HYBRID PARADIGM FROM EUROPEAN AND AMERICA CONCERNING PRIVACY AND PERSONAL DATA PROTECTION IN INDONESIA

Edmon Makarim[1]

Abstract

In the emerging era of information and technology, the importance of privacy and data protection is growing ever since. However, despite such common concern from the society, there is some confusion about the mechanisms of differentiation and scope of discussion about privacy with the protection of personal data and even impressed blended with issues of spamming issues. With comparison to Europe and the US legal perspectives, Therefore, this paper tries to discuss such problem in accordance to the perspective of laws to the communication itself.

Keywords: law, privacy, data protection.

I. Preliminary

Recently an Indonesian famous Newsletter writing down some of the problems related to Privacy and Personal Data in Indonesia. It is necessary to bear in mind about the prudence and legal awareness to the community. But unfortunately there is a little confusion where there is actually little difference in the mechanisms of differentiation and scope of discussion about privacy with the protection of personal data and even impressed blended with issues of spamming issues.[2] Although there is a common thread, but it should be written with quite comprehensive in order to avoid confusion in the understanding and protection mechanisms. Therefore, this paper tries to discuss such problem in accordance to the perspective of laws to the communication itself.

II. Meaning and Scope of Privacy

Literally, the essence of "Privacy" actually means to all things related to personal life of every human being (personal life) which is not only concerned about his/her dignity as a human being, but also the security and comfort themselves in the social life. It is not only understood within the scope of the

[1] The author is a Senior Law Lecturer at the Faculty of Law Universitas Indonesia. This article was presented in the Seminar of "Private Data Protection Draft Bill" on 15 March 2013 and conducted by the Ministry of Civil Official Empowerment and Bureaucratic Reform.

[2] In general, Spamming is the conduct to send unsolicited e-mail, often of a commercial nature. It is sent indiscriminately to multiple mailing lists, individuals, or newsgroups which may against the law and violates the privacy of the receiving parties.

motion corresponding private living space (private spheres) but also includes the effect of what is happening in the public sphere (public-spheres) against him. This can be seen clearly if everyone talking about someone with intentional and specific opinions about the values based on their personal life. Additionally pins when other people did exchange our personal data without permission or without the knowledge of the person concerned. As an initial note Privacy needs to be seen at least two scopes, namely (i) the scope of internal security, which includes everything against him (intrusion or interference from outside influences) and (ii) external scope includes everything that affects the comfort of her (exposure of the other party to the personal data concerning him well, opinion data[3] and data intentional[4]).

Most of common law's legal experts would define privacy in narrow definition as every person is not to be disturbed by others (right to be let alone) or in other words, everyone should feel safe in his personal life, his property, and also in his correspondence communications. While in a broad sense, privacy is not just about the safety of every person but also proper touch to comfort them in the social interaction. It is manifested in the form of anonymity, confidentiality of personal data to be accessible to others, protection from coverage solely intended to humiliate, and so forth. All thinking is a logical consequence of the existence of human values among couples with Honour

[3] Opinion data is data produced by certain professional about other people who become patients or users of its services.

[4] Intentional data is data that take other people's subjective impression of the person concerned.

and Privacy and reputation as contained in article 17 of the ICCPR:[5]

Article 17 ICCPR: (1). No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks.

Uniquely in Indonesia where the importance of the protection of honor and reputation, often seem forgotten or looked neglected, especially if it is confronted with the public interest. And what is the size that something is "public interest" was relatively vaguer than the size of the existence of privacy itself, because of the "public interest" should be kept in perspective and contextual within specific sectors. If not, then it will be a violation to individual's liberty. Such violation is actually not only committed by the state, but also by any person to another in the name of "freedom" and human rights, or by the corporation on behalf of the disclaimer, or even by people on behalf of the norms and interests of the public or public order.

III.Interactive Justice between Privacy and the Public Interest

Often we see that privacy be exposed to the public interest to open its own privacy. In fact, the "public interest" itself can be translated into two things, namely (i) the public interest to access information and (ii) the public interest to restrict access to the information itself in the context of confidentiality. Both opening and closing the information are actually protected by law. Legal principle has been recognized in Law 14 of 2008 on Public Information ("UU KIP") which is basically due respect to the interests of the privacy law, trade secret and confidential by the state categorized as Excluded Information.

