Atlantis Highlights in Engineering (AHE), volume 2
International Conference on Industrial Enterprise and System Engineering (IcoIESE 2018)

Privacy Protection and Role of Technology:

Citizen Perception on Electronic Voting Initiative

Muharman Lubis
School of Industrial Engineering, Telkom University
Bandung, Indonesia
muharmanlubis@telkomuniversity.ac.id

Tien Fabrianti Kusumasari
School of Industrial Engineering, Telkom University
Bandung, Indonesia
tienkusumasari@telkomuniversity.ac.id

***Abstract*—This study sought to identify factors that might increase the likelihood of the acceptance of electronic voting. Citizen satisfaction aimed to meet the expectation of having a better voting experience than before in relation to privacy protection. For the purpose of this study, the researcher delivered survey questionnaire to 790 people by using purposive sampling in Medan and Jakarta as well as an online method to add more variety to the result. It has been done by determining the proportion of study units in the population and categorizing them before distributing the questionnaire among the respondents.**

Keywords—privacy; technology; perception; voting; protection;

I. INTRODUCTION

Continuous and rapid technological change bring numerous benefit to the people's daily life simultaneously creates threats to established resource allocation and business models. Actually, the adoption of new technology can offer opportunities for organization to deliver sophisticated customer oriented service in faster and rightful to meet their expectation and satisfaction. With the rapid advancement of technologies, the decision from consumer's perspective to adopt these kind of technologies depends on several factors like the availability, ergonomics, expectation, protection, etc. [1]. Therefore, there is an agreement among academician that IT has tremendous impact on creating firms to be more productive but these only be realized when IT has become attached to nearly all of human daily activities [2]. However, due to a fast development of IT, especially interaction by Intenet, many of the laws from various countries have not accommodate its current state caused many citizen encourage their parliament to revised the regulation in order to have PDP on every cyber activities and to allow an efficient protection [3]. Moreover, the gaps between principle and execution exist, due to politics, which generated by particular interest in specific group against over citizen rights by constitutional, which accounted for policy development [4].

Given the tremendous increase in expenditures for campaign cost and bad culture demand. To some extent, it is not surprising if some of candidates might have desire related to their personal ambition, business affairs or economic interests through the manipulation process of government decisions after they secure position in the parliament. As the role of money arises significantly together with crucial government position to design the regulation, once the candidates and political party achieve victory in the election, they will owe huge debts to the contributors, which supplied and provided the means to be the champion. In this respect, the government eventually becomes the major purchaser of goods, the biggest client, and even the largest subsidizer, which exploits the tax income and the legal regulation to facilitate the needs of person or company that donated/contributed to the candidates. Actually, this political and social cycle have trapped the players and beneficiaries to be dependent solely to the power of money with certain demand and supply based on government position. Thus, the election process is very important to determine the future of the government and the country, especially related to the PDP. By exploiting the personal data, it can lead to vote fraud, transaction and coercion. Interestingly, the distinction between the campaign donation and the political bribe is almost a hair's line difference when the related article verse of regulation can be interpreted one way or another.

The technology use without the cyberlaw to manage the cyber activities has led to computer misuse or cybercrime widely [35]. Regardless the successes and failures documented in the numerous case studies recently published on *e*-voting, issue of privacy has not been ceded the attention and concern it deserves. How is the voters' privacy supposed to be protected in *e*-voting? Is the choice of technology already sufficient to guarantee the basic requirement of PDP? Can the available PDP devices be sufficient to tackle the numerous possible threats to *e*-voting systems and conceal their vulnerabilities? How to satisfy the public expectation to protect privacy in *e*-voting? Do citizens value their personal data more than the intrinsic value of money? Therefore, this study presents particular theory in the realm of technology acceptance and adoption to give glimpse on how the organization could develop their approach. On the other hand, this study also wants to bridge the gaps and bring new perspective to add more layers for the government in this case of e-voting to have concrete and simple explanation on how citizen perceive this initiative to replace traditional voting system with the latest.

