AN OVERVIEW OF LEGAL FRAMEWORK FOR PERSONAL DATA PROTECTION ON ELECTRONIC VOTING 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 launched the implementation of e-KTP to improve demography data for the purpose of eliminating the data redundancy and inaccuracies data of population, which was organized by Ministry of Home Affairs. It expected to enhance the quality of the statistic to support government policy and decision-making. In aligning with this implementation, there is a tendency and wishes to implement e-Voting for next election because it offers tremendous benefit to the society especially regards speed, accuracy and cost savings. Further, the primary concern of e-Voting to protection personal data of the voters for improving the quality of election than previous one. Nonetheless, the existing regulation in Indonesia still has been sadly lacking for mechanism and techniques. This paper provides the review for current legal framework in protecting personal data in Indonesia to be used especially for e-Voting purpose. Thereby, it brings the focus towards whole aspect of situation before, during and after the election, which should be considered by legal regulation by identifying the potential threats.

Keywords*-component; legal framework; personal data; privacy protection; electronic voting*

INTRODUCTION

In this following decade, beyond a doubt, information has transformed into exchange or tradable commodity, vastly expanding into multiple transaction which has numerous purpose such as be sold, mine, to add value or stored. Somehow, it is fulfilling the same function like money, which use on commercial and wealth tools. Nevertheless, considering new technologies that rapidly change such as biometric eyes that can compromise privacy and the lack of attempt to develop concrete system to overcome the issues. The government must initiate the regulation to provide the certainty and guidance, thought the long process wait for. Further, the scheme to form an alliance between technology solution, social norm and legal regulation come into the picture wherein each of them strengthen and supports complementary. Specifically, the objectives in terms of increasing the capacity to control the circulation of information others required, manipulate psychological state and enforcement of what people should oblige or not. However, the alliance also should not overlook the nature of flexibility like the self-control of voter's option independently at their hand.

In other aspect, an individual are often willing to relinquish or provide personal information in exchange for a perceived benefits or for service without understanding what their data reveal or how they can be used by the provider such as a location services (Pedreschi et.al, 2008). It happened due to lack of awareness in realizing the importance of their own personal data. In anticipating the impact could happen when the event take places, the legal regulation must communicate with social norm actively. Obviously, regard to the privacy issue, the lack of concern in government; regulator and executor can drag to unwanted circumstances so government has to take necessary step to develop the policy against this misuse together to increase the understanding of its importance. Meanwhile, Li & Xi (2010) emphasized the reason from literature on why people disclose personal information especially in the social network, which are the desire for identification with a community and the need for self-verifying feedback from other community member. He also located that commitment and social capital is the aspects decide on how people behave, communicate and interact in the social network. To reveal the mechanism of privacy on electronic voting, the social network is the best reference after all, though it should have to test and confirm through comprehensive study later on.

Social network can be categorized similar like *e-Voting* because it has been shared the same characteristic, which focus on recording and keeping personal data securely and only can be revealed based on the user consent through notification. Other aspect need consideration by the legal regulation relate to principle of concern and benefits though it is not supposed to guarantee the quality of the services to achieve safe and secure during the transaction process. Still, in this context the clarification by legal regulation will improve intangible aspect of agent and node involved in the process. This paper will review the status of existing legal regulation that can be considered as umbrella of law for the importance and necessity of law certainty and suggest the legal framework to protect personal data in implementation of *e-Voting* in Indonesia for the alternative. It is expected to initiate the

discussion to utilize the current law in protecting personal data and justify the need to enact the relevant regulation as soon as possible.

