TELKOMNIKA, Vol.15, No.1, March 2017, pp. 512~521
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v15i1.3804

Privacy and Personal Data Protection in Electronic Voting: Factors and Measures

Muharman Lubis*[1], Mira Kartiwi[2], Sonny Zulhuda[3]
[1]Telkom University, Jalan Telekomunikasi No. 1, Bandung, 40257
[2,3]International Islamic University Malaysia, 50728 Jalan Gombak, Kuala Lumpur
*Corresponding author, e-mail: muharmanlubis@telkomuniversity.ac.id

Abstract

In general, electronic voting as the technology advancement offers the opportunities to reduce the time and budget of implementation which present the greater advantages than traditional approach. It seeks establish the privacy framework in the context of electronic voting that aligns with the mutual comprehension of relevant factors and measures. The result found that privacy concern and perceived benefit have influenced personal data protection significantly. The success and failure of electronic voting implementation depend on the fulfilment of the voter needs on privacy and personal data protection.

***Keywords**: personal data protection, privacy framework, factors, measures, electronic voting*

1. Introduction

In common law, the recognition of privacy right has been evolved gradually based on certain circumstances, context and interest in respected country and without a doubt due to the significant effect of an essay [1] published in Harvard Law Review. Actually, the protection of privacy as the right has began long time before in British common law but limited only as physical aspect, then spiritual nature of feelings and intellect. Despite plenty of literature surrounding the concept of privacy, indeed, it has been devalued by the society until it became serious consideration as legal term [2]. In international document, article 8 of European Convention on Human Right (ECHR) on 1950 play a role to set a foothold to enforce each signatory country protects the individual privacy. Meanwhile, the 1990 Cairo Declaration on Human Rights in Islam signed by Muslim countries confirm the recognition of privacy rights as the essential for human being existence in more countries than before, which stated in article 4 and 18 (b). Hence, organization must find proper approach to manage personal data according to existing and complementary privacy regulation by considering the accessibility and usability of the data [3].

Over the years, there have been major changes in the way election system evolves on the casting the votes with an ideal voting technology would have four attributes: anonymity, scalability, speed, and accuracy [4]. Thus, all voting technologies involve translating the voter’s intent in some way, many of them multiple times and at each translation step accumulate the errors. Paper ballot or optical scan (marksense) has been used in elections for roughly two decades, as the systems that require voters to record their votes on a paper ballot then insert the ballot into scanner [5]. It employs a ballot card on which candidates and issue choices are pre-printed next to an empty rectangle, circle, oval or an incomplete arrow while voters record their choices by filling or completing them. Then, the voters either place the ballot in a sealed box or feed it into a computer-tabulating device at the precinct. The tabulating device reads the votes using "dark mark logic", with computer selects the darkest mark within a given set as the vote choice.

Election is a formal approach of democracy by certain population of specific location to choose the one to hold public office or government service in the state of legislative, executive and judicative. It became really critical in conjunction with the direction and changes of power, which implicated the neighbours region through specific principle for communication and interaction. The essence of democracy that offered to citizens in the form of election emphasized three important points which are determined by the voice of citizens, be supported from the hand of citizens and to serve in the sake of citizens' benefit. Therefore, many countries

Received May 1, 2016; Revised July 29, 2016; Accepted August 8, 2016

has been adopted democracy system as their political instrument to run their public service even though at some aspects there is major or minor differences of implementation such as the hierarchal power, responsibility limitation, aspiration channel, rights of leader, legal interpretation and so on.

In world of computation and digital, individuals are encouraged to recognize and establish a line that mark the limits or boundaries of their preferences to reach an agreement and compromise solution about their privacy status in particular context or spaces. The interactional and behavioural attitude has been found to be effective as first step for developing theoretical framework and observational studies in privacy protection, which concern to the IT utilization and adoption, or be associated to the interactive and dynamic communication in social media. While this perspective has proved reminiscent and suggestive, there remain significant to discuss the way to transform the ideas and the consequences in this context into actual application. Practical solution involves by designing the guiding to avoid privacy invasion (privacy aware design), privacy management mechanism (privacy enhancing technology and disclosure control), privacy implication and evaluation towards information system (privacy impact assessment) and interpersonal privacy practice assistance. In electronic voting context, many researches focus on the practical solution to deliver the suitable and fit mechanism to enhance the privacy protection with specific circumstances but lack of managerial aspect wherein the majority of electoral fraud can occurred from outside coverage of technical issues. Indeed, the theory cannot necessary to be remained same in different circumstances or actor, there is a high possibility to go to wrong direction considers the diverse relationship and interaction that might be dependent each other and complementary like thread tied together. Thus, this study explores the privacy framework to support personal data protection in electronic voting in terms of managerial, technical and enforcement.