II. THE ROLE OF TECHNOLOGY

A. Understanding Privacy Protection Issues

Opportunities and clashes will always be the factors related to the PDP mechanism, in which general understandings of boundaries and government accessibility level to personal data stored either in the particular database or cloud that was managed by institution, organization or company become critical consideration. The differences about the approach and event on information to be acquired and transferred for civil purpose, legal execution or regulatory objective; freedom of opinion for blog, posting and publications; corporate ability to promote their product in the internet and to personalize the users online by identifying cookies, metadata or other; and the deployment of drones for commercial and governmental data acquisition purposes also become fundamental factors that create misconception among people about role of the technology [5]. Without privacy mechanism, it may be extremely difficult for individuals to distinct their private and public lives, or to conduct other important activities based on his rights, such as religious, association and expression freedom [6]. As a result, technology remain, even continue to be the primary driving force behind PDP although, unfortunately, IT misuse has further weakened the PDP [7].

The current system being used for PDP, unfortunately fragmented in various regulation with different context and mostly gradual approach to privacy protection. Consequentially, it is very difficult for individuals to understand what they should do to protect their sensitive information and how to report when there is privacy incident occurred [6]. In exploring the complicated issues of privacy and trying to achieve the expected balance between the purpose of sharing information and commercialization of data, at one hand, and securing the channel and the database to eliminate identifiers, on the other hand; sometimes the court sought guidance from, what they called privacy expert due to his assignment in specific company, which are in reality have different perspective with citizen [8]. Is it really possible to measure the value that people place on privacy? And has less privacy truly become the new social norm in which some scholars have concluded that our society simply does not place much value on privacy [9]. For informed consent to be meaningful, it is generally recognized that whom giving the consent must understand what they are giving to, such as asking essential questions about the purpose and the approach to protect. It is also meaningless if the person has no option at all in the process of giving their consent [10].

B. Technology Acceptance and Diffusion of Innovation

Rogers [11] explains the step-by-step by which an innovation is communicated through certain channels over time between the members of a social system. He further described that the innovation occurred after going through several stages involving recognition, persuasion, decision, execution and validation that led to the development of adoption curve of innovators, early adopters, early majority, late majority and laggards. The organizational capacity is related to individual characteristics (attitude toward change), internal characteristics (centralization, complexity, formalization, interconnectedness, organizational stack, size) and external characteristics (system openness). In summary, this is a theory of how, why and at what rate new ideas and technologies spread across cultures, operating at the individual and business level in which individuals are considered to have different degrees of readiness to adopt innovations, and therefore, generally observed that the portion of the population that adopts an innovation is distributed normally over time.

Since the early applications of DOI to IS research, the theory has been applied and adapted in various ways such as material requirement planning (MRP), CAD/CAM, ERP, E-procurement, Intranet, inventory control and many more [2]. On the other hand, TOE framework identifies three aspects of enterprise's context that influence the process by which it adopts and implements a technological innovation which are technological context, organizational context and environmental context [12]. It also provides a useful analytical framework that can be used for studying the adoption and assimilation of different types of IT innovation and the potential of application to IS innovation domains though specific factors identified within the three contexts may vary across different studies. This framework is consistent with the DOI theory and makes diffusion of innovation theory better able to explain intra-firm innovation diffusion [13].

The use or rejection of technology is the result of an intention to produce the behavior, which is influenced simultaneously by the attitude of the individual attitudes, determined by beliefs and subjective norms [20]. According to TRA (theory reasoned action), the intention to decide the effective behavior that refers to the observable action, influenced by the perception of the external evaluation on using product or not [21]. TRA assumes that the people act upon their rational thinking by examining what they will lose or will gain as their manifestation of attitudes or themselves. In addition, Davis [22] proposed the TAM (technology acceptance model) to emphasize the reason of the users to accept or reject the IT and how to manipulate the acceptance, thereby providing support to predict and clarification. Thus, perceived use has a greater impact on behavior compare to perceived facilities, in which people choose to perform a behavior, even there is a disagreement, which might motivates them or other person [20]. Meanwhile, acceptance can be described as an important factor in developing success or failure of any IT adoption, which it has been conceptualized as a response variable from psychological aspect in decision making process [23]. Other study also indicated that the religious indicator and consistent training program to create awareness among student also can be used to manipulate behavior towards certain adoption of innovation [37].

