection derives from various legal areas, such as human rights law, telecommunication law, criminal law, and others.

The application of privacy and data protection in Indonesia is restricted by public interest. In Indonesia, public interest is more important than individual rights. Every implementation of rights and freedoms shall be subject to restrictions set by law solely for the purpose of ensuring the recognition and respect for the right of freedoms of others and to meet the demands of justice in accordance with moral considerations, values, and religion.

2. *Does the existing legal standard of data and protection provide adequate protection to people in Indonesia?*

The partial policies for privacy and data protection given by Indonesia legislation provide no single and unified policy. This means that various legislations can be used to protect privacy and disclosure of data. Legal protection of privacy and data protection can be derived from a variety of sources. There is no guidance or clear definition about privacy and personal data protection in Indonesia. The privacy and data protection in Indonesia are too general and only provide some provisions related to privacy and data protection, such as putting provisions in a Banking Law in relation with consumer bank protection, or non-disclosing data in a human rights law. The model of privacy legislation in Indonesia is less comprehensive. The different legislation about privacy and personal data ensures that the implementation is not consistent because it relies on the institutions, which recognize these policies as issues, such as privacy issues on the Banking Law. If there is a case, the bank that is involved with the case and Bank Indonesia, as the highest level bank in Indonesia, will take it over, and Bank Indonesia will have an authorization to make decisions in relation with this case or, if the privacy issues that arise concern human rights, the issues will be resolved by the National Commission on Human Rights.

However, in many cases, this legislation is not enough to protect citizens from misuse. There are a great many loopholes in policing privacy and data protection regulations in Indonesia. Some of the international principles in privacy and data protection are not recognized in Indonesian legislation. The lack of adequate protection is one of the drawbacks of Indonesian legislation in relation to privacy and data protection.

3. *What is the influence of international standards and regulations of privacy and data protection for the Indonesian situation? And is it important for Indonesia to have a specific regulation about privacy and data protection?*

International instruments for privacy and data protection have an important role in Indonesia. These could be a strong point for encouraging the development of privacy and data protection in Indonesia. As a part of international society, it is important for Indonesia to cooperate with other countries. The development of international standards in privacy and data protection

across the world such as has taken place in Europe, the U.S. or Asia will have a significant impact on Indonesia. It will influence a model of protection because of what special cooperation looks like in Europe, where such protections are strictly and properly regulated, which must influence the kind of cooperation that Indonesia engages in with these countries.

Privacy policies have been introduced as part of the law concerning human rights. Privacy is a part of human rights and personal data protection is one way to respect these rights. In Indonesia, there is an anxiety about protection for privacy and data protection because there still exists no clear and unambiguous legislation. Therefore, privacy and personal data protection issues have become an urgent matter. Many countries have established laws due to these issues, but no Indonesian law has been established with strong, specific regulations. The increase and the development of science and technology, the spread of globalization, and the power of the media have urgently strengthened the need for privacy and personal data protection.

In developing economies such as Indonesia, everything rests on trade, and business recently places much reliance on electronic communication. In fact, very soon we will use electronic tools for governance. Therefore, having laws facilitating personal data protection will be beneficial if those who use the new technology can do so with confidence, so the business-based technology information and e-commerce will be developed smoothly. Information privacy is of great importance for building confidence among traders, consumers, and the public. Privacy indeed is a right that is to be treasured.

5.2. Recommendation

- The fact that Indonesia does not have comprehensive regulation in privacy and data protection will cause the country to lag behind in the development of economic cooperation. Indonesia has to adjust its international development in the areas of protecting privacy and personal data by being included in the APEC Privacy Patchwork or consider the formulation of comprehensive regulation to provide

adequate privacy protection. Toward these goals, it is necessary to study the various existing international instruments.

- Indonesia needs to create a national initiative in privacy and data protection in order to formulate guidance or national standards to protect privacy and personal data protection by examining the existing laws.
- The Indonesia legislation needs to be more focused on the issues of privacy and data protection by avoiding the obscurity of provision by defining the scope and determining what the subject is and setting forth stricter and narrower provisions in the formulation of legislative protection.

Bibliography

Legislation /Directive/Convetion

Australian

Australian Law Reform Commission Report 108

Chinese

Chinese Constitution (1982)

1997 Chinese Criminal Law

EU

Article 29 Working Party. An additional Protocol 108

Charter of Fundamental Rights of the European Union, *OJ* C 341, 18.12.2002

Commission of the European Community. *Communications on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security*, Com (90)314.SYN 287, 44

Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 5 February 2010

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

Council of Europe Convention 1981

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31/07/2002

Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and

European Convention on Human Rights of 4 November 1950

Explanatory Amendment Explanatory Memorandum on the amendments to Convention 108 allowing the accession of the European Communities

Explanatory Report Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention.