2. Literature Review

2.1. Hyperpersonal Framework of CMC

Over decades, many academicians have been investigated social psychology aspect of computer-mediated communication (CMC) since the Internet takes place in the daily life for various purposes. One concern assumed that CMC as insufficient approach for individual to share intense feeling, much less create substantial and lifetime interconnection impression of social norm toward decision making, which is restricted by the lack of nonverbal cues, immature etiquette and depersonalization process [6]. Meanwhile, others described CMC as an approach as the prompts filtered out important aspects of face to face communication derived from the assumption that computer has a small social presence acquainted with paralanguage-pitch, intensity, stress, tempo, volume lead to social vacuum [7]. They identified that replacing CMC for face-to-face communication will give inevitable changes in inner and outer variables of personal. In the end, the present research is concerned with advancing a particular model used in CMC since 1996, which is the hyperpersonal model [8] that the model observe four components of the communication process to explain how computer mediated may influence the message construction and reception due to receiver process, among message senders, attributes of the channel and feedback effects. In addition there are many attempts to challenge, support and added the model claims with fifth component extensions to be applied in new social and dynamic condition innovatively. Schumaker [9] describe them to explain how individuals communicate interpersonally online and added that the theory provides the alternative as to how individuals identify themselves in a particular surroundings or conditions with special ways unlike the others to introduce the self to others. Meanwhile, it also explains both inner and outer side of their arrangement of group that measure that individual, as well as the interaction process, which may produce an expanded cycle function of exaggerated relationships.

2.2. Privacy Calculus Theory

During this past decade, academicians consumed a vigorous amount of time and attempt to investigate the factor that respresent the individuals' behaviour. This theory describes a particular method of reasoning and calculation system that majority of individuals prioritize to obtain profit and the effort of uncovering personal information before execution process of disclosure and during the decision making. Unfortunately, most users often undervalue the risk potentiality by having in the mind that it would not happen [10]. This observation was supported by their findings with the objective to analyze the mental state of the user on the privacy concepts by aligning norms, principles, confidence and orientation into developing conceptual and theoritical framework. Moreover, the result stated that an increase of user perception towards privacy risk in Internet is correlated to a decrease of inclination to present personal data as commodity in the Internet. Prior research in e-commerce has show constructive relationship between perception on the risk and privacy concerns but they considered personal curiosity to be an essential reason based on an acceptance to have interaction in particular activity that stipulate self-fulfilling satisfaction, which is expressed by the level of cognitive feature. After all, the current theory of calculus can be view as extension theory from Culnan and Armstrong [11] that argued, in the more detailed context of transaction that individual decision making derived from the process of acquiring their personal information to complete or seal the agreement. When consumers are acknowledging the intention and the purpose of personal data disclosure, they tend to perceive the process to be fair and acceptable so they agree to cooperate. In terms of the privacy calculus, the advantages connected to the self-disclosure must be differed strikingly with the cost of privacy. Privacy costs can be classified under privacy concerns, which individual assessment is significant in the process, while at the other hand, trust become the concept that influence self disclosure [12].

2.3. Privacy Trade-off Relationship

Over decade ago, there is no one would believe that certain individual will be willing to share their confidential information to the stranger, even their sensitive or secret information like health record or credit card number. Solove [13] says the 'nothing to hide' argument that supports the government policy where surveillance does not undervalue privacy itself and excuses any government attempt to monitor its citizens' activities. There are many arguments, which he uses to counter the first, such as "*Show me yours and I'll show you mine*", or "*I don't have anything to hide. But I don't have anything I feel like showing you, either*", confirming that government intrusion is only warranted by illegal activities. Meanwhile, the privacy trade-off issues is not limited on the security sides, Sloan and Warner [14] mentioned that the privacy trade-off important task to balance that relatively short list of benefits against the loss of informational privacy as potential risk with the ability to control the information about personal details though there is some restriction by the provider. They also emphasized in reality, notice and choice leaves trade-off issues and subsequent uses of personal information largely to the discretion of private business can deliver and concluded that the decision making by comsumers to refuse to give their personal data can bring large negative qualities for societies to harvest the benefits of Big Data and citizen’s privacy. Unfortunately, the policy makers and relevant person in privacy realized the privacy-trade-off issues, but they neglected them.

2.4. Privacy Protective Behavior

Self-regulatory policy in various countries somehow requires consumers to be responsible and be part of the process of privacy and security process that be represented into their appropriate behaviour [15]. They support the attempts for the consumers to have understanding of online security and privacy risk on the issue of what is happening to personal data, what tools are available to protect them, and what kind of skill to response. Therefore, for consumers to be aware of the situation, or acquire such sophisticated skill to adapt with the changes of technology evolution takes a lot time and effort of education. Indeed, consumers face the consistent and continuous privacy and security threats, when they decide to have Internet as their backbone to do shopping or other activities. Thus, they suggest that the examination to understand perception with experience affects the decision to engage in specific behaviour is essential predict the outcome of certain regulated strategy as well to anticipate the implication to the public domain. On the other hand, Walther [8] stated that individual interpret others' feedback in social interactions to establish understanding of others, which essential to develop relationships. Thus, electronic social support entails some changes in the delivery of these functions. Meanwhile, Kosa [16] mentioned that trust has a positive correlation to privacy while privacy has a negative correlation to trust.

