A GUIDELINE TO ENFORCE PRIVACY AND DATA PROTECTION REGULATION IN INDONESIA

Muharman Lubis
Kulliyyah of Information & Communication Technology
International Islamic University of Malaysia, 50728, Kuala Lumpur, Malaysia
Email: muharman.lubis@gmail.com

Mira Kartiwi
Kulliyyah of Information & Communication Technology
International Islamic University of Malaysia, 50728, Kuala Lumpur, Malaysia
Email: mira@iium.edu.my

Sonny Zulhuda
Ahmad Ibrahim Kulliyyah of Law
International Islamic University of Malaysia, 50728, Kuala Lumpur, Malaysia
Email: sonny@iium.edu.my

ABSTRACT

Indonesia has enacted the first cyberlaw, UU ITE 11/2008 as legal certainty and foothold to support transaction of electronic commerce in the Internet, within the boundaries of Indonesia. Generally, the regulation can be divided into two parts, the rule about concept of information, contract, certification and prohibition of illegal practice in terms of e-commerce through statement of remedies. In article 26 verse 1; it stated about the use of every information should be based on the user's consent. Unfortunately, the nature of UU ITE is still common and basic as fundamental law to set standard in fulfilling cyber requirement. Therefore, the primary component for electronic commerce to run smoothly resides on process of collecting the data as input to the database derived from customer submission or transaction logs. However, no clear and concrete statement in the first Indonesia cyberlaw to accommodate with this matter whereas data is the critical factor determining the successes and set inter-relationship between party. This paper will present guideline in applying privacy and data protection regulation in Indonesia, specifically in terms of commercial and administrative purpose.

Index Terms *– guideline, enforce, privacy, regulation*

INTRODUCTION

Currently, there are no specific regulations concerning the cyberspace in Indonesia until UU ITE enacted in 2006 refer to *UNCITRAL Model Law on Electronic Commerce and Electronic Signature, EU Directives on Electronic Commerce and Electronic Signature and Convention on Cybercrime* (Batan 2008). Previously, the law in Indonesia has an issue to allow the digital evidence in the court such as a document in the form of compact disk or a photograph negative whereas technology advancing for various sector like business and administrative application very effectively with paperless transactions in the form of *digital document*. It has a significant impact on the way people behave and react in their daily life and it has given rise to both benefits and costs. Other countries have regulations concerning cyberspace, such as the *Digital Millennium Copyright Law 1998* in the USA and the *Digital Signature Act of 1997* in Malaysia. The absence of the data protection act has allowed forms of data theft to go unpunished and needs to be erected to govern private data processing the processing of personal data such as in countries like Emirates, and Turkey (Hasani & Dehghantanha, 2011).

The fact that Indonesia has only single cyberspace regulations does not mean that the regulator are insensitive to accommodating technology developments and adopting business application for daily routine task. The issues focus more on result of the fact that regulations concerning cyberspace require detailed and in-depth study. It is expected to be truly on par and aligned with changes happen in people's trend as pattern of their activities. Meanwhile, the usual issues of privacy can be learned through voting process which emphasizes the importance of privacy. Based on analysis, Azhari (2005) mentioned the usual issues happened in voting implementation in Indonesia, *firstly* relate to the lack of registration process due to the residential system have improper function such as multiple identity of voters in various location that could be manipulated to increase the vote of certain candidate. The fictions voters that do not registered in that area or underage happened in certain area. *Secondly*, many invalid vote content in the verification process because of unclear procedure of marking or lack of presentation to the voters to familiarize and understand the voting procedure. *Thirdly*, each area of voting place has different speed of votes' collection cause the slow votes' count in the national tabulation that does not run as the first plan, it might due to different methodology or mechanism while voters tend to suspicious the possibilities of fraud or miscalculation in the middle. *Lastly, lack of the standard of voters' privacy protection*, it might influence the result of tabulation that does not represent the national hope.

This paper will investigate the importance of privacy protection in society and then suggest a guideline for applying and enforcing the privacy and personal data protection in Indonesia, considering the social component like norm and entities, which influence the requirement and process of development and implementation. By applying and enforcing the suggested guideline, it

is expected that relevant party handle and manage personal data as what its function should be; commercial sectors for commercial activities, administration requirement for administration purpose and identification mechanism for identification process.