Article 2 (4)	The Article's Legal Meaning
Public Information is exempt confidential in accordance with the Law, decency, and common interests based on the examination of the consequences if the information given to the public, and after carefully considering the closing of Public Information to protect the interests of greater than open or otherwise Explanation Paragraph (4)	What is meant by "the consequences" is the consequences that harm the interests protected by this Act if the information is opened. Classified information should be open or closed based on the public interest. If the larger public interest can be protected by covering the information, the information must be kept secret or closed and / or vice versa.

[5] See also, Article 12 Universal Declaration of Human Right: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Furthermore, it is also stipulated in the Regulation 61 of 2010 on the Implementation of Freedom of Information Law ("PP-KIP '), where the term of protection is in accordance with the provisions of applicable legislation. This implies the existence of the legal recognition of those special arrangements that exist in other laws.

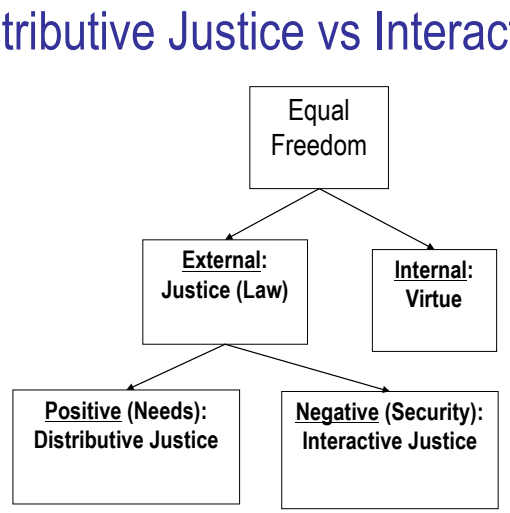
Article 8-KIP	The Article's Legal Meaning
(1) Exclusion Period Public Information when opened to reveal the contents of an authentic act of a personal nature and will last one's will or determined under the provisions of the legislation. (2) Exemption Period when opened Public Information and Public Information given to the applicant to reveal personal secrets established over a period of time required for the protection of one's personal secrets. (3) Public Information referred to in paragraph (1) and (2) can be opened if: a. revealed the secret party gives written consent, and / or b. disclosure relates to a person's position in the public offices in accordance with the provisions of the legislation. Explanation of	Paragraph (1) What is meant by "the provisions of legislation" such as legislation on archives. Paragraph (2) The term "public information which, if opened and given to the Public Information Applicant may reveal personal secrets" are: 1. history and condition of a family member; 2. history, condition and treatment, treatment of physical health, and psychological one; 3. financial condition, assets, income, and bank account a person; 4. evaluation results with respect to the capability, intellect, abilities and recommendations, and / or 5. records relating to an individual's personal unit activities related to formal and non-formal education unit. Paragraph (3) Letter a Self-explanatory. Letter b What is meant by "the provisions of legislation" such as legislation regarding eradication of corruption and legislation on combating corruption commission

Misunderstandings to always put privacy as being contrary to the public interest, seems to occur because of errors on the meaning of the word "freedom" is often perceived as a rather unrestricted freedom of personal freedom from the influence of others.[6] In theory it can be stated that the Justice Inter-

[6] See, Article 2 The Law No.40 Year 1999 concerning Press: Freedom of the press is one manifestation of the people's sovereignty based on the principles of democracy, justice, and rule of law.

active positive than negative freedom there is also freedom. In positive freedom of every person is protected by law, but on the other hand there are also negative freedom which every person must also have an internal awareness (virtue) to respect the rights of others. In the context of any communications in the information age must have into account the effect of mass communication slayings. Pretext of public interest can also be misused to attack others in public spaces. At that time, a good legal system should continue to provide equilibrium to every person to be able to recover its rights if it is violated by any person, whether by individuals, corporations, communities and law enforcement do the actions are arbitrary or unlawful.[7]

In the media regime, meaning Freedom is often equated with the presence of the Privilege, where it was divided into two properties, namely absolute privilege and qualified privilege. Absolute privilege in the context of disclosure of information in court proceedings or parliamentary session due to reveal the ultimate truth based on the evidence found. While qualified privilege in the context of the media, because the media is in fact never value-free or free from the influence of the subjective values exist. Therefore, they are provided with the code of ethics of high value to avoid betrayal of the mandate of developing of the public itself to meet the right people know to give control to the authorities or to the parties that perform governmental functions.