2.5. Personalization Privacy Paradox

There is an extensive opinion in the virtual communities that the latest generation are less aware on the privacy preferences compare to the older people. For example, Facebook founder

Mark Zuckerberg justified that privacy is no longer a social norm, which user prefer to change the privacy settings from default to others to give permission to everyone to view and look for any personal information in social media [17]. Even though most user agree upon the importance of privacy but they do oppositely. Unfortunately, majority websites have become so attached to be part of everyday users, which they regularly should present their personal data to be acknowledge in the interaction, though certain website do not have proper and sufficient privacy controls. At some occasion, consumers also say that they concern with privacy and security issues but in reality they still divulge personal information paradoxically [15]. Privacy paradox is commonly exist due to the emergence of Social Media, which mostly teenager want to be exist and be participated in the social interaction but using digital approach. They do not have reluctancy to share their private lives online, presenting enormous amounts of personal data for various purposes, especially to obtan self-sufficiency. Meanwhile, arguably, older peoples and academicians have fought extremily hard to keep personal data remain private, as they aware of the consequences of revealing information in the Internet and understand the public nature to bring its implications to future lives [17][18]. Paradoxically, government agencies and marketers are also collecting personal data about consumers for various reasons like surveillance, analytic, comparison or decision-making process.

3. Hypothesis Development

3.1. Legal Regulation

The principle represents a collection of values that direct the conduct or set a rule of a concrete society. Thus, the law create an act of action that is morally bound in the individual's mind based on the accepted values in the society. Supposedly, the individual freedom as primary reason that fulfil the purpose without persuasive practive through socialization process although the use of principle tends to be ignored. Meanwhile the limitation to communicate to particular audience will reduce the ability to express the idea and concept, make the mass media as the primary way to convey political statements and campaign messages [19]. In short, as the number increases in the electoral area, the effective communication of conveying the solution to the issue will most likely decrease. Actually, there remain a distinct gap between practice and principle, which the existence of political interest play significant role to create confilict over the privacy rights and the freedom of choices [20]. The intentional enforcement to certain policy, which develop unpleasant experience to the specific community should be considered as undesirable condition and huge mistakes though at certain point it can be justified legally but not ethically. In the absence of good reasons for inflicting punishment on individuals convicted of crimes the various actors of the criminal justice system are ethically culpable [21]. Arguably, the enforcement of regulation is not necessary encourage punishment but it could focus more in the prevention action or deterrence by prevent worst case scenario through preparation, training and education programs by motivating the execution with rewards, subsidiary, incentive or relaxed inspections to participate in the program firmly [22]. Thus, the function of the regulatory agency has moved toward collaborated approach between relevant parties by assist and support them for obeying the existing regulations.

Hypothesis 1*: Legal regulation significantly influences the concern of privacy.*

Hypothesis 2*: Legal regulation significantly influences to perceived benefits.*

3.2. Social Norm

Consent from data owners to utilize personal data is indeed, the most essential requirement to decide on the approach and technical aspects on how the data should be processed. Generally, for them to be meaningful, the individual acknowledgement should be aligned with the understanding of the execution and utilization method, which present clearly what kind of content refer to. On the other hand, it will be meaningless if the individual do not have option to accept or reject the data process at particular stage [23]. Therefore, the quality of intense, interest or approval as the enthusiasm from both sides, either the individual or the committee will determine the successes of privacy protection. Originally, Hyman [24] thought that socialization primarily as one facet of social structure and crucial to society because it was the means by which political values perpetuated themselves across generation. His approach provided two important arguments on social norm that (1) should be devised primarily as process by which social institution instill political values, rather than as a tendency process by which inherently different individuals create their own version of political determinations, and (2) due to social institutions and agencies shift more slowly than the individual, the social norm unavoidably plays as a brake to reduce the movement that decelerate abruptly. Primarily, he defined socialization as the learning of social patterns corresponding to certain issues of social position as mediated through various agencies of society. In addition, Merelman [25] stated that the structural characteristic and comparative importance of socialization agencies change spasmodically, which universal sequences of socialization can be postulated only if the investigator believes that individual maturation follows a more or less repetitive course dictated by characteristic interaction between environmental constraints or facilitations and developmental uniformities.