LITERATURE REVIEW

Based on theory, Chen & Shi (2009) lists three approaches for protecting privacy that gathered from literature review; firstly, *market regulation* that has same principles with advertisement, whereby the bad privacy practices will suffer from losses of business while the good practices will attract more users. Secondly, *self-regulation* is based on traditional components of legislation, enforcement and adjudication, are carried out by the private sector rather than the government. In assuring trust of consumers for secure environment, online merchant in the context of e-commerce has two ways to participate in self regulation, which are Internet seals of approval (ISA) programs such as *TRUSTe* and *BBBOnLine* as well as specialty groups that offers guidance to organizations and business (Forman, 2008). Lastly, *mandatory government rules*, that has similar concepts with self-regulation but exclusively handle and organized by government in specific country. Each of this regulation has its own context and advantages due to concerns, enforcement, decision-making, negotiation and crosscutting issues. Therefore, it is safe to assume that kind of type of regulation exist in *e*-Commerce because the frequent transaction and numerous provider of service. The appropriate framework should be in the form of mutually reinforcing because single type of regulation is not sufficient to control.

Further, it is recognized that the specific interests or values, underpinning privacy are in many ways dependent upon cultural tradition (Taylor, 2011) as the fundamental right that need to be protected securely. So the legal regulation should address privacy based on culture perception simultaneously balancing the privacy choice of individual. Further, the issues of privacy violation before, during and after transaction became the high consideration as well. In addition, it has the evidence that there is exist communication gap in theories and practical solution (Pedreschi et.al, 2011; Greenstadt & Smith, 2005). Specifically, the issues either, it restrictively protected by reactionary legislation or it rampantly abused by profit-driven business (Greenstadt & Smith, 2005). Everyone has the right of the protection of the law such interference or attack through prove and solid mechanism with it should be aligned with current regulation. For example Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms 1950, states that:

1. *Every one has the right to respect for his private and family life, his home and his correspondence*
2. *There shall be no interference by a public authority with the exercise of his rights except as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.*

Under Indonesian law, which can be retrieved from law and human rights ministry website, Article 14 of Human Right Act No. 39 of 1999 concerning human rights states that:

1. *Everyone has the right to communicate and obtain the 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.*

Furthermore, Article 21 of Human Right Act No. 39/1999 states that: '*Everyone has the right to integrity of the individual; both spiritual and physical, and as such shall not be made the object of any research*'. Meanwhile, Article 47 of KUHAP Act No. 8/1981 gives the police permission to open private mail sent via post and telecommunications offices, with a special permit of the chief justice of the district court. Articles 38 of Act No. 36/1999 on Telecommunications states that '*Every person is prohibited from taking actions, which may cause physical and electromagnetic disturbances to telecommunications operations*' while Article 57 of Act No. 36/2009 on Health state that: '*Everyone is entitled to personal confidential health conditions that have been advanced to health care providers'*. From this example, it indicated that Indonesia current regulation and law already protected privacy although the protection spread over a several pieces of legislation differs with other countries, which protection of privacy under a single consolidates piece of legislation. To simplify the disparate of privacy definition and concept, which can be understand differently in terms of authority and limitation, one alternatives through convergence regulation that has purpose to connect all the relevant regulation and set the clear definition of terms to prevent disagreement among responsible institution. In addition, single and complete new regulation in the form of personal data protection also can be enacted and handle the issue comprehensively, which it will pinpoint and locate the targeted issues accordingly. The enactment of legal regulation is really complicated and ambiguous, especially to formulate the social norm. It requires statement of fact and agreement within the party that has interests and lists of question should be answer and negotiated like impacts, trend, pattern, benefits, budget and mainstream.

Obviously, legal regulation have been instrumental and key to protect personal information and sensitive information as well as to keep every instances remain neutral to view such cases arises. Nevertheless, the regulation in the form of content should be constantly updated and adjusted with current and future technology in mind with comprehensive discussion involves the regulator, organizations and stakeholders (Pearson & Benameur, 2010). In the sense of transaction, driven by business efficiencies and the need for a competitive advantage, enterprises are now collecting more clients' information to increase market share and to offer better services, while the hyper-growth of business and competition increases the implementation of ubiquitous and pervasive computing have created a privacy void, in which clients' information is sent over from machines to machines without the assurance of information security (Ng & Dong, 2008). This trend emerge the complicated situation where client's information became such commodities which no assurance whether that information protected or not, although there are

existing-legal constraints on the treatment of users' private data by providers, which vary according to jurisdiction. Impacts of legal regulation enactment not always in the positive direction, in worst case can lead to degrade the citizen's view on government capacity in understanding and analysing the pattern on requirement among society. It was shown on the case of enactment of first cyberlaw, which brings in bad image of government's intention because, the lack of concept, context and content (Lubis & Maulana, 2010). The question always arise if the legal regulation want to accommodate the IT subject and object, the hardest part involves in defining the jargon, term and scope that overlapping and changing easily and quickly in the meantime.