Article 29 Working Party, First orientations on Transfers of Personal Data to Third Countries -- Possible Ways Forward in Assessing Adequacy

Article 29 Data Protection Working Party (2005) Working document on data protection issues related to RFID Technology

Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data

Working Party 74, Article 29-Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 2003.

Working Party 107, Article 29 - Data Protection Working Party. Working Document Setting Forth a Co Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", 2005 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_en.pdf

Indonesia

1945 Indonesia Constitution (UUD) 1945

Penal Code of Indonesia

Law Number 8 Year 1981 concerning Criminal Procedure Law

Law Number 10 year 1998 on Banking

Law Number 39 Year 1999 concerning Human Right

Law Number 24 year 2000 on International Treaties

Law Number 10 year 2004 on the Establishment of Regulation

Law Number 29 year 2004 concerning medical Practices

Law Number 11 Year 2008 concerning Information and Telecommunication

Law Number 36 year 2009 on Health Law

Government Regulation number 7/6/PBI/2005 concerning the Transparency of Information to Banking Product and Consumer personal Data Use

The International Convention/Guidelines/Framework/Work Plane

APEC Privacy Framework 2004

APEC Data Privacy Pathfinder Projects Implementation Work Plan – Revised, 2009

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted on 23 September 1980

The US

U.S Freedom of Information

The United Nation

Convention for the Protection of Human Rights and Fundamental Freedoms

International Covenant on Civil and Political Rights, United Nations, 1966

Universal Declaration of Human Rights, United Nations, 1948

Books, Journals, Articles &Papers

Ali, Ahmad, *Law and Development in Changing Indonesia*, IDE Asian Law Series No. 8 Law and Development in Asian Countries, Institute of Developing Economies (IDE), JETRO, 2001.

Altahf marshoof, *The Right to privacy in the Information era : A South Asian perspective*, Scripted, Volume 5, Issue 3, 2008

Bennett, Colin. J & Raab, Charles. D, The Governance of Privacy: *Policy Instruments in Global Perspective,* Ashgate Public & Co, 2003, Chapter 4, Page 74-77.

Bing, Jon, "Data Protection, Jurisdiction and the Choice of Law," paper delivered at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong 14 September 1999, http://www.pcpd.org.hk/english/infocentre/files/bing-paper.doc

Boehmer, R. and Palmer, T.S, "The 1992 EC data protection proposal: an examination of its implications for US business and US privacy laws", *American Business Law Journal,* Vol. 31 No. 2, pp. 265-31, 1993

By Yu Du, Matthew Murph, *Privacy protection in China-Latest Development*, 2010, http://www.mmlcgroup.com/sitebuildercontent/sitebuilderfiles/privacy270810.pdf

C. Chung and I. Shin, *On-Line Data Protection and Cyberlaws in Korea* , 27 Korean J. of Int'l and Comp. L. 21, 1999.

Crompton, Malcom, *Chapter 3 Overview of Asian privacy Law Lesson Learned and Possible Way Forward*, Privacy Symposium Sponsored by the Institute of Law China Academy of Social Science, Role of Information Service Providers, 2006

De Hert. P, Gutwirth. S, Moscibroda. A, Wright. D, Fuster. MG, *Legal safeguard for privacy and data protection in ambient intelligent,* 2008

De hert, Paul & Guthwirth, S, *Data Protection in the Case Law of Strasbourg and Luxemburg Constitusionalisation,* in Action, in Gutwirth S, Y Poullet, P. De Hert, J Nouwt & C. De Terwangne (Eds), reinventing Data Protection?, Springer Science, Dordrecht, 2009, page11 (C. Riehle, Book review of B Siemen, C.M.L.J., 2007, page 1193-1195)

Dewi, Shinta, Cyberlaw : Perlindungan Privacy atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional, Widya Padjajaran, 2009.

Dewi Shinta, *Cyberlaw : Praktik Negara-Negera dalam mengatur Privacy dalam E-Commerce*, Widya Padjajaran, 2009.

Electronic Privacy Information Center (EPIC) and Privacy International (PI): "Privacy & Human Rights 2006" (P&HR 2006), *Overview of Privacy*, https://www.privacyinternational.org/article.shtml?