IV. Privacy vs Public Interest and Spamming

With regard to the public interest above, it is often forgotten that the actual Privacy protection is also a public interest in the context of the obligation to respect the dignity of others. The public interest is actually the sum of each individual's own interests. It cannot be denied that the public interest in practice is not voiced by the public itself, but by a group of people on behalf of a particular society (particular group / special interest group) represents a

[7] See Richard W. Wright, "The Principles of Justice" (2000) 75 Notre Dame Law Review 1859.

particular interest. That by itself was never cleared of conflict of interest and the determination of a particular agenda setting.

In connection with the above, the next concern is the question of "whether the actual delivery of commercial and promotional information through other means of communication is in the public interest that should be appreciated that the privacy beat everyone?" In developed countries like the U.S. alone, it is not categorized as freedom of speech, because commercial speech is communication for the benefit of for-profit and not in the public interest. Therefore, in the development, promotional information in some countries has been set up to not harm the privacy of others, even the OECD has conducted a study and recommendation to regulate spamming. Furthermore, even the ITU and Cybercrime convention directs spamming activities as something that needs to be criminalized because in fact been detrimental to the public interest itself, in particular the protection of privacy of any person certainty.

Spamming is inevitable that generally occurs due to abuse of the acquisition and use of personal data to others, therefore it is necessary to prevent a "presumed liability" to any party who obtained personal data, private and state is no exception. Everything should be responsible for keeping personal data everyone gained. Legal obligation is placed upon the party which creates the data and not to the owner of the data handed to the trust is used only to the extent set forth affair to him.

V. Trends and Dynamics of Global Privacy Laws

Looking at the literature review on Privacy and Data Protection globally, there are at least two different paradigms and regimes between America and Europe. Then, it narrows down to propose a middle way in the form of OECD privacy Guidelines which then evolved again into the proposed APEC Privacy Framework. At least, it can take an understanding that in fact the Privacy has a broader scope than the protection of Personal Data. Privacy will further aspect refers to a wider range with more look to the predicate attached to a Legal Subject. Such thinking is carried by most experts in the United States where, in principle, they are doing a subjective approach to the expectation of privacy of a person's own (reasonable expectation to privacy). They believe that the State should not intervene in depth about the privacy protection mechanism itself through a particular state administration. It is all depends on the society itself (Self Regulatory Organization). They view it would make economic cost becomes higher.

In practice in the U.S., they will perform contextual application of the doctrine of the knowledge of a risk of disclosure of information to others (general Assumption of risk). If the question had been aware of a possible disclosure of information to other parties concerned and do not mind then it is not regarded as a violation of Privacy.

The main constitutional provision in both Canada and the US where privacy is read into, is the provision protecting against unreasonable search and seizure. The chapters suggest that this right is formulated in terms that are perhaps too physical, but the cases quoted show that the wordings are (still?) open

enough for the courts to apply them in a rapidly changing world. A crucial element in both rights is that they protect people, not places. This approach has significant advantages in a technology-driven world where traditional notions of place become blurred. In a world of Ambient Intelligence, 'place' becomes something centering on people rather than on physical objects or geographical locations, since the surroundings change along with the people acting in them.

Courts in Canada and the US also use the criterion of 'reasonable expectations of privacy' to determine whether certain measures are unreasonable or not. Its application, especially in the US, seems rather tricky for privacy protection in a rapidly changing world where technology permeates everyday life. As technology develops, the 'reasonable expectation of privacy' develops along with it, generally to the detriment of privacy as technology of itself tends to decrease privacy expectations. An example is the Kyllo case in the US, where the Supreme Court used the criterion of a device being 'in general use' to determine whether or not it infringed privacy; as most technology applications tend to develop from limited, sectoral use to general, public use, the related privacy expectations at one point in time will become unreasonable. Hence, using 'reasonable expectations of privacy' to face developments in technology poses the risk of a slow but sure erosion of privacy. Although the criterion is not wholly absent in the caselaw of the European Court of Human rights, courts and legislatures should be cautious in applying it in the field of technology law.[8]