BACKGROUND

The concept of privacy is admittedly elusive, which most individual would agree in the context of human right, the personal data must be protected by the responsible party. But it's hard to achieve the situation whereby everyone agree upon the limitation and restriction of privacy. Currently, the concept of privacy within the boundaries of legal system still in its development stage due to technology advancement, whereby one can state the definition of privacy in given situation but it differ in different case. Historically, Warren and Brandeis (1890) recognized the right of privacy in Harvard Law Review by their famous statement; *"Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, -- the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession -- intangible, as well as tangible."*

They also stated the importance of privacy protection due to following reason; "*Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish; no generous impulse can survive under its blighting influence.* Meanwhile, Prosser (1984) described that right of privacy is not simply a tort of one distinctive feature; instead, he argued that it is a complex of four. *The Law of privacy comprises four distinct kinds of invasion of four different interest of the plaintiff, which are tied together by the common name but otherwise have almost nothing in common except that each represents and interference with the right of plaintiff, which are 'Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs, Public disclosure of embarrassing private facts about plaintiff, Publicity which places the plaintiff in a false light in the public eye and Appropriation for the defendant's advantage, of the plaintiff's name or likeness'*. However, at that time the concept of privacy itself also broadened due to simultaneously technology use in the society, such as the case when people capture the image of certain people in the street and upload it into social media. In addition, the legal regulation must capture the essence of definition and the scope of privacy in relation with the technology use routinely of in respective country.

Considering dialectical nature of the relationship between legal regulation and social norm in the technology application, it's safe to assume that elasticity concept of privacy rights is both a reflection and an engenderment of the elasticity of the limits of private life (Ahmad, 2005). In addition, he also mentioned that better for the study of privacy use a concept that is known in another legal system as a criterion to judge the extent to which privacy is valued in the society and law under, and to determine the extent to which the law governing to protect individual privacy, the aspects of the laws governing property, contracts and crime. At some extent, public and private life in society should be considered as well. In relation with Indonesia issues in term of privacy enforcement, some indications from *Bussiness.com* (2011) that around 25 million of customer data in telecommunication has been leaked to unauthorized party. It could happen as the lacked of concern and less serious of respected organization in anticipating business expansion and maintaining the customer data. This issue was arisen if there is no proper regulation to force relevant parties' treats and protect the data accordingly, even the worst situation might happen like swindling, fraud and disguise often. To overcome the potential damage, it was difficult for BRTI as Indonesia Telecommunication Regulation Body to confront and accuse this violation if only by UU Telekomunikasi No. 36/1999.

On the other hand, the impact of privacy infringement troubled the citizen in mental and material such as when fraud with fake SMS request to send some amount of credit to certain telephone number or even some of money to specific account number. Unfortunately, many people were swindled easily by this trick especially if the SMS was sent at the right time and moment or claim to be the relatives who was '*asking for help*'. In relation with this swindle case, police urged for mobile phone user to be careful in keeping their personal data and beware with similar *modus operandi* or technique (Bussiness.com, 2011). Somehow the methods evolving quickly which exploits the vulnerabilities of current privacy protection mechanism.

The attempt of police to overcame the issues as though helpless to follow up and investigate further these cybercrime. No special authority in the current cyberlaw for police to inspect relevant institution responsible for and track the activities involved in *modus operandi* to find out the digital evidence. It is one of the primary reasons to explain the helplessness of not only police but also attorney to prosecute the privacy issues case besides the principles of data protection and no clear definition and limitation of privacy. The statement indicated not to show the 'no benefit' of the regulation in term of privacy but rather than expect the concrete guidance on what police should do to find the evidence and how the attorney prosecute the case as well as what kind of personal data is protected by the regulation. Under the data protection act 1998 in the United Kingdom, it is specified that personal data shall be:

1) *Processed fairly and lawfully and, in particular, shall not be processed unless—*
   i. *At least one of the conditions in point 2 is met, and*
   ii. *In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*
2) *Obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*
3) *Adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*
4) *Accurate and, where necessary, kept up to date.*
5) *Processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*
6) *Processed in accordance with the rights of data subjects under this Act.*

7) *Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
8) *Not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

The principles has function to set the boundaries and the important of protection so the kind of enforcement can be defined further. However, the surveillance or wiretapping as the alternatives have several factor to be considered reflected by the execution of several attempt in USA and Germany (Schwartz, 2002) such as absence of constitutional protection if a party to a communication offers her consent to state surveillance and the permit based third-party consent to searches by government bolstered a societal interest which can be hard to signed due to the necessary reason on danger or interest.