Each country has set their own regulation bind the citizens and people at that country. The issues resides which it cannot execute directly the performers out of country, even in some case, it will have some conflicts with other foreign countries' regulation, such as the case in gambling that forbid in Indonesia while in other countries allow those kind of activity legally (Lubis & Maulana, 2010). It happened because the different understanding and definition about one term as a concept subjectively like privacy. If privacy is intuitively seen as some kind of boundary that surrounds an individual and protects them from outside interference, then this automatically fosters the conditions conducive to the exercise of autonomy (Taylor, 2011). In this sense, privacy is of teleological benefit, though still appears clearly individualistic and a lack of privacy also leads to the loss of aspects of individuality and dignity (Taylor, 2011). Indeed, the scope of cases that the European Court has found to fall within the definition of 'private life' is huge and varied (Moreham, 2008). Meanwhile, even at the court has stated that private life is a broad term not susceptible to definition, when without a definition, identification of the underlying value(s) becomes of genuine practical importance if both domestic law and practice is to attempt to give respect to the right (Moreham, 2008).

An opportunity to strengthen global governance component could be as alternative in multilateral scheme of transnational cyberlaw enforcement such as agreement of extradition or multi-stakeholders public private partnership (Moedjiono, 2006). However, There is enough evidence to suggest that merely reproducing 'core principles' in codes of practice itself does not affect behaviour (Goold, 2004) but genuine knowledge of the principles has a better chance of affecting working practices. Still, the issues are not merely the lack of knowledge but the motivation resides on the people whether they agree to implement or to decide not to. The idea that privacy is based very centrally upon autonomy and its protection serves to ensure that people can set their own preferences, make their own life choices determine what the subject used to and how the object influence their daily routine. However, being individualistic means it is inevitably problematic to those who feel that its strength as a protected right is 'anti-social' (Taylor, 2011). The status of what degree or the boundaries is the fundamental issues to define and ensure the protection of privacy will satisfy or fulfill the requirement of population.

The Importance of Privacy Perception

At fundamental level, for simplicity purpose, the attempt to generalize the concept of privacy inherent to every sector can support the further discussion and perception. At health sector, the privacy breaches have the inherent attribute with the application which really critical for individual while customer expectation depend more on the hospital or health care application management wholly. It emphasized by Nayeri & Aghajani (2010) that conclude to provide education for care providers and medical students essentially, as well as patients and their families so the joint approach may be adopted by all concerned, it's not sufficient merely to issue guidelines and instructions only. From research on patients in Iran, around 50,6% of the respondents believed that their privacy had been observed on a *weak level* while 49,4% chosen the *level on good*, it also indicated there was significant correlation between some of *demographic factors* and the *level of respect for patients' privacy* while the result also highlighted that older patients' experiencing more breaches of privacy.

Moreover, a Ponemon Institute study (2010) about Americans' opinions on healthcare privacy revealed that 75% considered the privacy of their health information to be important or very important. The study also showed that Americans trusted their healthcare providers much more than any government or private IT vendor with protecting their privacy. However, a different Ponemon Institute study (2009) published several months earlier asked HIT personnel about their perception of the security of electronic PHI (Personal Health Information) in their organizations, especially in databases, and found that 61% of respondents believed that they did not have the resources to ensure the privacy and security of sensitive data. On the other hand, 70% also believed that senior management did not view the privacy and security of patient data as a top priority. Further, the study reported that 80% of the respondents had at least one data breach, which resulted in loss of PHI. Of those, 58% had two or more breaches. In a similar study authorized by the Health Information Trust (*HITRUST*) Alliance (2008), a cross section of mid-level to c-suite security executives from various healthcare entities reported that they were not completely satisfied (82%) with the overall security of health information across the industry, with most of them (79%) being very critical of the security practices of their external partners. Almost all (98%) of the executives believe the industry needs standardized guidelines for all organizations to implement while a majority (96%) also want to have a uniform way to verify whether organizations are properly securing PHI.