The main constitutional provision in both Canada and the U.S. where privacy is read into, is the provision protecting against unreasonable search and seizure. The chapters suggest that this right is formulated in terms that are perhaps too physical, but the cases quoted show that the wordings are (still?) open enough for the courts to apply them in a rapidly changing world. A crucial element in both rights is that they protect people, not places. This approach has significant advantages in a technology-driven world where traditional Notions of place Become blurred. In a World of Ambient Intelligence, 'place' becomes something centering on people rather than on physical objects or geographical locations, since the surroundings change along with the people acting in them.

Courts in Canada and the U.S. also use the criterion of 'reasonable expectations of privacy' to determine whether certain measures are unreasonable or not. Its application, especially in the U.S., seems rather tricky for privacy protection in a rapidly changing world where technology permeates everyday life. As technology develops, the 'reasonable expectation of privacy' develops along with it, generally to the detriment of privacy as technology of itself tends to Decrease privacy expectations. An example is the Kyllo case in the U.S., where the Supreme Court used the criterion of a device being 'in general use' to Determine Whether or not it infringed privacy; growing niche as most technology applications to develop from a limited, sectoral use to the general, public use, the related privacy expectations at one point in time will Become unreasonable. Hence, using 'reasonable expectations of privacy' to face developments in technology poses the risk of a slow but sure erosion of privacy. Although the criterion is not wholly absent in the caselaw of the Eu-

[8] Ronald E.Leenes, Bert-Jaap Koops and Paul De Hert, Constitutional Rights and New Technologies, (Leiden, Netherlands: T-M-C Asser Press, 2008), pp. 265-285. See also the continuing research in the context of Indonesia. (Edmon Makarim, et. all., Hak Konstitusional dan Teknologi Informasi, 2010).

US	European
1. Notice / Awareness (Notice / Awareness): This is the most fundamental principle, consumers should be notified about the information practices of a company before personal information is collected from them. The scope and content of the notice varies from company to company. Other basic principles will only have meaning when consumers are informed about the information practices and the rights of those who are associated with them. 2. Choice / Consent (Choice / Consent): This principle requires that consumers be given a choice about the use of personal information collected from them. 3. Access / Participation (Access / Participation): This principle requires that consumers be given access to the information collected about them and the ability to juxtapose the accuracy and precision of the data. 4. Integrity / Security (Integrity / Security): This principle requires companies to take steps to ensure that information collected from consumers is accurate and secure them from unauthorized use. 5. Application / Repair (Enforcement / Redress): This principle requires the government or self-regulatory mechanism to impose sanctions on non-compliance practices fair information.	The eight data protection principles which must be considered by the data controller, namely: 1. Personal data should be obtained in an honest and legitimate. 2. Personal data should be held only for one or more specific goals and legitimate. And should not be further processed in a way incompatible with those purposes. 3. Personal data should be feasible, relevant, and not too large in relation to the purpose or purposes of the processing. 4. Personal data shall be accurate and where necessary kept up-to-date. 5. Personal data shall be processed in accordance with the purpose and should not be held for longer than the time required for the purpose or benefit of those goals. 6. Personal data shall be processed in accordance with the rights of data subjects as stipulated in this law. 7. Actions appropriate safeguards should be taken to respond to the processing of personal data and the illegitimate and unexpected loss or damage of personal data. 8. Personal data should not be sent to other countries or territories outside the territory of European Economic unless the country or territory to ensure a level of protection of the rights and freedoms of data subjects in relation to the processing of personal data. Rights of Data Subjects □ To be informed by the data user of the data collection □ To have access to the personal data □ To be supplied with a copy of the personal data □ To correct / update the Data □ To Prevent collection Likely to cause damage or distress

ropean Court of Human rights, courts and legislatures should be cautious in applying it in the field of technology law.