MEANS DEFINING PRIVACY AND PERSONAL DATA PROTECTION CONCEPT

Expectation

Interestingly, the complex of the organizational structure in organization usually bring a lot of confusion especially in bureaucracy, administration, allocation workload and coordination. People are the component that really difficult to handle because the necessity, needs, problem and many abstract things influence more in the people minds. It could lead to the degradation of performance, decreased of capability, internal conflict, etc. In terms of developing privacy policy meet the user expectation; the attitudinal factors associated with the people who work in the organization need to be defined in terms of intrinsic rewards and individual motivation (Leavitt,, 1965). Technology relate to the system or tools be used by institution to make easy the task involves application, software, artificial intelligent, etc. Since the technological infrastructure plays the role of the enabler, the right IT investment address the attempt for privacy protection should be enhanced for the reason of supporting. If this issue is properly being taken care, it will increase the performance and productivity. The technology is needed to accommodate the user requirement, particularly in improving the performance and capability. The enhancement of the technology should be integrated between each other, it is required if procedure imbued in the policy. Adopting the bad performance and poor capability technology will bring such disaster to the privacy protection.

Obviously, privacy policies also has the essential meaning as the approach to guide and manage relevant instance to guide in the proper manner by determining set of standards and procedure, which was developed in the form of statement or legal document. By this means, policy is a must to promote privacy among the environment, which is required the enforcement as well. Privacy policies will be diverse that is limited by specific boundaries and jurisdiction, implicated the local paradigm and perspective in defining and controlling privacy as the concept. Furthermore, Kosa (2010) argued that the available case studies presented in policy based research take a fact based approach, without examining the ethics of privacy. Therefore, privacy policies to manage or control is expected by the user is likely similar that they expected in their real life. The consent to develop the suitable privacy policy, which fit with the environment, has importance goal to protect the human assets from privacy breaches resulted severe consequences, such as humiliation, discrimination or economic hardship (Weber-Jahnke & Williams, 2011)

Moreover, the privacy policies also should take the consideration of the user, most and foremost, whether the policy influencing user behavior to support privacy or helping to make informed decision. The privacy should be clear presented with prominent information as the expectation of the user. It should take a note, that information as simple as accommodate the user's expectation. Thus, it is not necessary cover the whole area as majority user seldom to read curiously or no intention to get along with. The new regulation in the form of UU TIPITI (Information Technology Criminal Offense) can be benefit by understanding attitude and behavior to determine appropriate policies to be developed in supporting the UU ITE. The privacy policy is the beginning phase to implement the enforcement on privacy protection with providing clear authority, responsibility as well as limitation, importantly the hierarchy of the policy should be considered as well in ensuring the mandate.

Concern

The data protection act should be able to control collection, preservation, and using and implementation of personal data by any parties. Therefore, privacy of all individual data would be guaranteed by creating a set of common regulations for handling and managing of private data (Hasani & Dehghantanha, 2011). The data protection act will apply to any information or opinion which are processed by either online or offline means. Information, which is used in the data protection act, relates to a person either living or deceased and from which the person's identity is ascertainable. Information in the data protection act includes all opinions, statements of intentions, and all form of personally identifiable information both recorded online and offline. The data users will use The data protection act to regulate the usage of personal data for data subjects. The data subjects in this instance is the individual who is the subject of the personal data, while the data users are individuals, and/or organizations who controls the collection, holding, processing, or usage of any personal data.