Kumaragu, et. al. (2006) found another interesting study from India about how social norms affects one's perception of privacy. He observed and found that less awareness of privacy were identified among Indians compared to Americans. The American respondents have more sophisticated understanding of privacy than Indian respondents. Furthermore, the subjects in India mostly related privacy to personal space and subjects in the US mostly related privacy to information privacy. Most of the US subjects related privacy to some form of control of information or data protection. On the other hand, Indian subjects related privacy into physical, home and living space. It also found the differences in the awareness of and concerns about privacy and technology. US Subjects were more concerned about computerization of data than the Indian subjects. Subjects in the US discussed specific privacy issues related to the computer and Internet privacy. At summary, it concluded that the difference might be attributable to differences in the technology penetration and high frequent US media coverage of privacy issues.

Based on evidence from literature review Nayeri & Aghajani, 2010; Ponemon Inst. 2009 & 2010; HITRUST, 2008) the developed and developing countries has different views in defining the importance of privacy, though it will be same agreement on privacy as important. The lack of concern to implement privacy and personal data protection in developing country has added other obstacle for privacy protection. Due to public opinion, which view privacy as the secondary priority or the environment that shape the privacy concern as the communal interest, the government and organization approach drag to bad approach in delivering the service and concern relate to privacy. Even though the regulation has enacted and implemented, but the problem in enforcement, negotiation and decision-making prevent privacy and personal data protection to be successful implementation. The overlook on privacy principle in system development in mostly developing countries can bring the emergency situation at national level; to many attributes at stake and government as well the citizen should aware of this situation before the condition become worst than ever. The active participation from all element of the society and cooperation from the provider and coordination from government will decide the effectiveness of legal regulation.

The importance of the perception is clearly showed in defining the concept privacy. The legal regulation as the tools or approach to set the standards for the purpose of control and monitoring the citizens should align with privacy perception into their content to prevent the conflict or clash. The attempt of enforcement to protect the personal data can be through punishment or reward. However, if the strategy or mechanisms of the protection do not connect with the citizen perception, it will be fail in the implementation phases. Support from citizen is essential in developing legal regulation, as the nature of law is to accommodate the issues arises in the community as part of society so the life will run smoothly and peacefully. After identifying the privacy perception, the scheme take a step further to optimizing the ways of legal regulation operationally to incorporate the social influences and behaviour through utilization of current legal regulation based on the function and the coordination from government to community and to the society.

Privacy Legal Framework in Indonesia for Electronic Voting

In accordance of today's conflict trigger by 9/10 in USA or Mumbai incident in India, people tend to assume that security overlap privacy. One should reveal their personal information even when contrary with their consent for the sake of nation security that no basis to justify. The trend was quite exaggeration pulled by the phobia among citizen about their life safety that somehow, this exploitation has been neglected the importance of privacy as the nature of human. In this sense, government must take critical role to organize personal data of citizens and other relevant data as the pre-attempt for harm-prevention or errors detection, to avoid the worst case happened. It is not like no willingness from citizen to reveal their personal data for greater good, but the attempt of government to maintain and keep the record remained secure among medium or channel so the objective according to the agreement and concern unless there is notification or negotiation further for dealing certain issues.