Hypothesis 3*: Social norm significantly influences the concern of privacy.*

Hypothesis 4*: Social norm significantly influences to perceived benefits.*

3.3. Technology Solution

Enormous amount of data is process through storing or transfering from various location to multiple or single location to allow the tabulation process. Therefore, large volume of data would likely attract the huge attention from hackers, intensified technical failure and mechanical impact and high probability of violation of transparency principle, which unconsciously present information collection about voters' personal data in sophisticated form [26]. On the other hand, there are also accessibility-related and velocity issues arise that should be considered as well to avoid worst case scenario. Meanwhile the server should has a repository to verify and validate the priviledge by authentication and authorization policies that mention the resources and the requirement for relevant user to provide, of course the process should be certified by particular independent institution [27]. On the other hand, Vrhovec [28] emphasized there are four aspects to manage data privacy risk as safeguarding personal information to be protected in its lifecycle involves business process, technology, governance and policy. When voting takes place in an electronic environment, the possibility of fraud is unavoidable since ensuring the trust is not an easy task. Thus, individual verifiability is important to raise public trust in *e*-voting [29]. Enabling human verifiability of secure system operation is an important goal for any secure system implementation [30]. Meanwhile, secure voting can be implemented by granting voters full control over which data is actually checked by an application through the using of the identity card. Hence, unjustifiably and unauthorized access of data on the utilization process, in which have implication to the results can be prevented [31].

Hypothesis 5*: Technology solution significantly influences the concern of privacy.*

Hypothesis 6*: Technology solution significantly influences to perceived benefits.*

3.4. Privacy Concern

Dalager [19] noted about concern issue in election context by summarizing that the actuality and degree of voting issues in specific setting of election based on the context can be controlled by certain factors, which related to the effectiveness and efficiency of communication process. First, the electorate must be presented with the required information related to the primary trend, which clearly show the stand from the candidate on those particular topic. Second, the voters should not only respond to the information, but they also required grasp the essence of the reply message. Therefore, the existing approaches to election implementation based solely on the quality of administrators who collected paper votes manually to be verified and tabulated by computers or people. In every voting place, usually multiple group of people stay in the polling location to witness the process as the careful mechanism to prevent worst case scenario by observing the administration to be reliable in every critical step of election phase [32]. These prove that privacy concern mainly important to set assurance of the mechanism used. However, there is an indication that majority users are not concerned of the risks, which they presume weak implications or threats to their future life. Many cases was reported that user selectively revealing personal information to the strangers [33].

Hypothesis 7*: Privacy concern will have a positive effect to personal data protection in election.*

3.5. Perceived Benefits

Blais and Loewn [34] considered the relationship of engagement with formal electoral politics and the decision to vote in elections. They suggested that youth are not casting their votes because they have found more meaningful political activities in which to engage. Blais and Young [35] added that the perceived benefit of choosing the electoral votes for national candidates does have a significant implication the cost of voting and personal data protection. At last, they stated that the votes should not response to the every possibility of casting definite votes but focused to the arrangement of package offered to increase the utility and efficacy. Thus it requires that voters be notified of over votes before a ballot is cast and be given the opportunity to correct errors before record is produced [36].

***Hypothesis 8**: Perceived benefits will have a positive effect to personal data protection in election.*

4. Analysis & Result

4.1. Instrument

The survey questionnaire consisted of six (6) sections namely demographic with 11 multiple answer questions, three section of factors with 14, 15 & 13 questions respectively and one section of 15 outcome items with likert scale question as well comment section. To strengthen the reliability and validity of the instrument that is constructed, the researcher evaluates each item in the questionnaire through 2 stages of pilot study, which is pre-test (6 people) and post-test (44 people) to avoiding time and budget waste. Pilot study also was conducted in limited scale to improve the design and prediction for appropriate sample size, to anticipate potential risk and to collect clear outcomes, so it can be adjusted for larger scale further. After check the reliability and validity of each question, the researcher conducted survey study with total of 779 participants from offline (Medan and Jakarta) and online (Google Docs). It uses Indonesian to make easy the message delivery in every question items with circling the represented number using 6-likert scales. The analysis of result used smartPLS v2 [37] to verify and validate the accuracy and reliability of the hypothesis. An important characteristic of PLS-SEM is that the model estimates depend on the model under consideration for instance, eliminating or adding certain indicators or constructs, which have an effect on the model estimates in different parts of the model [38].

4.2. Measurement Model Result

Using a two tailed test with degree of significant at 10%, the path coefficient will be meaningful if the t-value is greater than 1.64 or p-value smaller than 0.1 (weak), 0.05 (medium) and 0.01 (strong). To find the reliability gauge for value through examining each plane of the outer loadings, preferably the value should be greater or in the position of 0.7, but arguably, for the purpose of exploratory research, the value of 0.4 or larger is tolerated [36]. Thus, after factor analysis there are total 13 out of 45 items was deleted which interestingly have p-value less than 0.1, which indicated significant indicator of outer loadings.