C. The Role of Technology as Solution

A new technology which offers as the best solution to solve previously encountered problems may not prove to be as

effective as anticipated and may even give rise to a newer and even graver problem than the old technology [14]. Motivations in the form of basic needs, goals, purposes and plans can both foster and hinder future actions which have to be considered in the planning [15]. For example, UK privacy law have had difficulty keeping pace in data collection and information sharing trend in the society, resulted to the PDP process has become excessively incoherent and has broken to numerous pieces [6]. The principles must be delivered in the technology stack and organizations must take appropriate technical and organizational measures to do so [16]. PDP laws exist because it is believed that, without them, technology will enable or cause data controllers and processors to trample on fundamental rights and freedoms [17].

In e-voting process, large number of data is collected and transmitted from numerous location to various or specific location to conduct tabulation process and calculate the voting result. Without doubt, these processes attract high attention from cybercriminals to exploit the vulnerabilities of the system. Meanwhile, it also likely to create miscommunication among technician that bring incoordination resulted mistrust among party. Thus, the system that handle big data environment should provide a set of advanced information about security procedure, technical documentation, troubleshoot process and performance indicator [18]. The server also need to have a stored for authentication policies and authorization process, which defining the type of resources require particular user to provide specific attributes to be certified and to aligned with other metadata such as data provider [19]. On the other hand, Vrhovec [24] emphasized there are four aspects to manage data privacy risk as safeguarding personal information to be protected in its lifecycle, involving business process, technology, governance and policy. Companies must implement reasonable measures and technology controls for data protection that enable employees to securely access, use, and share information necessary to do their jobs [25]. In addition, individual verifiability is important to raise public trust in *e*-voting as important goal for any secure system implementation [26]. However, some elements in the operational aspect of PDP can only be enabled by technology while others are made more manageable or cost-effective [27].

A user-friendly e-voting interface can avoid the distrust from the voters towards the mechanism and they essentially do not need to learn about complex techniques used in the voting system and its additional component [28]. Hence, future revision of the data protection legal framework should not only be promoted taking into account new technology developments but also the new data subjects and their behaviors [29]. Technology can be used to organize standards intended to limit undesirable effects, to define scope of regulation, to nudge the market in a certain direction that is considered desirable by policymakers [30]. To minimize this risk, institution provide step-by-step implementation by utilizing their efforts on IS to reduce the vulnerabilities and threats in the system, although the personal error somehow became the major antecedent in the data loss issues, which should be the first to be maintained through training and assessment [31].

Technological solutions are very useful for an organization to address issues of data loss. It also can be used to conduct security strategy, maintain the performance and provide emergency procedure, especially as countermeasures to tackle illegal access or attack whether intentionally or error incident [32]. The collaboration of increasing performance, capacity and capability of IT and the decreasing clarity as well as disagreement on PDP concept raises issues of cyberlaws, policies and ethics. Meanwhile, the advances in IT have recently threatened privacy and lessened the amount of control over personal data, which create another negative and complicated problem [33]. In addition, the universal verifiability requirement can be viewed as means to assure correctness, increase personal data protection and avoid electoral fraud although, to some extent, it has conflict with the process of ballot validation [28]. In the context of election, based on the user perspective through survey, the legal standards was is not sufficient to effectively regulate the development and the voting machines adoption, particularly, in respect to approved security mechanism, performance indicator, tabulation program, assessment technique and certification process [34].