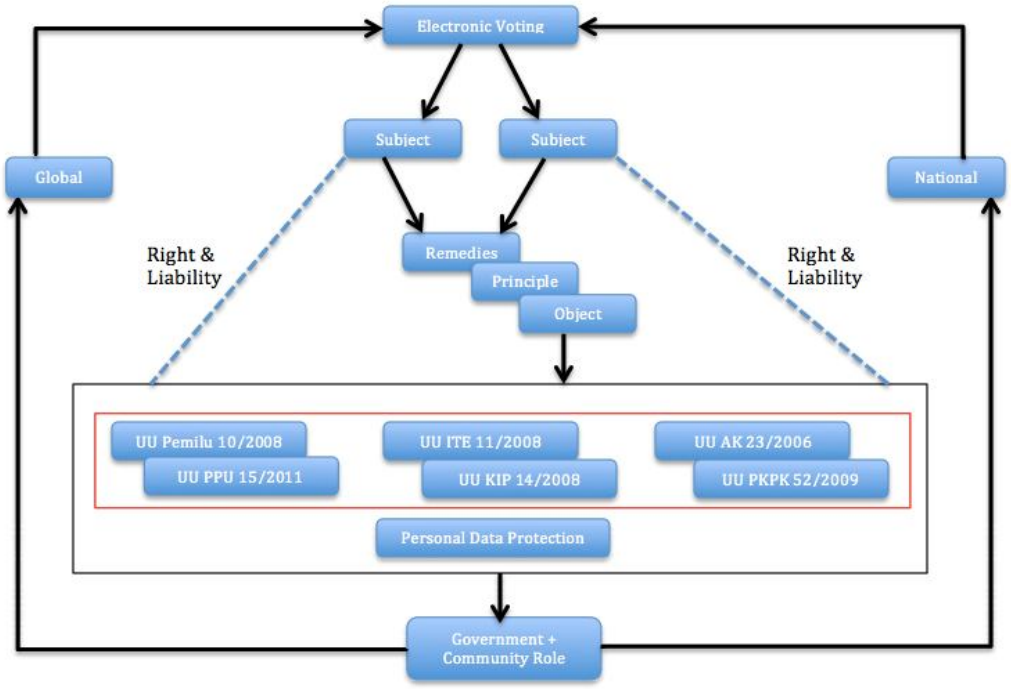
The idea to enhance trust into privacy could be absurd but not impossible. Therefore, the attempt for the alignment could be done by balancing different interests and expectations from different entities, which have relation, on how to set the definition of balance and factor influences as well as the mechanism. Moreover, the legislation and standards that help regulate these innovations often lag far behind, especially as it pertains to the security of data and privacy (Mather, et. al., 2010). Individual concerns about organizational privacy practices are found to have four dimensions: collection, unauthorized access, errors, and secondary use (Stewart & Segars, 2002). Different opinions on privacy are further enhanced by cultural differences and individual autonomy. Services and data-storage can be located in any part of the world so users of technology will have to deal with the different cultures predominating specific locations (Timmerman, et.al., 2010).

Based on Indonesia regulation (UU No. 3/1999) about general election (PEMILU), it clearly states the basic principle of Indonesia election based on Luber & Jurdil, which stand for *Langsung (Direct), Umum (General), Bebas (Independence), Rahasia (Secrecy), Jujur (Trustworthy)* and *Adil (Fairness)*. *Langsung (Direct)* means every citizen that has right to vote by themselves without medium in selected area as their wish. Then, *Umum (General)* means every citizen has the right to select their candidate or become candidate to be selected if the requirement has been fulfill such as age and nationality without discrimination. Meanwhile, *Bebas (Independence)* refer to the right be assured by regulation that no one or things forced them to select the things that contradict with their wish. On the other hand, *Rahasia (Secret)* relate to assurance that the vote content is protected and secured so no one can reveal during election process while *Jujur (Trustworthy)* refer to all component include people, government, party and administration must behave as the current procedure and regulation. Lastly, *Adil (Fairness)* relate to the equal treat to every concern without deception.

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 *e-Voting*, technology relate to the system or tools be used by government to make easy the task involves application, software, calculation, tabulation, data transfer, privacy protection etc. Since the technological infrastructure plays the role of the enabler, the right IT investment need to address the legal regulation interest while at the same time the capacity should be enhanced. If this issue is properly being taken care, it will increase particularly, the performance and productivity where it accommodates the user requirement. The enhancement of the technology should be integrated into the system based on regulation such as authorization in tabulation or information transparency.