Table 1. Outer Model Statistic Result

Reflective Constructs	Reflective Indicators	Outer Loadings (Outer Weights)	t Value	p Value	90% Confidence Levels
LReg	LR2	0.703 (0.234)	5.884/3.272	0.00111	0.507; 0.899
	LR3	0.691 (0.258)	5.681/3.785	0.00016	0.490; 0.892
	LR4	0.745 (0.296)	9.063/4.599	0.00000	0.880; 0.610
	LR6	0.740 (0.280)	8.310/4.530	0.00000	0.887; 0.593
	LR7	0.760 (0.300)	9.890/4.672	0.00000	0.663; 0.887
SNor	SN1	0.816 (0.581)	10.324/6.990	0.00000	0.686; 0.946
	SN8	0.843 (0.624)	12.329/7.392	0.00000	0.731; 0.955
TSol	TS1	0.750 (0.367)	7.644/4.962	0.00000	0.588; 0.912
	TS2	0.717 (0.345)	7.946/4.847	0.00000	0.568; 0.866
	TS3	0.697 (0.300)	5.848/4.557	0.00000	0.893; 0.501
	TS9	0.721 (0.370)	7.788/5.020	0.00000	0.568; 0.874
PBen	PB1	0.785 (0.276)	10.802/7.700	0.00000	0.665; 0.905
	PB2	0.738 (0.241)	9.470/6.617	0.00000	0.609; 0.867
	PB3	0.725 (0.235)	8.307/7.009	0.00000	0.581; 0.869
	PB4	0.719 (0.264)	7.723/7.509	0.00000	0.566; 0.872
	PB5	0.829 (0.293)	16.929/7.290	0.00000	0.748; 0.910
PCon	PC2	0.798 (0.469)	11.219/7.035	0.00000	0.681; 0.915
	PC4	0.723 (0.393)	6.760/5.958	0.00000	0.547; 0.899
	PC5	0.773 (0.439)	10.230/6.864	0.00000	0.648; 0.898
PDPro	PDP4	0.719 (0.422)	6.527/4.596	0.00000	0.537; 0.901
	PDP5	0.724 (0.392)	5.588/4.422	0.00001	0.509; 0.939
	PDP6	0.790 (0.522)	11.666/5.599	0.00000	0.678; 0.902

4.3. Structured Model Result

The result showed that the connection of LReg over PBen has insignificant value where p = 0.447 while LReg over PCon has weak significant where p = 0.095. Further, the relationship of SNor to PBen has strong significant (p=0.001) while SNor to PCon has weak significant (p=0.061). On the other hand, TSol has both strong relationship (p=0.000) involved TSol to PBen and TSol to PCon. In addition, PBen has strong relationship to PDPro (p=0.000) and PCon has weak relationship to PDPro (p=0.108). Furthermore, there is an indication that LReg has directed insignificant on PBen but has direct significant to PCon which both as measures that differs with other that has direct significant to both PBen and PCon, so both measures to PDP as outcome. According to t value, LReg moves in direct quantity of 0.71 as its coefficient to PBen that present a 100 points change in LReg will amend 71 changes in PBen in the positive direct. Meanwhile, LReg moves in direct quantity of 1.67 as its coefficient to PCon that present a 100 points change in LReg will amend 167 changes in PCon, also in the positive direct. On the other hand, there is no negative value in t value indicates that the impact changes to each construct bring positive impact.

Table 2. Inner Model Statistic Result

	Path Coefficient	t-Value	Significant Levels	p-Values	90% Confidence Levels
LReg -> PBen	0.088279	0.710757	NS	0.47744784	[-0.117, 0.292]
LReg -> PCon	0.196456	1.667318	*	0.09585363	[0.001, 0.391]
SNor -> PBen	0.364202	3.061312	***	0.00120610	[0.245, 0.483]
SNor -> PCon	0.193295	1.608530	*	0.06175647	[0.073, 0.313]
TSol -> PBen	0.441832	3.719134	***	0.00021427	[0.246, 0.636]
TSol -> PCon	0.440688	3.939844	***	0.00008886	[0.256, 0.626]
PBen -> PDPro	0.472056	3.249418	***	0.00227949	[0.168, 0.560]
PCon -> PDPro	0.266033	1.870739	*	0.10812484	[*-0.005*, 0.391]

4.4. Measurement Validity

Cronbach alpha also can be used besides AVE for internal consistent reliability with values of 0.60 to 0.70 in exploratory research and values from 0.70 to 0.90 in more advanced stages of research are regarded as satisfactory whereas values beyond 0.60 indicate a lack reliability [38]. Meanwhile, from the table 4.6, there is contrast result with SNor value for cronbach alpha has 0.546 while the other has more than 0.60 but based on AVE, only SNor has satisfactory reliability value with 0.688. However, from list of value in composite reliability showed value more than 0.80 except PDPro with 0.789 indicated the high reliability for each construct in exploratory research. For convergent validity also showed good result with all construct have AVE value more than 0.50 with the smallest value 0.521 for TSol.