Faiz, Pan Mohamad, *Human Rights Protection and Constitutional Review: A Basic Foundation of Sustainable Development in Indonesia,* paper presented on International Students'Scientific Meeting 2008, The Institute for Science and Technology Studies (ISTECS) and Indonesian Student Association of nederlands, Delft University of Technology,Delft, The Netherlands on 13-15 May 2008

Freshfields Bruckhouse Delinger, Privacy Protection Across Asia - A regional Perspective, Freshfiel bruckhouse Delinger LLP, 2008 http://www.freshfields.com/publications/pdfs/2008/oct08/24238.pdf

Ghani, Abdul Norjihan & Sidek, Zailani Mohamed, *Personal Information Privacy Protection in E-Commerce*, WSeas Transaction on Information Science and Application, Issue 3, Volume 6, March 2009.

Gross, Hayman, *The Concept of Privacy 42*, New York University Law Review 34, 1967.

Gutwith, S. & Hert, P. de, *Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action*, Poullet, Y.; Gutwith, S.; De Terwanghe, C.; Hert, P. de (Ed.) *Reinventing data protection?, Springer science, Dordrecht, 2009, 3-44, page 5*

Hong Xue, *Privacy and Personal Data Protection in China:an Update for the year end 2009*, Institute for the Internet Policy & Law, Beijing Normal University, PR China, Elsevier Ltd, 2010.

International Chamber of Commerce, ICC Task Force on Privacy and Protection of Personal Data, ICC report on binding corporate rules for international transfers of personal data, report prepared by Christopher Kuner and Robert Bond. Paris. 2004.

Jean Slemmons Stratford, Jean Slemmons & Stratford, Juri, *Data Protection and Privacy in the United States and Europe*, presented at the IASSIST Conference, May 21, 1998, at Yale University, New Haven, Connecticut. Jean Slemmons Stratford, University of California, Davis, and Juri Stratford, University of California, Davis.

JoongAng Daily, *Phone Camera Makers Are Told to Use 'Click' to Protect Privacy*, November 12, 2003, https://www.privacyinternational.org/article/phr2006-republic-south-korea#[77]

K. Orito and M. Kiyoshi, *Privacy Protection in Japan : Cultural influence on the Universal Value*, 2002-2006 , http://bibliotecavirtual.clacso.org.ar/ar/libros/raec/ethicomp5/docs/pdf_papers/52Orito,%20Yohko.pdf

Kuner, Christhoper, *Regulation of Transborder Data Flows under Data Protection and Privacy Law*, TILT Law & Technology Working Paper No. 016/2010, October 2010, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 016/2010, http://ssrn.com/abstract=1689483

Kuner, Christopher & Bond, Robert*, International Chamber of Commerce, ICC Task Force on Privacy and Protection of Personal Data*, ICC report on binding corporate rules for international transfers of personal data, Paris, 2004.

Levin, Avner and Nicholson, *Mary Jo, Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground.* University of Ottawa Law & Technology Journal, Vol. 2, No. 2, pp. 357-395, 2005. Page 361, SSRN: http://ssrn.com/abstract=894079

Makarim, Edmon, *Tanggung Jawab Hukum Penyelenggara Sistem Electronic*, Lembaga Kajian Hukum Technology, Fakultas Hukum UI, Rajawali Press, Jakarta, 2010

Malcouronne, Peter, *Report on the First Regional Conference for the Asia and Pacific Region on the Ethical Dimensions of the Information Society*, Hanoi, 2008, portal.unesco.org/...**Conference**.../Final_Report_Hanoi_**Conference**.doc

Official Journal of the European Communities, Directive 95/46/EC of the European parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data,281/31, 1995

Peter B. Swire and Robert E. Litan, *Avoiding a Showdown over EU Privacy Laws*, Brookings Policy Brief, no. 29 (February 1998) (URL http://www.brook.edu/comm/ policy briefs/pb029/pb29.htm)

Posner, Richard A, *Economic Analysis of Law*, 5th edition, New York, Aspen Publisher, 1998.

Purtova, Nadezhda, *Private Law Solution in European Data Protection Relationship to Privacy , and Waiver of Data Protection Rights,* Netherlands Quarterly of Human Rights, 2010, vol. 28, nr. 2, pp. 179-19, page 3.

Regan, P.M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill / London 1995.

Rita M. Walczuch, Sanjay K. Singh, Todd S. Palmer, *An Analysis of The Cultural Motivations for Transborder Data Flow Legislation,* Information Technology & People, Vol. 8 No. 2, 1995, pp. 37-57. MCB University Press, 0959-3845,(URL http://arno.unimaas.nl/show.cgi?fid=10243)

Robert Aldrich, "Privacy Protection Law in the United States," (NTIA Report 82-98) in the US Congress. House Committee on Government Operations. Oversight of the Privacy Act of 1974: Hearings. 98th Congress, 1st Session, 7-8 June 1983, 489 (Y4.G74/7:P93/11/974)

Robinson, Neil, Graux, Hans, Botterman, Maarteb & Valeri, Lorenzo, *Review of The European Data Protection Directives,* Technical Report, International Commissioner's Office, Rand Corporation, 2009,

Sarah Ellis and Charles Oppenheim. "*Legal Issues for Information Professionals, Part III: Data protection and the Media – Background to the Data Protection Act 1984 and the EC Draft Directive on Data Protection*," Journal of Information Science 19 (1993):85.