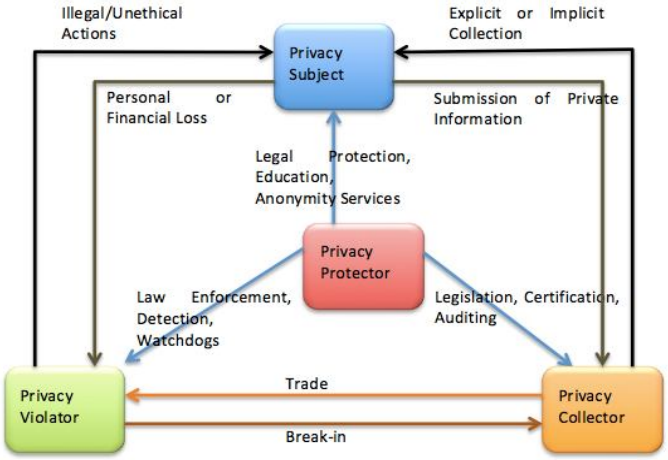
The case of category of personal data can be problematic to determine like gender and age, which can be seen in the public. Those data are important in terms of decision support making in analyzing the trend and pattern for business-oriented purpose. Those information can be extracted directly without the needs of permission from the relevant person except that they close/hide all of their body or close their face with mask to prevent somebody identify them. Still if this as the attempt they choose, everybody will be suspicious with their act, even police has the authority to catch temporary. However, problem arises if the data are not protected accordingly and reveal to illegitimate purpose lead to robbery, thievery or stalking by identifying the right time

and moment. The critics tend to attack the efficacy of privacy policies, majority concern regard the effectiveness of the implementation in the practical.

Meanwhile, the use of 'opt-in' and 'opt-out' is the techniques that describe nicely about our right to prevent or keep hidden some information to be revealed by the others illegitimately. In the case of email, when we choose 'opt-in' means we allow to receive "bulk" e-mail, that is, e-mail that is sent to many people at the same time while when we choose 'opt-out' means instead of giving people the option to be put in the list, they are automatically put in and have the option to be taken out. Therefore, the developer should provide those kinds of techniques to ensure the secret information should not reveal easily and automatically, though through various mechanism. If this became the issue, the ethical reside on the developer, but when developer already provide configuration where person can utilize it, but that person unaware of it, so the kind of responsibility reside on him/her alone. More concern in term of concept, context and content which accommodate the requirement of citizen especially in term of privacy (Lubis & Maulana, 2010).

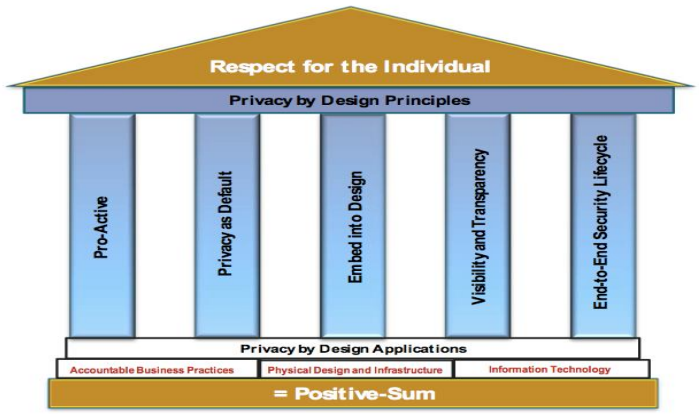
THE IMPORTANCE OF ENFORCING THE PRIVACY AND DATA PROTECTION

The proper privacy protection should follow basic principles namely '*data subject consent for disclosure and process*', '*data subject notice the description and purpose*', '*data management and control*' as well as '*information transparency and completeness to prevent misleading and misuse*' (Canon, 2005). These principles fulfill the basic rights of subject. Therefore, Government can handle this issue by approved the regulation in the formed of 'Personal Data Protection Act' as the management approach. The personal data shall not be kept for a longer period of time than it was intended for and shall not be kept longer than it is necessary for the purpose it was collected for. Withholding of data for a period that exceeds the terms and conditions as stated will be viewed as a violation of personal data, and organizations caught doing so will be fined (Ho, Dehghantanha & Shanmuga, 2010). In short, Users should be able to give their explicit consent on how to use their personal data, it should be clear be delivered by institution that responsible to that information.