Meanwhile, different approaches developed in Europe, they are more objectively look at the application of Privacy. Without undisputed substances

of information have to explain myself that it is related to a person's privacy. For example, is information about a person's intimate relationship with another person, a person's medical records or subjective conditions both physical and mental health of a person. It is equivalent to the existence of personal data of everyone. With control corporeal approach to the ownership of personal information data for each person (objective approach) the protection of privacy will be more secure. They saw that the Personal Data is the right of ownership over one's personal data attached to the self (Data Owners) and not to the person who obtained the data (Data Controller) and / or the parties to process such data (Data Processor).

With the approach of the EU's objective is more focused on the confidentiality and security of personal information is itself in perspective becomes an important issue. State deems necessary to intervene in the data protection mechanism itself through certain agencies were also given the authority to investigate it. Therefore, any party seeking to collect personal data of others must go through the licensing obligation and / or notice and supervised by state agencies for certain security and comfort of every person to be undisturbed.

It should be noted that the administrative core of the differences which arise are two different paradigms, the first paradigm (AS) is preferred to encourage the completion of a self-regulatory without government intervention because more emphasis on individual freedom itself and Self-Regulation mechanism whereby the state continues to strengthen it by giving administrative sanction for the violation. In accordance to electronic privacy act, the prosecutor may demand fines to the offender's privacy case and investigate public complaints about it. While the EU would prefer to take the role of state interference is strictly through Data Office and Registrar in protecting the interests of every citizen.

Electronically both paradigms also has a derivative different regulatory mechanisms. Derivative of Subjective approach is the application of mechanism-Out Option ("Opt-out"), where each person is considered free to say hello or try to initiate communication with others first, but if the relevant objections and voiced his opposition to the person should stop actions. If it is done by sending messages via electronic communication, the sender must provide the means to express disapproval (unsubsribe). After the rejection, if they do then that's when sending information privacy violations. Furthermore, in the context of communication via telephone then the business must provide a system of Do-Not-Call-Registry ("DNCR"), which allows anyone who bothered to register themselves to not be bothered. It is as if protecting consumers on the one hand, but on the other hand actually burdening consumers because they actually have to pay to do the call to the DNCR.

While the derivative of the objective approach is Option-in mechanism ("opt-in"), where each person should ensure basic legal right to communicate with others. Concerned have an obligation that what does not violate the privacy of others. In practice, the sender has had a measure of the consent of the parties who want to greet. One example is the mention of reference from which he obtained the address of the communication to the relevant parties.

Furthermore, the practice of trade between them, the U.S. had considered not properly protect the privacy of European perspective, then they agreed on the safe-harbor provisions to enforce the Fair Information Practice

Principles set by the U.S. Federal Trade Commission to the EU Data Protection principles, thus sprang 7 principles of safe-harbor equipped with a Self Certification as an embodiment of the enforcement of the Data Protection and Privacy.

The scheme establishes seven Safe Harbor principles which are broadly equivalent to the standards established by the principles of the Act.

- Notice: giving individuals notice of the purposes for which their data are collected, notice of the third parties to whom the data may be disclosed, information to enable the individuals to contact the organisation for enquiries or complaints and the means offered for limiting use and disclosure.
- Choice: offering individuals the choice of opting out of disclosure to third parties and the choice of whether or not to allow the organisation to use the data for purposes other than those for which they were originally collected. An opt-in approach is required if sensitive data are involved.
- Onward transfers: data may be disclosed only to third parties who either subscribe to the Safe Harbor principles, or who are subject to the Data Protection Directive, or who enter into a written agreement to provide the equivalent level of privacy protection.
- Access: providing the individual with access to his data and giving him the right to have the information corrected upon request, unless the burden or expense of doing so is disproportionate or would violate the rights of another individual.
- Security: taking reasonable precautions to protect personal data from loss or misuse and from unauthorised access, disclosure, alteration and destruction.
- Data integrity: ensuring that data are accurate, up-to-date, relevant and reliable for their intended use.
- Enforcement: providing effective enforcement mechanisms and dispute resolution procedures.

Although the principles are broadly equivalent to the UK standards, there are differences. For example Principle 7 of the Act requires "appropriate" security measures whereas Safe Harbor requires a "reasonable" precaution which is not necessarily as high a standard. Once a US organisation has established a privacy policy which declares its compliance with Safe Harbor principles and has decided to participate in the Safe Harbor scheme, it must self-certify its compliance in writing with the US Department of Commerce. This can be achieved by a letter which sets out certain information including details of the organisation's activities in relation to the data collected and a description of its privacy policy. The Department of Commerce will maintain and make public a list of those self-certified organisations and their self-certification letters.[9]

In global terms the meeting of two different paradigms between the United States (subjective approach) with the European Union (objective approach) then mediated by the presence pivacy OECD Guidelines, and later evolved into the APEC Privacy Framework.