Table 3. Latent Variable Quality Overview

	AVE	Composite Reliability	R Square	Cronbachs Alpha	Communality	Redundancy	LV Index Values
LReg	0.530432	0.849415		0.778964	0.530432		4.951774
SNor	0.687876	0.815039		0.546706	0.687876		4.527046
TSol	0.520809	0.812888		0.694102	0.520809		4.944040
PBen	0.578391	0.872425	0.572917	0.816928	0.578391	0.046626	5.063385
PCon	0.586243	0.809292	0.489818	0.647314	0.586243	0.100488	4.932448
PDPro	0.554889	0.788709	0.469154	0.602740	0.554889	0.218820	5.016462

4.5. Discriminant Validity

The analysis on Average Variance Extracted (AVE) is used to determine the model of discriminant validity (DV). The square root of the AVE (bold highlighted) for each construct is compared and should be larger than any correlations of the latent variable pair [40]. To initiate DV, Fornell and Larcker [39] also recommended the result should be higher than any other correlation values among the latent variable. In this case, all the square root of AVE construct has greater value than those in all field of correlation values except for PDPro (TSol) that have value of correlation 0.750, larger than its AVE (0.744) indicated DV table specifically is sufficient (see table 4.7). Furthermore, SNor (0.829) has highest number of square AVE root above all, while TSol (0.722) became the lowest. However, the DV is satisfactory when constructs have an AVE loading larger than 0.5 indicated that at least 50% or half of measurement variance was expressed by the respectable construct.

Table 4. Discriminant Validity

	LReg	SNor	TSol	PBen	PCon	PDPro
LReg	0.728308					
SNor	0.519945	0.829382				
TSol	0.630405	0.570358	0.721670			
PBen	0.548503	0.600023	0.662200	0.760520		
PCon	0.661912	0.585599	0.688261	0.750632	0.765665	
PDPro	0.716656	0.634542	0.750692	0.714829	0.725987	0.744908

4.6. Research Hypothesis

The two exogenous constructs (PCon & PBen) together explain 46.9% of the variance of the endogenous construct PDPro (R^2 = 0.469), as indicated by the value in the construct circle. LReg, SNor and TSol also jointly explain 57.3% of the variance of PBen (R^2 = 0.573) and 49% of the variance of PCon (R^2 = 0.49). This study also interesting to evaluating the indirect effect via mediating constructs that PBen and PCon acted as the bridging to the endogenous constructs personal data protection (PDPro). The total effect of LReg on both PBen and PCon became the lowest with 0.088 and 0.196 respectively.

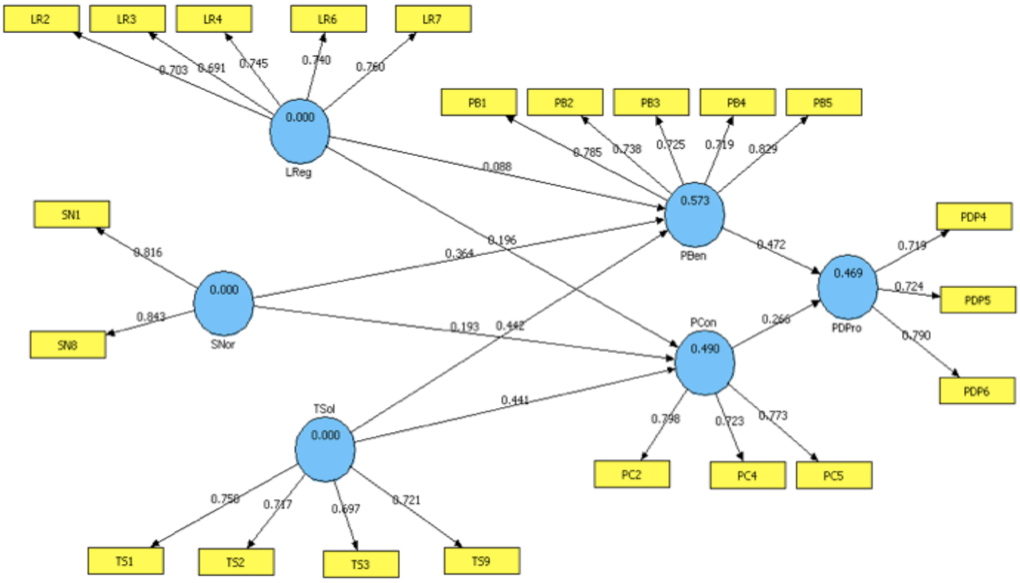

Figure 1. Privacy Framework Model PLS Result

***Hypothesis 1**:* With regard to path analysis, the changes of LReg on PCon has coefficient of 0.088 with p equal to 0.477, and confidence interval of 90% (-0.117, 0.292) that does not indicate significant influence on the construct, then null hypotheses 1 cannot be rejected.
***Hypothesis 2**:* With regard to path analysis, the changes of LReg on PBen has coefficient of 0.196 with p equal to 0.095, and confidence interval of 90% (0.001, 0.391) that indicates weak significant influence on the construct, then null hypotheses 2 can be rejected.
***Hypothesis 3**:* With regard to path analysis, the changes of SNor on PCon has coefficient of 0.364 with p equal to 0.001, and confidence interval of 90% (0.245, 0.483) that indicates strong significant influence on the construct, then null hypotheses 3 can be rejected.
***Hypothesis 4**:* With regard to path analysis, the changes of SNor on PBen has coefficient of 0.193 with p equal to 0.061, and confidence interval of 90% (0.073, 0.313) that indicates weak significant influence on the construct, then null hypotheses 4 can be rejected.