In the context of concern and benefits, Ritchie (2009) explained, there might be an expectation on the citizen's behalf that unless they commit an offence, their presence will be ignored and the footage will be retained only with the strict condition affecting access. On the other hand, there might be a perceived issues pertaining to personal safety relating to non-compliance. The

development of regulation to be comprehensive and the arrangement to be right on the target should catch the requirement on the citizen behalf. In addition, two perspectives to characterize between legal regulation and social norm; the *external aspect*, which is self-verify and self-govern of citizen through obedience regularly whereby the impact of violation come from society like isolation; and the *internal aspect* which emphasize in term of individual cognitive in the sense obligated to follow the rule, otherwise influence the quality of reflective attitude. Meanwhile, from this internal aspect legal regulation acquires its normative quality to deliver the motivation from individual internally. Another issues in justify the framework relate to ranking of regulation and rule of recognition; the dilemma of primary and secondary rule of uncertainty about what the law is used and its criteria of validity, In addition, the rigidity of rules, which in certain case can be change or updated that allows legal regulation to be varied and last problem on how to resolve legal disputes or settlement through mediation from which rules of adjudication arise.



Legal Framework for Privacy Protection in Implementing Electronic Voting in Indonesia (Adopted from Makarim, 2005)

The disparate location of regulation, which disperse in multiple regulation where specify the rule on personal data protection will influence the efficiency. There are some of solution can be offered to solve this issues such as through the enacting of convergence regulation that its function to connect all relevant personal data protection verse and close the gaps of communication between regulation. Another method, by through single regulation that focus on in the form of *personal data protection* act as guideline and procedure. In organizing the Indonesia election, the committee will follow the standard regulations, which are UU Pemilu 10/2008 on election and UU PPU 15/2011 on the implementation. Besides those regulations, the regulation that has connection with election implementation should be considered with, such as on population record like UU AK 23/2006 on administration and UU PKPK 52/2009 on population development as well information regulation such as UU ITE 11/2008 on information transaction and UU KIP 14/2008. Therefore, those regulation mention above have not been considered specifically on privacy as the primary concern in terms of protection even though, at article 26 of KIP Act No. 39 of 1999 discuss about *the responsibility to do mediation and adjudication on public information*, it stated limited only on the information which government should present to the society but personal data of community remains untouched. The question arises; if the personal data has stored by third party out of government circle or independent institution, which government has limited authority. In this framework, we argue that coordination with respectable act as the high priority. The multi-dimension in explained some term in some situation could be varied, but the control in time of election in the hand of *Komite Pemilihan Umum* (KPU). The role of KPU is important in ensuring privacy protection exist in the e-Voting. Moreover, the time constraint need by the house representative in discussing the solution in terms of suitable act lead to another problematic situation. The participation from community and government determine the effective of the regulation, therefore, it should be clearly state the boundary and the definition of privacy, at least the minimum requirement based on perception from community and society. In this framework, it emphasizes on three point need to be formulated in ensuring privacy protection is aligned with legal regulation, which remedies, principle and object. Those three point should be clearly state and define in determine the standard and limitation of the rule and scope of privacy protection that government acknowledge with.

Mostly, the government of developed countries adopted the previous principle in the global institution or from developed countries. In sense they plan to increase the awareness and cooperation from society, as well the continuity of information flow and spread among themselves which government cannot neglect at all due its importance, like encouraging the community with remedies is one approach can lead to successes of implementation which ask the active participation among citizens involves rewards, campaign, incentive, subsidizes or even punishment. However, the common issues of developing countries relate to the

society, which have not thought about the privacy as the priority due to perception on privacy itself or its myth. Likewise, many myths of privacy is understood by community such as privacy protection cost too much or complicated to used, the privacy standards will hinder the convenient of technology, only relevant person need to take care about privacy, the existing device is secure enough, etc.