[9] The US Safe Harbor scheme, http://www.out-law.com/page-8173

OECD Privacy Guidelines	APEC Privacy Framework
1. Collection Limitation Principle: 2. Data Quality Principle: 3. Purpose Specification Principle: 4. Use Limitation Principle: 5. Security Safeguards Principle: 6. Openness Principle: 7. Individual Participation Principle: 8. Accountability Principle:	1. Preventing Harm 2. Notice 3. Collection Limitations 4. Uses of Personal Information 5. Choice 6. Integrity of Personal Information 7. Security Safeguards 8. Access and Correction 9. Accountability

Need to be observed in the table above, that although generally look the same, but look different one important point, namely the APEC mentioned beforehand that prevention efforts must be guaranteed to the detriment of others first (Preventing harm) prior to collecting personal data other. In other words, it is not directly imply an interest to look at the feasibility of a system used to obtain personal data of others. In the context of communication via the Internet website, we can see it as a best practices or growing prevalence that each presenter will usually load the site Privacy Statement to its users.

VI. Privacy and Constitutional Obligations in Indonesia

Although the Constitution of Indonesia (NRI Constitution 1945) does not mention or use is expressly Privacy terminology and there is no specific law governing the protection of personal data, but that does not mean that Indonesia does not have laws that protect it as some related laws such as the Law of Personal Data. 23 of 2006 on Population Administration ("UU Adminduk"), Act No. 11 of 2008 on Information and Electronic Transactions (the "Act-ITE") and Act No. 14 of 2008 on Public Information ("UU KIP") , can be said to be sufficient to provide the obligation to perform data protection of everyone. In Indonesia, not just each individual must respect the rights of others, but also requires the State Administration to appreciate it.[10]

Looking more deeply, than 9 (nine) that protects the human rights clause contained a clause which states the duty of every person to respect the rights of others. This is also reinforced by article 27 of the Constitution that requires each person to respect the rule of law and without exception. Lowering the constitutional mandate contained chapters 29, 30, 31, 32 and article 35 in the Human Rights Act which states security of the person both in his home (privacy of the property) to the communication aspect of it does.

Meanwhile, in an electronic context, Article 26 of Law ITE has provided a wider sense, namely (i) privacy in your body, (ii) privacy in your property, and (iii) privacy in your communication. UU ITE provides certainty that the delivery and retrieval of personal data must be with the consent of the data

[10] See the Law No. 23 Year 2006 concerning People Administration.

owner is concerned. Furthermore, it is also related to the prohibition in Article 32 with the threat of punishment in Article 48 of Law ITE also provides protection for the acquisition and disclosure of confidential information by the threat of criminal prosecution following a high threat of criminal weighting if it is committed by a corporation.

Article 26 UU ITE:	Explanation of Article 26
(1) Unless otherwise provided by legislation, the use of any information through the electronic media regarding one's personal data must be made with the approval of the concerned person. (2) Any person who violated their rights as referred to in paragraph (1) may file a lawsuit for damages caused by this Act	In the utilization of Information Technology, protection of personal data is one part of the private rights (privacy rights). Personal rights implies the following: a. Private rights is the right to private life and free from all kinds of interference. b. Personal rights is the right to be able to communicate with other people without action spy. c. Private rights is the right to control access to information about one's private life and data
Article 32 UU ITE: (1) Any person intentionally and without right or unlawful in any way modify, add, subtract, transmitting, damaging, removing, moving, hiding an electronic information and / or electronic documents belonging Another person or public property;	Article 32 Self-explanatory

Furthermore, if traced back Privacy linkages with other legislation such as the Telecommunications Act, the Health Act, the Banking Act and other related laws. Thus it can be said that the Privacy is also protected existing industry. Therefore it can be said that although Indonesia has no special law on Privacy or Data Protection, but the relevant provisions can be said to have been distributed fairly set. But if we look into electronic form as well as the access and distribution through electronic systems, the data protection settings to do the details on the state administration responsible for the development and supervision of the affairs of information and communication. In other words, UU ITE following PP-PSTE and Regulation of the Minister of Communications and Information backrest can be said to be suitable for the implementation of the regulation mechanism of protection of Personal Data Privacy and Protection.