Hypothesis 5*:* With regard to path analysis, the changes of TSol on PCon has coefficient of 0.442 with p equal to 0.0002, and confidence interval of 90% (0.246, 0.636) that indicates very strong significant influence on the construct, then null hypotheses 5 can be rejected.
Hypothesis 6*:* With regard to path analysis, the changes of TSol on PBen has coefficient of 0.441 with p equal to 0.00008, and confidence interval of 90% (0.256, 0.626) that indicates very strong significant influence on the construct, then null hypotheses 6 can be rejected.
Hypothesis 7*:* With regard to path analysis, the changes of PCon on PDPro has coefficient of 0.472 with p equal to 0.002, and confidence interval of 90% (0.168, 0.560) that indicates strong significant influence on the construct, then null hypotheses 7 can be rejected.
Hypothesis 8*:* With regard to path analysis, the changes of PBen on PDPro has coefficient of 0.266 with p equal to 0.108 and confidence interval of 90% (-0.005, 0.391) that indicates weak significant influence on the construct, then null hypotheses 8 can be rejected.

5. Conclusion

In election context, based on the user perspective through survey, the legal framework was not sufficient to effectively manage and control the personal data protection, especially when using voting machines and considering social culture of multiple ethnicity and races. Therefore, some aspects need more consideration as primary concern in ensuring PDP such as security safeguards, the certification process and the application for tabulation. However, the absence of strong regulatory framework can lead to the failed state of suppliers to align the technology use with security requirements and social context, creating the voting machines that is vulnerable and susceptible towards threats from every corner. On the other hand, there are many prospects of sources of mistake in any research project, in which the researcher try to reduce the errors at minimal level. But, there remain conviction and credibility in these research result due to systematic approach followed rigorously but it was limited to certain extent such as coverage and time so they cannot cater the various cultures and diversity of population as the purpose of the study. According to public opinion that recognize the importance of privacy as the secondary regard, it can be extended that the environment in actual that shape the privacy concern as the communal interest. Meanwhile, the government role and the organization approach to protect personal data in election electronically should take into account the way to providing the suitable mechanism to increase the value of technology solution in term of benefit and establish frequent awarenss program to raise concern. Generally, there are numerous studies indicated that IS project management still show its high failure rate, which major issues related to uncertainty of legal concept and lack of focus in the policy [41]. By recognizing the benefits of IT governance and investment are essential for competitive advantages and to reducing the failure rate of IT projects [42].

References

[1] Warren S, Brandeis L. The Right to Privacy. *Harvard Law Review*. 1890; 4(5): 193-220.
[2] Taylor N. State Surveillance and the Right to Privacy. *Surveillance & Society*. 2002; 1(1): 66-85.
[3] Sutikno T, Stiawan D, Subroto IMI. Fortifying Big Data Infrastructures to Face Security and Privacy Issues. *Telkomnika*. 2014; 12(4): 751-752.
[4] Schneier B. Schneier on Security. Indiana: Wiley Publishing. 2008: 118-119.
[5] Herrnson P. Niemi R, Hanmer M, Bederson B, Conrad F, Traugott M. Voting Technology: The Not-So-Simple Act of Casting a Ballot. Washington DC: Brooking Institution Press. 2009: 20-22.
[6] Kiesler S, Siegel J, McGuire T. Social Psychological Aspects of Computer-mediated Communication. *American Psychologist*. 1984; 39: 1123-1134.
[7] Culnan MJ, Markus M. Information Technologies. In: Jablin F.M, Putnam LL, Roberts K.H & Porter LW. Handbook of organizational communication: An interdisciplinary perspective. Newbury Park: Sage; 1987: 420-433.
[8] Walther JB. Computer Mediated Communication: Impersonal, Interpersonal and Hyperpersonal Interaction. *Communication Research*. 1996. 23: 3-43.
[9] Schumaker EM. Exploring the Hyperpersonal Model: Determining the inflated nature of feedback in computer-mediated communication. Ohio State University: Ohio Communication. 2013: 1-2.
[10] Dinev T, Hart P. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*. 2006; 17(1): 61-80.
[11] Culnan M, Armstrong P. Information Privacy Concerns, Procedural, Fairness and Impersonal Trust: An Empirical Investigation*. Organization Science*. 1999; 10(1): 104-115.

[12] Krasnova H, Veltri NF. *Privacy calculus on social networking sites: Explorative evidence from Germany and USA*. IEEE 43rd International Conference on System Science (HICSS). Honolulu. 2010: 1-10.