Framework for Privacy Protection in Electronic Commerce (Head & Yuan, 2011)

The Government is one of the largest collectors and producers of these personal information dossiers. Virtually every major event in an individual's life is recorded in government digital paradigm. Head and Yuan (2001) explain their framework at privacy protection in *e*-Commerce, for instance, the government collects information about citizens' income and tax payments, banks collect information about clients' payment transactions and hospitals collect patient information for health care. Once the private information is gathered, it is the collector's legal responsibility to maintain its security and privacy. Internet, database and data mining technologies allow collectors to compile extensive information about individuals from many different sources. The e-Commerce has the same nature with *e-Voting* in the essence of characteristic from commodity have been using for transaction but the mechanism for protection of personal data and the approach to keep and store data is very different. The way of *e-Voting* treat the personal data strictly forbid the existence of relationship between the user and the content, so the other node is isolated in executing their function. It is really interesting to see how the legal regulation can define and accommodate the technical description of the mechanism.



Framework for Privacy by Design Privacy Impact Assessment (Jeselon, 2011)

Data is the important resource like fuel that drives the manufacture industry and organizations would malfunction of there is no data. It ensures every system and every process within the organization functions at maximum level. The use of data influencing every decision-making, risk management analysis, offers insight into markets, products testing and services, customers' relationship management, pinpoints a organization exposures, vulnerabilities and threats. Regard of privacy protection; Jeselon framework that is carried into the application of the *Privacy Assessment Principles* to an organization's information technology, business processes, physical spaces and networked infrastructure have an objective to ensure the implementation meet with the organization structure. He argued that the methodology should be applied continuously at all stages (conceptual, physical and logical) of the design and it specified the list of analysis in terms of:

1) *Description of the business purpose(s) of the application, discussion and analysis of the organization's current privacy and security policies, procedures and processes, as well as governance and accountability structures,*
2) *End-to-end description and analysis of business processes and data flows relating to the application, including a description of the actors involved in the collection, use, disclosure, transfer, retention, and destruction of PI,*
3) *Detailed analysis of the application's privacy controls (such as those for consent management, access control and audit logging/alerting/reporting, user notification),*
4) *Detailed description and analysis of the design of the application, including the security features or controls; and identification of privacy and security risks associated with the application, accompanied by proposed recommendations to mitigate, or eliminate, the risks.*

PRINCIPLES AND GUIDELINE TO ENFORCE PRIVACY AND DATA PROTECTION IN INDONESIA

Data Subject Consent For Disclosure And Process

In *Article 1 verse 12*, digital signature was meant to be the tools for verification and authentication. Privacy related closely with revealing the data or disclosure. User as the data subject has the right in the form of consent to determine to whom and what process the personal data is given the process of disclosure. So the disclosure might be unlawful even if the third party is relative or family member of the data subject, or a local authority, government department even the police. Important factor to consider is whether the disclosure is relevant to and necessary for the conduct of the user's business or objective. Being able to satisfy and fulfill the necessity meet certain condition for processing will not on its own guarantee that the processing is fair and lawful. The legality of the response must still be looked at separately. Based on the current Indonesia cyberlaw, it is clear stated the need of owner's consent to use the data in the *article 26 verse 1*, mentioned that *user has the right to store and possess the private data and information without other interception*. In relation with Islamic perspective, it was stated in hadith, *"A sale is a sale only if it is made through mutual consent."* (*Ibn Majah*, No: 2176).

Generally, it would be appropriate to disclose a staff's contact details according to an enquiry or request related to certain function for which they are responsible like performance report. But it would not be reasonable to disclose a staff's personal address or bank account details without their consent as if the relevant party do not appreciate staff's right to maintain the loyalty and trust. However, the sensitive conditions, such as information about an individual's health or criminal record must be clear the mechanism for disclosure because the potential damage greater than regular objective. Sensitive data tend to be kept close only for the sake of the owner of the data unless the permission or consent was given whether verbal or through digital signature. The nature of the consent depends on the type and importance of data. The data object is kept for certain purpose based the agreement with the subject, the appropriate to disclose the data in whatever situation by confirming to the data subject accordingly.