III. METHODOLOGY

This study used quantitative methods through survey questionnaire, which was distributed offline and online to Indonesians that are eligible to cast votes. Before conducting these, preliminary test was conducted to two experts for the purpose to identify the weaknesses and to evaluate the quality of form structure. The questionnaire has 11 items related to technology solution with 8 demographic data. It used Indonesian language to make it easy to deliver the objective and question, which was used 6-likert scales with ticking box. The analysis used ordinal logistic regression because it is more informative because it presents by how much the dependent variable changes as the independent variable changes, whereas the correlation coefficient presents only whether or not the two variables move in the same or opposite directions and the degree of linear association [36]. However, the information from regression is just gained through more restrictive assumption, which the response variable is a function of the predictor variable.

TABLE I. ORDINAL REGRESSION STATISTICS

No	Threshold	Estimate	Std. Error	Wald	Sig.
TS1	[TS1R = 1.00]	-20.175	1.040	376.152	0.000
	[TS1R = 2.00]	-18.976	1.032	337.967	0.000
	[Election=2]	0.815	0.391	4.332	0.037
	[Education=1]	-16.203	0.637	646.065	0.000
	[Education=2]	-16.379	0.634	667.114	0.000
	[Education=3]	-16.407	0.604	737.289	0.000
	[CL4=0]	-0.608	0.307	3.920	0.048

TS2	[TS2R = 1.00]	-18.393	0.757	590.405	0.000
	[TS2R = 2.00]	-17.049	0.749	518.178	0.000
	[Education=1]	-15.785	0.514	942.451	0.000
	[Education=2]	-16.509	0.499	1094.345	0.000
	[Education=3]	-16.857	0.457	1362.586	0.000
	[Work=4]	1.231	0.537	5.244	0.022
TS3	[TS3R = 1.00]	-1.459	1.415	1.064	0.302
	[TS3R = 2.00]	-0.139	1.413	0.010	0.921
	[Gender=1]	0.368	0.165	4.969	0.026
TS4	[TS4R = 1.00]	-1.732	1.377	1.582	0.208
	[TS4R = 2.00]	-0.287	1.373	0.044	0.834
	-	-	-	-	-
TS5	[TS5R = 1.00]	-0.206	1.302	0.025	0.874
	[TS5R = 2.00]	0.541	1.302	0.173	0.678
	-	-	-	-	-
TS6	[TS6R = 1.00]	-0.734	1.398	0.276	0.600
	[TS6R = 2.00]	0.660	1.396	0.224	0.636
	[Work=4]	1.078	0.457	5.568	0.018
TS7	[TS7R = 1.00]	-18.701	0.710	694.442	0.000
	[TS7R = 2.00]	-17.445	0.705	611.628	0.000
	[Gender=1]	0.421	0.172	6.031	0.014
	[Education=1]	-17.202	0.504	1163.481	0.000
	[Education=2]	-17.294	0.500	1195.592	0.000
	[Education=3]	-17.512	0.471	1379.665	0.000
TS8	[TS8R = 1.00]	-19.477	0.812	576.027	0.000
	[TS8R = 2.00]	-18.143	0.804	509.621	0.000
	[Education=1]	-17.236	0.566	926.886	0.000
	[Education=2]	-17.350	0.560	958.358	0.000
	[Education=3]	-17.378	0.529	1080.168	0.000
	[Work=1]	0.701	0.350	4.002	0.045
	[Work=2]	0.948	0.319	8.837	0.003
	[Work=4]	1.319	0.499	6.995	0.008
TS9	[TS9R = 1.00]	-0.828	1.285	0.415	0.519
	[TS9R = 2.00]	0.524	1.284	0.167	0.681
	[Age=2]	0.829	0.334	6.176	0.013
	[Age=3]	0.817	0.314	6.758	0.009
	[Age=4]	0.900	0.340	7.019	0.008
	[CL3=0]	0.434	0.191	5.175	0.023
TS10	[TS10R = 1.00]	0.756	1.311	0.332	0.564
	[TS10R = 2.00]	2.045	1.314	2.423	0.120
	[Age=2]	0.742	0.369	4.057	0.044
	[Age=5]	1.404	0.537	6.843	0.009
	[Education=1]	2.778	1.211	5.625	0.022
	[Education=2]	2.509	1.207	4.324	0.038
	[Education=4]	2.729	1.247	4.791	0.029
TS11	[TS11R = 1.00]	-0.564	1.251	0.203	0.652
	[TS11R = 2.00]	0.589	1.251	0.221	0.638
	[Education=1]	2.555	1.134	5.073	0.024
	[Education=2]	2.627	1.134	5.367	0.021

TS1: KPU (the General Elections Commission) should devote more time and effort to prevent illegal access anytime to election database.