Article 29	Article 29
1. Everyone has the right to protection of self, family, honor, dignity, and rights of his 2. Everyone has the right to recognition everywhere as a person before the law wherever it resides.	Self-explanatory
Article 30 Every person has the right to feel safe and secure as well as protection against the threat of fear to do or not do something.	Article 30 Self-explanatory
Article 31 (1): The residence of anyone should not be disturbed; (2) Stepping on or entering a residence or yard into a home against the will of the people who inhabit it, are only allowed in cases specified by law.	Article 31 subsection (1): What is meant by "not be bothered" is related to the right of privacy (privacy) in his place.
Article 32 Independence and confidential correspondence relationships including communication via electronic means should not be disturbed, except by order of a judge or other lawful authority in accordance with the provisions of the legislation.	Article 32 Self-explanatory
Article 35 Everyone has the right to live in a society and a state of peace, safe, and secure, are respected, protected, and fully implement human rights and basic human obligations as stipulated in this Law. Explanation	Article 35 Self-explanatory

Based on the ideas and discussion above, then in the end I think that the first thing you should do is optimize the conditions. Redress for the losses suffered by each owner of the data, it can be said to have enough instruments modest recovery. In addition to a civil action or administrative sanctions have been there are also criminal sanctions for violations of the Privacy and Personal Data in Indonesia.

VII. Closing

Based on the explanation above, then an interesting thing happened in the development of law in Indonesia, that it can be said that Indonesia has conducted a second hybrid paradigm different between the U.S. and Europe, by marrying the two principles. The existence of the Act and the Regulation

No.82 Year ITE 2012 ("PP-PSTE"), essentially following the rule of privacy and personal data protection ala EU, but details of the mechanism and solution to the problem following the US-style expectations, which does not have to involve the government as concerned may did claim compensation directly. In implementation, it is also consistent with the APEC Privacy Framework where protection can be optimized with involvement of a professional independent agency (Institute of Competence Certification) that can examine the feasibility and the latest signal that the system is worthy of trust (Trustmark) as a known category. One category Trustmark is privacy protection reliability (Privacy Mark) as a fifth category. It has indirectly following the recommendation of APEC to implement more flexible privacy to supporting the empowerment of professionals in the field of ICT for issuing the Privacy Mark.

While waiting for the long-term establishment of a Special Law on Privacy and Personal Data, the authors propose that the existing problems can be resolved in a tactical operational regulation as mandated in PP-PSTE, the government can take public expectations as a representation of consumer interests public rather than the interests of businesses are expect more implementation of the policy of Do-Not-Call-Registry rather than opt-in policy implementation in an electronic communication.

Some recommendations can be given with respect to the formulation of policies on Privacy Candy is necessary to refer to the APEC Privacy Framework as a forum rather than a relatively more neutral than the OECD represents developed countries of course have an interest in big-legalize access their data from most developing countries. At least legally speaking, there are 5 (five) minimum Fair Information Practices Principles, namely: (i) Notice, (ii) Choice, (iii) Access, (iv) Security and (v) Enforcement.

Meanwhile, addressing the grievances against Spamming issues are still growing, it is relatively easy to solve, namely by applying PP PSTE the telecommunications network and telecommunications services in Indonesia. It actually happened because Operators was negligent in performing the duty registration and administration for the negligent conduct airworthiness applications used together with a Content Provider Operator. The problem may be seen clearly when there is a lawsuit Consumers move both personal and class action against Unlawful acts committed, and asked interim decision to the judge to dismiss the temporary services and confiscate application system is used to clarify the extent of commitment of entrepreneurs to implement its promises to consumers in the electronic systems that are running. The issue will be completed soon interrupted when the judge gives the verdict and grant full compensation claim both materially and immaterial filed. Thus the rogue businesses will think twice to do the mischief that had been impressed understandable because the permissive culture of our customers.