The attempt to awaken the awareness and understanding of privacy should touch the trend and issues arise in the society. Particularly, the fundamental idea of privacy already covered through existing regulation by developed countries or global institution but the implementation and perception might be different between each society. In aligning with these, the government should explore the circumstances and factor influence on the society. The enforcement to the society is the primary goal of legal regulation and it can be executed effectively if the arrangement consider characteristic of object on the society which the regulation want to take care of, especially in terms of right and liability. The nature of object in privacy protection act focus on attribute and properties of personal data, whether the process to maintain, transfer or change follow the procedure. It has the function to give clear picture to the responsible party to respect the right of the user as the subject together with related personal data. Any misconduct and violation can be categorized as the obedience and user can sue and claim to the court for breaking the rule. However, the right and obligation between user and organization should be balance fairly, whereby no party get more benefits rather than the other. Furthermore, the legal frameworks in implementing *e*-Voting in Indonesia can be guided through this path with following existing relevant regulation, while the mechanism will be authorized by other regulation derived from election committee or ministry rules based on its hierarchy. Therefore, the importance to accommodate by single regulation in the terms of Personal Data Act or Convergence Act is really essential due to efficiency reason of regulation. The practice of execution on personal data protection act in global or national level can lead to develop the responsible act comprehensively, either through convergence or single entities, even other alternatives approach.

CONCLUSION

The formulation of legal protection derived from accumulation of the requirement on the society. The supports from each single entity of society determine the path of the protection to be brought though government determine the standards. The privacy is like double edge sword, which has the advantages and disadvantages, so the legal framework must behave like holster to prevent the potential damage not only comes from society but also from government institution as well. This overview of legal framework in implementing e-Voting has objective to take initiative step to close the gap between rapid changing of technology and the passive state of legal regulation. The different characteristics between two-essential elements in protecting privacy cannot be accused as the main obstacle but they should be utilized effectively. The privacy perception as the ingredients of social norms is the leading path can be considered before exploring more in developing the suitable legal regulation that will be comprehensive and satisfied enough.

REFERENCES

Canon, J. (2005). Privacy: What Developers and IT Professionals Should Know. Addison-Wesley Professional.

Chen, X. & Shi, S. (2009). A Literature Review of Privacy Research on Social Network Sites. *International Conference on Multimedia Information Networking and Security* (pp. 93-97). IEEE Computer Society.

Depkumham. (1981). UU Republik Indonesia No. 8 Tahun 1981: KUHAP. Retreived At January 4th, 2012 From: http://www.djpp.depkumham.go.id/inc/buka.php?czoyODoiZD0xOTAw KzgxJmY9dXU4LTE5ODFidC0xLmh0bSI7

Depkumham. (1999). UU Republik Indonesia No. 39 Tahun 1999: Hak Asasi Manusia. Retreived At January 4th, 2012 From: http://www.djpp.depkumham.go.id/inc/buka.php?czoyNToiZD0xOTAw Kzk5JmY9dXUzOS0xOTk5Lmh0bSI7

Depkominfo. (1999). UU Republik Indonesia No. 36 Tahun 1999: Telekomunikasi. Retrieved at January 9th, 2012 from: http://denysetia.files.wordpress.com/2011/09/uu-36-1999- telekomunikasi.pdf

Depkominfo. (1999). UU Republik Indonesia No. 14 Tahun 2008: Keterbukaan Information Publik. Retrieved at April, 10th 2012 from: http://www.pppl.depkes.go.id/_asset/_regulasi/UU14th2008_ttg_KIP.pdf

Depkes. (2009). UU Republik Indonesia No. 36 Tahun 2009: Kesehatan. Retrieved at January 10th, 2012 from: http://www.depdagri.go.id/media/documents/2009/10/13/UU_No.36- 2009.doc

European Convention. Retrieved at February 20th from: http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7a/0/englishanglais.pdf

Forman, A. E. (2008). *E-Commerce Privacy and Trust: Overview and Foundation*. (pp. 50-53). IEEE Computer Society.