TS2: Information on whether I have voted or how I cast the vote is secured and have not been published.

TS3: Biometric (authentication process by part of body recognition) is the best solution to assure the vote content integrity.

TS4: I would like to have full control and access of my own data for verification and validation purposes.

TS5: I do not want to case vote if I feel threaten by the risk of threats from the hackers.

TS6: Polling stations (TPS) should be set as the data backups for clients that submit result to KPU server in avoiding lost data or missing data.

TS7: Electronic voting introduces new risk for personal data protection.

TS8: Technology solution will be useless if the human resources do not have the best IT (Information Technology) skill.

TS9: Authorization of voter's identity only involves the registered one in TPS unless there are some exemptions.

TS10: It is better to have digital receipt rather than paper-based to prevent vote selling.

TS11: Disconnecting ballots content and identity of voters should preserve secrecy.

IV. DISCUSSION

Education background became the most frequent category that had strong relationship over model constructs (variables) include TS in the context of e-voting with various effects. A decrease occurred by high school student with -16.203, by diploma student with -16.379 and by bachelor student with -16.407 of ordered logit of being TS1 lower level while the other variables in the model are held constant. Being a voter who participates less than three times increases the ordered logit of being in the lower levels of the TS1 category by a factor of 0.815, while an increase by a factor of 0.608 by having office application skill when other variables in model are held constant. The people who have less experience in election are more likely to expect KPU to do more works and attempts to prevent illegal access than whom experiences more than three times of election. Meanwhile, people who have no skill in office application are more likely to disagree that KPU should devote more time and energy in protecting personal data. This result is not necessarily capable to show the skepticism of eligible voters about KPU commitment, but they have different opinion on how KPU should allocate their time and effort proportionally.

Being an entrepreneurship increases the ordered logit of being in the higher levels of the TS2 category by a factor of 1.231 when other variables in model are held constant. There is high relationship (0.022) between entrepreneurship working background and strong effect to trust e-voting keep secret personal information of voter. Meanwhile, other working backgrounds, namely private worker (0.078) and government officer (0.085) have medium relationship to TS2 with strong effect, also second category of earnings (0.053) and internet computer skill (0.099). The use of technology to support daily working activities gives more understanding to the worker in almost every sector on how important the electronic system to achieve business objective effectively and efficiently. Actually, certain voters do not want their personal data to be published for whatever reason by KPU, either prior or subsequent of election. Due to the fact that data will not have to be replicated, there is less chance of human errors being made which leads to more accurate information available.

The negative tendency influenced by educational institution in viewing TS statement might be as a result of concern for KPU to focus more to the primary goals and voter's satisfaction. Information retrieval is the activities of obtaining relevant information from resources involving search algorithm and identification procedure. In this process, the authorization and authentication became the important aspect to prevent the person who does not have permission to get the access to important, critical and sensitive information. Some set of rules and restriction must be initiated to avoid the information be shared to numerous channels by some sort of human errors or bugs. Due to the search engine capacities, internet users can freely access billions of pages of information regardless of time and space constraints with a simple typing and clicking.

The information that kept in the website will be easily accessed by unknown user while the assurance has the ambiguity related to the distinct opinion from the user on the limitation. Thus, the user expects relevant information that can be linked to their personal information, which is not necessary to be revealed unless for the mutual agreement or an urgent need, the responsible party must hide it by all means. Being a male increases the ordered logit of being in the higher levels of the TS3 category by a factor of 0.026 when other variables in model are held constant. However, gender has strong relationship to TS3 but the effect is low, even though biometric as the best solution at this time to assure the authenticity of personal data in the identification and integrity of vote content in the validation process. The odds ratio of being in a higher category of the dependent variable in TS3 for male versus female with statistically significant effect x^2 (1) = 4.969, p=0.026. Male feels the biometric solution in *e*-voting could assure PDP more than the female, while the third category of age (26-30 years) have medium relationship (0.083) to TS3.