Shaffer, Gregory, "Globalization and Social protection : The Impact of EU and International Rules in The Ratcheting Up od U.S. Data Privacy Standards", *Yale Journal of International law*, Vol 25, 1-88, 2000.

Stratford, Jean Slemmons & Stratfor Juri, *Data Protection and Privacy in the United States and Europe*, Paper presented at the IASSIST Conference, May 21, 1998, at Yale University, New Haven, Connecticut. Jean Slemmons Stratford, University of California, Davis, and Juri Stratford, University of California, Davis.

Solove, Daniel J., *Conceptualizing Privacy*. California Law Review, Vol. 90, p. 1087, 2002. SSRN: http://ssrn.com/abstract=313103

Suryawan , M.A, *Bukan Sekedar Hitam Putih*, Azzahra Publising Ed I, 2006

Tan, Bryan, Data Protection Guide : Singapore, Keystone Law Corporation, 2010, http://www.keystonelawcorp.com/downloads/SingaporeKeystoneLaw20103C.pdf

Tan, Johanna G, *A Comparative Study of the APEC Privacy Framework-A New Voice in the Data Protection Dialogue?*, Asian Journal Comparative Law, Volume 3, issue I, 2008, page 1, http://www.bepress.com/cgi/viewcontent.cgi?article=1071&context=asjcl.,

The first report on Towards an International Infrastructure for Surveillance of Movement, Transfering Privacy : The Transfer of Passenger Records and the Abdication of Privacy

Weber, `Rolf. H, *Internet of Things – New Security and Privacy Challenge*, computer law & security review 26, Elsevier Ltd, 2010

Westin, Alan F, *Privacy and Freedom*. London, Sydney, Toronto: the Bodley Head, 1967, page 7

White, Alison, "Control of Transborder Data Flow : Reaction the Data Protection Directive", *International Journal of law and Technology*, Vol 5 No 2, 2011

Walcuzuc, Rita. M, Singh, Sanjay. K, Palmer, Todd. S, *An analysis of the cultural motivations for transborder data flow legislation Website*, MCB University Press, Information Technology & People, Vol. 8 No. 2, 1995.

Website, Online contents and Others sources of information

Ali Budihardjo, Nugroho, Reksodiputro website, avalaible online at http://www.pranata.lipi.go.id/wpcontent/uploads/2009/01/UUTIE.pdf, last accessed 24 april 2011

Anonymous, Data Nasabah Bocor Tanggung Jawab Bank, Suara Merdeka Cybernews, March 24, 2011, http://suaramerdeka.com/v1/index.php/read/cetak/2011/03/24/141103/Data-Nasabah-Bocor-Tanggung-Jawab-Bank, last accessed 24 April 2011

Anonymous, BI Tak Bisa Berbuat Banyak kasus Penjualan Data Nasabah, March 30, 2011, http://www.vibiznews.com/news/banking_insurance/2011/03/30/bi-tak-bisa-berbuat-banyak-kasus-penjualan-data-nasabah/10, last accessed 24 April 2011

Data Protection, http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Dataprotection, visited 24 april 2011

Freedom of Information, Title 5 U.S.C. 552(b) (6), available online at http://www.justice.gov/oip/amended-foia-redlined-2010.pdf, last accessed 12 may 2011

Freshfield Bruckhause Deringer, Data Privacy Protection Across Asia, available online at http://www.freshfields.com/publications/pdfs/2008/oct08/24238.pdf, last accessed 5 may 2011

Indonesia Legislation http://hrli.alrc.net/mainfile.php/indonleg/133/, last accessed 12 June 2011

International Chamber of Commerce website, http://www.iccwbo.org/uploadedFiles/ICC/policy/ebusiness/pages/FINAL_ICC_BCRs_report_rev.pdf, last accessed 12 June 2011

Info-communication Development Authority of Singapore, Policies and Regulation, http://www.ida.gov.sg/Policies%20and%20Regulation/20060627155443.aspx, last accessed 12 june 2011

Indonesia face dualism core, http://www.antaranews.com/en/news/68319/muhammadiyah-avoids-movement-backing-ahmadiyah-dissolution, last accessed 12 june 2011