Data Subject Notice The Description And Purpose

In *article 3*, stated that technology is advancing and government give the clear chance for the current and future technology in serving the best to customer. To process the data, both subject and party must aware and agree towards the use of data, in terms of details objective and data driven activity. In respect, the party can inform the subject in the beginning of agreement through

contract with mentioning the important of submission their data, process in storing the data and utilization of the data. Somehow, certain condition forces the relevant party to use the data without asking for subject's consent. Although the party willing to confirm, other issue arise in the form of time management and operational cost whereas the purpose of data process relate on the interest of subject directly. In the process of daily routine like frequent back up or data update; it is impossible to inform regularly the subject in asking and waiting for their consent. This kind of issues allows the data subject to deliver the notice if they recognized the misuse. Thus, the party should plan their daily routine accordingly and put the utility and usability process, which utilize the data or the general notice, which both data subject agree upon.

Meanwhile, all possible situations in anticipating potential risk must be considered by party to prevent compromise among the employee toward the need on data function. Notice is the fundamental principle in service process in which data subject made aware a party about legal process affecting their right, obligation and duties. Within this power, data subject can charge the party as the defendant to satisfy due process if it was not following the detail and objective at the contract within agreement. It has the function to give the balance check from the owner's side to ensure that responsibility and mechanism to protect still there. By this warning, the party is expected to use the data as it is, because in the first place acquire and obtain benefits through consumer willingness to disclose personal data to ensures that essential business decisions are based on accurate, consistent and verifiable information. The details right of notice and how to issue to the party should be imbued in the personal data protection act, so data subject can ensure the personal data is protected by the party, while the party maintain the trust of the data subject in increasing their prestige.

Data Management And Control

To manage and control privacy of data, Organization for Economic Co–operation and Development (OECD) (2010), issued privacy guidelines so countries' member consider domestic policies when processing and re–exporting personal data from other member countries. It encourage the member to take appropriate steps to ensure that trans-border flows of personal data are secure. In respect, it should desist from restricting trans-border flows of personal data between themselves and other countries which do not observe privacy guidelines or conflict with domestic privacy legislation. At last, the approach expected to avoid creating legislation in the name of personal data protection which actually create obstacles to trans-border flows of personal data. Meanwhile, when collecting personal data, the data subject has the right to be informed whether it is obligatory or voluntary for them to supply personal data while there is such procedure to reports on the misconduct of personal data being processed, review the report to verify its authenticity, and send a notification unto the person that made the report and to the assailant as mentioned in the report (Ho, Dehghantanha & Shanmuga, 2010).

In *chapter 5, article 17* and *18*, it indicated the right to organizing the data in the private or public approach. However, no clear indication to determine on legal certainty of appropriate way to manage and control data, whether solely in the hand of party or lean into data subject will. As the markets change into imperfect, the volume of data to be managed is increasing, adding greater complexity to the process, in term of maintaining and transmitting. Data management has for too long been regarded as an infrastructure problem for IT, the issue is not limited in the approach use to control but also the ethics and norm. The reality is that data management is as key success in almost all IT implementation and adoption as sustainable operations as risk management. Data management is not just technology or a tool or a component – it is a business enabler. Proper data management and control can enhance the enforcement of privacy protection with the autonomy or independence attempt by respective party authorized by regulation. Personal information can be consist numerous data, it could be biographical, genealogical, historical, biological, transactional, locational, relational, or reputational, which is the stuff that makes up our modern identity. It must be managed and control responsibly.

Information Transparency And Completeness To Prevent Misleading And Misuse

Information transparency has three important element, firstly, relate to public institution process in making decisions should be understandable and open to the audience, secondly, the decisions themselves should reasonable and argumentative; thirdly, the information on which decisions are based should be available to the public with large scope and completeness means it addresses the issue in a practical, pragmatically and informative manner (EPDS, 2005). Transparency is an opportunity to increase the profits directly, communicate pertinent information to their stakeholders and at the same time become the obligation for corporations. In *UU KIP 14/2008 article 2*, it mentioned that citizen could access their interest information regard public data except the confidential data. It is the obligation and mechanism for public institution to reveal the important data to public audience as the report in justifying what has done. It has the function to evaluate the performance, whether it is accepted or rejected.