There is no significant relationship and effect between demographic factor over TS4 and TS5, which might indicate that voter prioritizes protection over control. Also, it might indicate that voters do not fully grasp with the terminology of full control, half control or no control. Therefore, the private worker is quite likely to expect that voter has the access and control on personal data although with limitation and restriction (sig. value of 0.102). Meanwhile, person with age 26 and 30 is quite likely not participating in the election if they feel threatened from hackers' threat (sig. value of 0.097). Being an entrepreneur increases the ordered logit of being in the higher levels of the TS6 category by a factor of 0.018 when other variables in model are held constant. There is strong relationship between working backgrounds with the lack of willingness to having TPS as client data backup before sending to KPU to prevent data loss. There is also medium relationship (0.095) between the age category (26-30 years) and multimedia computer skill over TS5. They might dislike this initiative because it will increase the operation cost significantly while the other alternative approaches can be done to optimize the need of having data backup such as cloud storage or physical documentation.

The odds ratio of being in a higher category of the dependent variable in TS7 for male versus female with statistically significant effect x^2 (1) = 6.031, p=0.014. The tendency to view the adoption of the new system can bring new risk is not necessary to be negative things but the caution against opportunities. The third age category (26-30 years) and fifth category (36-40 years) have moderate relationship and quite likely to agree that *e*-voting as the risk for PDP. They might think that the change of approach brings more pressures to the committee to perform their duties. Interestingly, there is strong relationship between educational institution and strong effect on the idea that *e*-voting does not introduce the new risk. By having knowledge about *e*-voting can bring more understanding in preparing strategy to optimize the execution and to anticipate the threats. The more voters learn about *e*-voting in term of its benefits and concepts from their

educational institution, the more they will be confidence on its importance in PDP.

There is strong relationship between education and working background on strong effect of TS8. The educational background influences the voters to be more likely to agree that the quality of election committee in IT determines the success of e-voting, while the working background influences the opposite. An increase occurred by student with 0.701, by private worker with 0.948 and by entrepreneur with 1.319 of ordered logit of being higher level of TS8 while the other variables in the model are held constant. In reality, working and education background are mutually exclusive, whereby education enables individual to prepare for his future job by developing competent skill, which will be used in the working field to struggle and survive. The possible rationale for different effects of student as working background and educational institutional over TS8 that individual may be unaware of the election committee competence and capacity can be improved through intense training. There are also different motivation between voters who learn about *e*-voting from university with purpose of investigation and exploration. Some of them want to offer the proper solution while the others focus into the depth of problem statement. Furthermore, there is high relationship between age category and TS9 for the less involvement of other independent parties in authorization process besides the officer in the polling place. An increase occurred by age of 20-25 with 0.829, by age 26-30 with 0.817 and by age 31-35 with 0.900 of ordered logit of being higher level of TS9 while the other variables in the model are held constant. The use of e-KTP is sufficient to prevent ballot stuffing and data manipulation in the verification process of voter identity. Being a person who has internet computer skill decreases the ordered logit of being in the higher levels of the TS9 category by a factor of 0.434 when other variables in model are held constant. They are more likely to disagree that identification process of eligible voters only involve authorized person. They want to optimize PDP in the checking process by minimizing the error with the engagement of more independent parties and human witnesses. The internet increases the privacy concern of voter based on the current trend and behavior in the society. Human error is the most frequent factor that causes the privacy infringement as the result of human incapability to work based on the proper procedure.