JoongAng Daily, *Phone Camera Makers Are Told to Use 'Click' to Protect Privacy*, November 12, 2003, https://www.privacyinternational.org/article/phr2006-republic-south-korea#[77]

MUI Won't Back Down on Ahmadiyya Fatwa, http://www.thejakartaglobe.com/home/mui-wont-back-down-on-ahmadiyah-fatwa/423342, last accessed 12 june 2011

MUI urges government to ban Ahmadiyya http://www.thejakartapost.com/news/2011/03/08/mui-urges-government-ban-ahmadiyah.html, last accessed 12 june 2011

Official website of OECD, www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html, last accessed 12 June 2011

Official website of Europian Legislation, http://europa.eu/legislation_summaries/information_society/l14012_en.htm, last accessed 12 june 2011

Official website of OECD, avalaible online at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, last accessed 16 June 2011

Osborne Clarke, Binding Corporate Rules: Data export solution or data export headache?, issue of the World Data Protection Report, BNA International Inc, 2008, http://www.osborneclarke.com/~/media/Files/publications/import/en/binding-corporate-rules-data-export-solution-or.ashx, last accessed 12 june 2011

Official Website Law Library of Congress, Malaysia, avalaible at http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205401926_text, last accessed 12 April 2011

Official website Council of Europe, Data protection, History, http://www.coe.int/t/dghl/standardsetting/DataProtection/History_more_en.asp, last accessed 12 june 2011

Official website Indonesia-China cooperation, http://www.cic.mofcom.gov.cn/ciweb/cci/info/Article.jsp?a_no=257621&col_no=521

http://www.iccwbo.org/uploadedFiles/ICC/policy/ebusiness/pages/FINAL_ICC_BCRs_report_rev.pdf, last accessed 12 june 2011

Official website of European Union, Trade, http://eeas.europa.eu/delegations/indonesia/eu_indonesia/trade_relation/index_en.htm, last acceseed 12 june 2011

Official website of Central Statistic Bureau http://www.bps.go.id/, last accessed 12 june 2011

Official website of Constitutional Court of the Republic of Indonesia
http://www.ccourt.go.kr/home/history/world/pdf/05.pdf

Official website of Ministry of Communication and Information Technology,
http://www.postel.go.id/content/EN/regulasi/telecommunication/uu/law36-1999.pdf

official website of Indonesia Parliament,
http://www.dpr.go.id/complorgans/commission/commission1/risalah/K1_risalah_MP_III_TS_10-11_Risalah_RDP&RDPU_Kom_I_dg_BRTI,_ID-SIRTII,_Operator_Telekomunikasi.pdf, last accessed 24 may 2011

official website of Ministry of Communication and Information Technology,
http://www.postel.go.id/update/id/baca_info.asp?id_info=1636, last accessed 5 may 2011

Official website of Ministry of Health,
http://depkes.go.id/downloads/UU_No._36_Th_2009_ttg_Kesehatan.pdf, last accessed 6 june 2011

Official website of OECD,
https://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf , last ccessed 12 may 2011

Privacy international overview of Republic of South Korea, 2007,
https://www.privacyinternational.org/article/phr2006-republic-south-korea

The adequacy decision of the European Commission was published at the Official Journal of the European Communities, volume 43. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF, last accessed 12 june 2011

The principles of OECD guidelines on the protection of privacy and transborder flow of personal data,http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, last accessed 12 june 2011

The APEC Privacy Framework as endorsed by Ministers in November 2005, available online at: http://203.127.220.112/content/apec/news___media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.downloadlinks.0001.LinkURL.Download.ver5.1.9, last accessed 12 june 2011

US-EU Safe Harbor Principles overview, Export.Gov, US-EU Safe Harbor, U.S Departement of Commerce, https://www.export.gov/safeharbor/eu/eg_main_018476.asp, last accessed 12 june 2011

US-EU safeharbor official website, https://www.export.gov/safeharbor/eu/eg_main_018476.asp, last accessed 12 june 2011

Working Party 107, Article 29 - Data Protection Working Party. Working Document Setting Forth a CoOperation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules".2005 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_en.pdf

Wahono, Tri, Indonesia Pengguna Facebook Terbesar di Asia, Kompas, June 1, 2010, http://tekno.kompas.com/read/2010/06/01/22190833/Indonesia.Pengguna.Facebook.Terbesar.di.Asia-12, last accessed 24 april 2011

Zain, Winarno, *The pain, gain from ACFTA*, The Jakarta Post, april 25, 2011, avalaible at http://www.thejakartapost.com/news/2011/04/25/the-pain-gain-acfta.html, last accessed 24 april 2011