Greenstadt, R & Smith, M. D. (2005). *Protecting Personal Information: Obstacles and Directions*. Fourth Workshop on the Economics of Information Security (WEIS05) 2005.

Goold, B.J. 2004. *CCTV and Policing: Public Area Surveillance and Police Practices in Britain* Oxford University Press.

Health Information Trust Alliance (HITRUST). (2008). *Report, A need for a common security framework: Survey of attitudes towards information security in the healthcare industry*. Retrieved at February 20th from: https://www.mercy.edu/ias/POST%20DEFENSE%20THESIS%20- %20Is%20HIPAA%20Ready.pdf

Kumaraguru, P., Cranor, L. F. and Newton. E. (2006). *Privacy Perceptions in India and the United States: An Interview Study*. Retrieved at March 3rd, 2012 from: http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf

Li, X. and Xi, C. (2010). *Factors Affecting Privacy Disclosure on Social Network Sites: An Integrated Model*. International Conference on Multimedia Information Networking and Security.

Lubis, M. & Maulana, F. (2010). Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia. *Proceeding*

3rd International Conference on ICT4M 2010.

Mather, T. Kumaraswamy, S. and Latif, S. (2009). Cloud security and privacy: An enterprise perspective on risk and compliance. O'Reilly.

Moedjiono. (2006). Internet Governance in Indonesia. *Internet Governance Forum Athens, Greece*. October 30th – November 2nd 2006.

Moreham, N. 2008. 'The Right to Respect for Private Life in the European Convention on Human Rights: a re-examination', *European Human Rights Law Review*, 44.

Nayeri, N. & Aghajani, M. (2010). Patient's Privacy and Satisfaction in the Emergency Department: A Descriptive Analytical Study. Nursing Ethics, 17 (2), 167-177.

Ng, R. & Dong, L. (2008). *A Case Study: The Deficiency of Information Security Assurance Practice of a Financial Institute in the Protection of Privacy Information. Proceedings 1st International Conference on Ubi- media Computing 2008.*

OECD. (2010). OECD Privacy Principles. Retrieved at April 4th, 2012 from:http://www.oecd.org/document/18/0,3746,en_2649_34223_181518 6_1_1_1_1,00.html

Pearson, S., & Benameur, A. (2010). *Privacy, Security and Trust Issues Arising from Cloud Computing.* International Conference on Cloud Computing Technology and Science (pp. 693-702). IEEE Computer Society.

Pedreschi, D., Bonchi, F., Turini, F., Verykios, V.S, Atzori, M., Malin, B., Moelans, B. and Saygin, Y. (2008). *Privacy Protection: Regulation and Technologies, Opportunities & Threats.* F. Giannotti and D. Pedreschi (eds.) Mobility, Data Mining and Privacy. Springer-Verlag Berlin Heidelberg 2008.

Ponemon Institute, LLC. (2010). *White Paper, Americans' opinions on healthcare privacy*. Retrieved at 19th, February 2012 from: http://tinyurl.com/4atsdlj

Ponemon Institute, LLC. (2009). *White Paper, Electronic health information at risk: A study of it practitioners*. Retrieved at 19th, February 2012 from: http://tinyurl.com/46z5vn5

Ritchie, D. (2009). Is it possible to define 'privacies' within the law? Reflections on the 'securitisation' debate and the interception of communications. International Review of Law, Computers & Technology Vol. 23, Nos. 1–2, March–July 2009, 25–34

Stewart, K.A., and Segars, A.H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1), pp 36-49.

Taylor, Nick. 2011. A Conceptual Legal Framework for Privacy, Accountability and Transparency in Visual Surveillance Systems. *Surveillance & Society* 8(4): 455-470.

Timmermans, J., Ikonen, V., Stahl, B.C. and Bozdag, E. (2010). The Ethics of Clound Computing: A Conceptual Review. 2nd IEEE International Conference on Cloud Computing Technology and Science.