In short, this study identify several factors, which increase the likelihood of acceptance of e-voting adoption from citizen perspective in utilizing the technology to protect privacy. Those factors are the attempt by KPU to prevent illegal access either through simulation or authentication, the assurance of anonymity attributes in conducting election, the internal motivation to anticipate and measure risk posed by introducing new technology to the current system and the good assessment of human resource in term of skill and capability in using technology from KPU or relevant institution. Thus, KPU can focus to improve their performance by prioritizing several indicators to meet factors that determines the citizen satisfaction. It will increase the likelihood trust of citizens especially from males, entrepreneurs, young generations, university students and programmers' background.

V. CONCLUSION

The adoption of *e*-voting has main purpose to develop better election in term of privacy protection compared to previous one in order to reduce the high risk of widespread fraud, data manipulation and privacy infringement at polling station level or national tabulation process. As any other type of technology upgrade and advance, *e*-voting systems could increase the current capacity and quality in term of technical aspect such as storage, speed, scope, verification and validation. Thus, to facilitate high percentage of widespread social acceptance, the election committee should socialize this initiative regularly in various locations and sustain its support with legal basis and advice or recommendation from expert or consultant as well. It needs to show clear and concrete benefits to the eligible voters; things that they might be able to see or review. If voting process becomes easier, more accessible and more convenient for the citizens, they might accept and support the new system voluntarily. In this study, it clearly shows that majority of respondents have positive perception over the technology use in the election despite the type of computer skill that they are familiar with. They prefer the adoption to solve previous problem because they believe over the benefits and solutions are offered by the technology use. Interestingly, the majority of citizen prefers not to participate in the *e*-voting if they feel insecure upon the hackers' threats, even the one who possess the programmer skill. They also prefer to have digital receipt rather than paper to prevent vote transaction, large quantity of vote buying and selling. The contribution of this study is to provide insight to develop privacy framework in e-voting that align the relevant factors such as legal regulation, technology solution and social norm.

REFERENCES

[1] P.C. Lai, "The Literature Review of Technology Adoption Models and Theories for the Novelty Technology". Journal of Information Systems and Technology Management, vol. 14, no. 1. Sao Paulo, Jan/Apr 2017. ISSN 1807-1775.

[2] T. Oliveira and M.F. Martins. "Literature Review of Information Technology Adoption Models at Firm Level". The Electronic Journal Information Systems Evaluation, vol. 14, issue 1 2011, pp. 110-121.

[3] J. Sidgman and M. Crompton. "Valuing Personal Data to Foster Privacy: A Thought Experiment and Opportunities for Research". Journal of Information Systems, 30(2). pp. 169-181. 2016. DOI: 10.2308/isys-51429

[4] J.K. Dalager. "Voters, Issues, and Elections: Are the Candidates' Messages Getting Through?" The Journal of Politics, 1996, 58 (2), 486-515.

[5] A.C. Raul. "The Privacy, Data Protection and Cybersecurity Review". Edition 1. November 2014. Law Business Research. London. ISBN 978-1-909830-28-8.

[6] C. Raab and B. Goold. "Protecting Information Privacy. Equality and Human Rights Commission Research Report". series no 69. 2011. ISBN 978-1-84206-347-7.

[7] F.Z. Borgesius, J. Gray and M. van Eechoud. "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework". Berkeley Technology Law Journal. 2015, Vol. 30 Issue 3, p2073-2131. 59p. DOI: 10.15779/Z389S18.

[8] S. Romanosky and A. Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives". Berkeley Technology Law Journal vol. 24, pp. 1061–1102, 2009.

[9] A. Gonsalves. "Facebook CEO: Less Privacy is Social Norm". Information Week, January 12. 2010.

[10] E. Rouviere and J.A. Caswell. “From punishment to prevention: A French case study of the introduction of co-regulation in enforcing food safety”. Food Policy, 37, 246-254. 2012.

[11] E.M. Rogers. “Diffusion of innovations”. Fourth Edition ed., New York, Free Press, 1995.

[12] P.F. Hsu, K.L. Kraemer and D. Dunkle. “Determinants of e-business use in us firms”. International Journal of Electronic Commerce, Vol. 10, No. 4, pp 9-45. 2006.

[13] L. Tornatzky and M. Fleischer. “The process of technology innovation”. Lexington, MA, Lexington Books. 1990.