Transparency and privacy, both go hand in hand, in delivering certain benefit into the individual and by the party. In fact, individuals have the obligation to withhold and protect their personal information to have a secure life and self-determination, still not going to far in the radical way. Endorsing and supporting individual privacy and institutional transparency simultaneously is not illogical; it is common sense, though it seems overlapping, but it just a matter of understanding the approach and believes one another by setting the limitation of disclosure. Information privacy is the foundation of a nowadays society, not only because of the reason relate to damage that can occur from blackmail, identity theft, impersonation, disguise, cyber-stalking or other cybercrime. When data can be assembled into profiles, matched with other info and used to making the decision and judgment about individuals, such as whether or not to hire them, or to use invest to service or to issue a claim, or whether to calculate benefits or terms of an offer or continue the business, it should make us shudder and horrified to think that we are living in a world where all is known and nothing is forgotten.

Private Investigator Commission And Services Agency

To stimulate a healthy electronic commerce environment, privacy protection and business as well public interest must be balanced by analyzing the activities, key roles, responsibilities and information flows among the privacy parties (Head & Yuan, 2001). While the principle are imbued in the regulation, but in the context of execution and implementation are weak, the success of privacy protection will be at doom. The necessity of establishment of commission, which accept reports on the misconduct of personal data being processed, review the report to verify and confirm its authenticity and then send a notification unto the person that made the report or to the assailant as mentioned in the report are really important. The commission in investigating the notice, complaint and accusation should conduct a thorough investigation to find any means of misconduct to secure the right personal data solidly whether stated on the report or not, when the commissions investigator sees fit. The privacy commission should carry out duties actively concerning that lack of awareness or understanding of data subject. The big question arise, whether should the commission's investigation yield results of misconduct in the processing of personal data, the assailant shall in turn be fined depending on the misconduct and a notice of enforcement shall be placed unto the assailant, of which the assailant must comply, else face stern reprimand (Ho, Dehghantanha & Shanmuga, 2010). It does not seem to be a consensus over whether privacy is a public or a private right. So, The lack of consensus may contribute to the fact that strong, coherent privacy protections specifically addressing electronic health records have not yet been built into existing privacy legislation in a consistent manner (Gordon, 2010).

Codes Of Practicing And Reporting The Misconduct

The biggest concern with the current institutional approach is concerned towards the expensive of operational cost for both users and suppliers, as well as the complex mechanism in relation with the data subject. Restriction access of employee's authority in the system requires administrative support to implement the privacy protection by requests or through monitoring. In addition, user also must have immediate access to the data, though through restriction, in some instances, it can be through charged an additional fee as well. Therefore, if not design properly, these obstacles can limit the use of a data file and, therefore, reduce its scientific impact (Albright, 2011). Nevertheless, even in such cases, having ensured that the data subject know the existence and purpose of such countermeasures means that they have the capability of judging the security level of the services offered to them; aligned with transmission of such information is imposed by *the communication protocols, seeking anonymity, use of pseudonym, limited to the purpose disclosure of data, cautious use of e-mail-lists, cautious downloading of medical information, avoid installation of cookies* and *be aware of applicable legislation* (Gritzalis, 2004). The right of data subject is limited, so as the responsibility of the party. The report of the misconduct will be as the path in leading the proper enforcement of privacy protection followed by legal certainty of regulation, while the commission follow up and investigate by code of practice.

CONCLUSION

In conclusion, data subject as the person or party, who utilized personal data based on the agreement by the relevant person limited to specific purpose, excluded the obvious data that revealed automatically, the responsibility are protecting the personal data. Each person also has the responsibility to be aware about kind of data that he/she should be revealed. In modern "digital societies," privacy and confidentiality remain important values to the human realm. The obligation reside on each party whether want to make it right or not. As far as the technical solution are concerned, it should focus on ensuring the security of the communication channels, protecting the anonymity of the users, protecting the confidentiality of the information through encryption, supporting digital signatures, etc. The regulation should have privacy principle, the tools to investigate and code of practice as the proper enforcement.