[13] Solove D. I've Got Nothing to Hide and Other Misunderstandings of Privacy. Washington DC: George Washington University Law School. 2011: 3-4.

[14] Sloan RH, Warner R. Big data and the 'New' Privacy Tradeoff. Chicago: Kent College. 2013: 2-7.

[15] Milne GR, Labrecque LI, Cromer C. Toward and Understanding of the Online Consumer's Risky Behavior and Protection Practices. *The Journal of Consumer Affairs*. 2009; 43(3): 449-473.

[16] Kosa T. *Vampire Bats: Trust in Privacy*. IEEE International Conference on Privacy, Security and Trust (PST). Ottawa. 2010: 96-101.

[17] Blank G, Bolsover G, Dubois E. A New Privacy Paradox: Young People and Privacy on Social Network Sites. Oxford: Oxford Internet Institution. 2014: 1-3.

[18] Barnes S. A privacy paradox: Social networking in the United States. *First Monday*. 2006; 11(9).

[19] Dalager JK. Voters, Issues, and Elections: Are the Candidates' Messages Getting Through? *The Journal of Politics*. 1996; 58 (2): 486-515.

[20] Sniderman PM, Brody RA, Tetlock PE. The Clash of Rights: Liberty, Equality and Legitimacy in Pluralist Democracy. New Haven: Yale University Press. 1996: 235-258.

[21] Ward T, Salmon K. The Ethics of Punishment: Correctional practice implications. *Aggression and Violent Behavior*. 2009; 14: 239-247.

[22] Rouviere E, Caswell JA. From punishment to Prevention: A French case study of the introduction of co-regulation in enforcing food safety. *Food Policy*. 2012; 37: 246-254.

[23] Whitley EA. Informational Privacy, Consent and the ''Control'' of Personal Data. *Information Security Technical Report*. 2009; 14:154-159.

[24] Hyman HH. Political Socialization: A Study in the Psychology of Political Behavior. Glencoe: The Free Press. 1959: 50-52

[25] Merelman R. The Adolescence of Political Socialization. *Sociology of Education*. 1972; 45(2): 134-166.

[26] Kshetri N. Big Data's Impact on Privacy, Security and Consumer Welfare. *Telecommunications Policy*. 2014; 38: 1134-1145.

[27] Camenisch J. Information Privacy?! *Computer Networks*, 2012; 56: 3834-3848.

[28] Vrhovec G. Beating the Privacy Challenge. *Computer Fraud & Security*. 2011; 2011 (3): 5-8.

[29] Cetinkaya O. *Analysis of Security Requirements for Cryptographic Voting Protocols.* IEEE International Conference on Availability, Reliability and Security (ARES). Barcelona. 2008: 1451-1456.

[30] Kiayias A, Korman M, Walluck D. *An Internet Voting System Supporting User Privacy*. IEEE 22nd Annual Computer Security Applications Conference (ACSAC). Miami Beach. 2006: 165-174.

[31] Kofler R, Krimmer R, Prosser A. *Electronic Voting: Algorithmic and Implementation Issues*. IEEE 36th International Conference on System Sciences (HICSS). Honolulu. 2003: 1-7.

[32] Selker T, Goler J. The SAVE system - secure architecture for voting electronically. *BT Technology journal*. 2004; 22 (4): 89-95.

[33] Mvungi B, Iwaihara M. Associations between privacy, risk awareness, and interactive motivations of social networking service users and motivation prediction from observable features. *Computer in Human behavior*. 2014; 44: 20-34.

[34] Blais A, Loewen PJ. Youth Electoral Engagement in Canada. Ottawa: Elections Canada. 2009: 13-16.

[35] Blais A, Young R. Why Do People Vote? An Experiment in Rationality. *Public Choice*. 1999; 99: 39-55.

[36] Fischer EA. *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*. Domestic Social Policy Division, Science and Technology. The Library of Congress. Order Code RL32139. 2003.

[37] Ringle CM, Wende S, Will A. SmartPLS 2.0.M3. Hamburg: SmartPLS. 2005. Retrieved from http://www.smartpls.com

[38] Hair JF, Hult GT, Ringle CM, Sarstedt M. A Primer on Partial Least Squares Structural Equation Modelling (PLS-SEM). California: SAGE Publication, Inc. 2014: 101-149.

[39] Gefen D, Straub D, Boudreau M. Structural equation modelling regression: Guidelines for research practice. *Communications of the Association for Information Systems*. 2000; 4 (7): 1-77.

[40] Fornell C, Larcker D. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*. 1981; 18(1): 39-50.

[41] Putra SJ, Subiyakto A, Ahlan AR, Kartiwi M. A Coherent Framework for Understanding the Success of an Information System Project. *Telkomnika*. 2016; 14(1): 302-308.

[42] Amali LN, Mahmuddin M, Ahmad M. Information Technology Governance Framework in the Public Sector Organizations. *Telkomnika*. 2014; 12(2): 429-436.