[14] A. Marzilli. “Election Reform: Point Conterpoint”. Chelsea House. Infobase Publishing. 2011.

[15] D. Dunning. “Social Motivation”. Psychology Press: Taylor & Francis Group. 2011.

[16] S. Room. “Data Protection and Compliance in Context”. British Computer Society. 2007.

[17] S. Room, P. Almond and K. Clark. “Technology’s role in data protection - the missing link in GDPR transformation”. April 2017. Price Waterhouse Coopers, LLP.

[18] N. Kshetri. “Big data's impact on privacy, security and consumer welfare”. Telecommunications Policy, 2014, vol. 38, 1134-1145.

[19] J. Camenisch. “Information privacy?!” Computer Networks, 56, 2012. 3834-3848.

[20] P.M. Silva and G.M. Dias. “Theories About Technology Acceptance: Why the Users Accept or Reject the Information Technology?” Brazilian Journal Information Sciencce, vol. 2, no. 2, pp.69-86, Jul/Dec 2007.

[21] M. Fishbein and I. Ajzen. “Belief, attitude, intention, and behavior: an introduction to theory and research”. Boston (MA): Addison-Wesley, 1979.

[22] F.D. Davis., R.P. Bagozzi and P.R. Warshaw. “User acceptance of computer technology: a comparison of two theoretical models”. Management Science, Ann Arbor (MI), v.35, n.8, p.982-1003, 1989.

[23] A. Dillon and C. Morris. “User Acceptance of Information Technology”. In W. Karwowski (ed). Encyclopedia of Human Factors and Ergonomics. 2001. London: Taylor and Francis.

[24] G. Vrhovec. “Beating the privacy challenge”. Computer Fraud & Security, March, 2011, pp. 5-8.

[25] Shey, H., Mak, K., Balaouras, S., Luu, B. Understand the state of data security, privacy: 2013 to 2014. Forrester Research Inc., 1 October.

[26] O. Cetinkaya. “Analysis of Security Requirements for Cryptographic Voting Protocols”. *International Conference on Availability, Reliability and Security*, pp. 1451-1456. IEEE. 2008.

[27] D. Brown. Technology Solutions to the GDPR Challenge. International Data Corporation, June 2016.

[28] C. Ta-Li and M-S. Hwang. “The voting process should be as simple as possible". *Sixth International Conference on Information Technology: New Generation, IEEE* pp. 449-454. 2009.

[29] S. Gutwirth, R. Leenes and D. Paul. “Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges”. Springer. 2014. ISBN 978-94-007-7539-8

[30] W. Maxwell and M. Bourreau. “Technology neutrality in Internet, telecoms and data protection regulation”. Hogan Lovells Global Media and Communications Quarterly. 2014.

[31] H. Nissenbaum. “Privacy in Context: Technology, Policy, and the Integrity of Social Life”. Stanford, CA: Stanford University Press. 2010.

[32] P. Janes. “People, Process and Technologies Impact on Information Data Loss”. Information Assurance and Security Integrative Project. Sans Institute, November 7. 2012.

[33] J. van den Hoven, M. Blaauw, W. Pieters and M. Warnier. Privacy and Information Technology. Stanford Encyclopedia of Phyloshophy. 2014.

[34] M. Lubis., M. Kartiwi and S. Zulhuda. “Privacy and Personal Data Protection in Electronic Voting: Factors and Measures”. Telkomnika, vol.15, no.1, March 2017, pp.512-521.

[35] M. Lubis and F.A. Maulana. Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia. IEEE ICT4M 2010, pp. C-13-19.

[36] L. Eboli and G. Mazzulla, “An Ordinal Logistic Regression Model for Analysing Airport Passenger Satisfaction,” EuroMed Journal of Business Vol. 4 (1), 2009, pp. 40-57. DOI 10.1108/14502190910956684.

[37] A. Ahlan, M. Lubis and A.R. Lubis. “Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures”. Procedia Computer Science, 2015. 72, 361–373.