REFERENCE

Ahmad, A.A. (2005). The Right To Privacy And Sunnè Islamic Law: Preliminary Remarks, Retrieved at October, 10th 2012 from: http://ahmadatifahmad.blogspot.com/2005/09/privacy-and-islamiclaw_12.html
Albright, J. A. (2011). Privacy Protection in Social Science Research: Possibilities and Impossibilities. The Profession, October 2011.
Azhari, R. (2005). E-Voting. Retrieved at 21st, October 2012 from: http://www.cs.ui.ac.id/WebKuliah/riset/hibah-B/VVCS/pdf/e-Voting.pdf
Batan (2008). UU ITE 2008. Retrieved at 21st, August, 2012 from: http://www.batan.go.id/prod_hukum/extern/uu-ite-11-2008.pdf
Batan. (2008). Tanya Jawab Seputar UU ITE. Retrieved at 21st, October 2012 from: http://www.batan.go.id/sjk/uu-ite.html
Bisnis.com (2011). Data Pelanggan Bocor, Operator akan dikonfrontir. Retrieved at October, 11st 2012 from: http://www.bisnis.com/articles/datapelanggan-bocor-operator-akan-dikonfrontir
Bisnis.com (2012). Hati-hati penipuan sms dulu mama minta pulsa kini rumah kontrakan. Retrieved at October, 11st 2012 from: http://www.bisnis.com/articles/hati-hati-penipuan-sms-dulu-mama-mintapulsa-kini-rumah-kontrakan
Canon, J. (2005). Privacy: What Developers and IT Professionals Should Know. Addison-Wesley Professional.
Data Protection Act 1998. Retrieved at October, 11st 2012 from: http://www.legislation.gov.uk/ukpga/1998/29/contents
Gordon, M.E. (2010). A Framework for the Protection of Privacy in an Electronic Health Environment. Thesis of Master, Faculty of Law, University of Toronto.
Gritzalis, S. (2004). Enhancing Privacy and Data Protection in Electronic Medical Environments. Journal of Medical Systems, Vol. 28, No. 6, December 2004.
Hasani, T & Dehghantanha, A. (2011). A Guideline to Enforce Data Protection and Privacy Digital Laws in Iran. 2011 International Conference on Software and Computer Applications IPCSIT vol.9 (2011) © IACSIT Press, Singapore.

Head, M. & Yuan, Y. (2001). Privacy Protection in Electronic Commerce: A Theoretical Framework. Human System Management, 20, pp. 149-160.

Ho, V., Dehghantanha, A. & Shanmugam K. (2010). A Guideline to Enforce Data Protection and Privacy Digital Laws in Malaysia. 2nd IEEE International Conference on Computer Research and Development.

Jeselon, P. (2011). A Foundational Framework for Privacy by Design Privacy Impact Assessment. Retrieved at October October, 11st from: http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf

Kosa, T. (2010). Vampire Bats: Trust in Privacy. Internationl Conference on Privacy, Security and Trust (pp. 96-101). IEEE Computer Society.

Lubis, M. & Maulana, F. (2010). Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia. Proceeding 3rd International Conference on ICT4M 2010

Leavitt, H. J. (1965). Applying Organizational Change in Industry: Structural, Technological, and Humanistic Approaches. In Handbook of Organizations, edited by James G. March. Chicago: Rand McNally.

OECD. (2010). OECD Privacy Principles. Retrieved at April 4th, 2012 from: http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html

Prosser, W.L. (1984). Philosophical dimension of privacy: an anthology. Privacy [a legal analysis]. Ins. Schoeman, F.D., pp 104-155. Cambridge: Cambridge University Press.

Schwartz, P. M. (2002). German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance. Berkeley Law Scholarship Repository.

Warren & Brandeis. (1890). The Right to Privacy. Retrieved at October 10th, 2012 from: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Warren, A. (2002). Right to Privacy? The protection of personal data in UK public organization. New Library World. 103, 11/12. ProQuest Education Journals, pp. 446.

Weber-Jahnke, J. & Williams, J. (2011). Beyond Privacy Policies: Assessing Inherent Privacy Risk of Consumer Health Service. International Conference on Privacy, Security and Trust (pp. 229-237). IEEE Computer Society.