Protection of User Data Privacy in Presidential Election Campaign: Learn From United States' Case

Schancya Gillian W, Eko Purwanto, A. Hasan Al Husain, and **Nurul Safitry Fathullah**

Postgraduate Department of Communication Science,
Hasanuddin University, Makassar

Abstract

In this modern era, social networking has become very popular, with most people using the services of several social media platforms. With the increase in the use of social media, the issue of privacy of personal data has arisen. This paper will discuss the issue of private data protection in Indonesia ahead of the 2019 Presidential Election. It will also discuss the impact of the unauthorised use of personal data obtained from social media accounts, especially Facebook. This study employs the analytical and descriptive research methods. Data collection was done by literature research; library research was performed to obtain secondary data, and a literature review of some online media references, such as online magazine sites from several countries. We conclude that there is no legal umbrella protecting Indonesians with respect to the safety of their personal data. Therefore, the country may be vulnerable to cyber media-based campaigns as we move towards the 2019 Presidential Election.

Keywords: Social Media; Facebook; Data Privacy; Presidential Election

Introduction

In every social circle, almost everyone who uses smartphones has social media accounts, like Facebook, Twitter, Path, Pinterest, Instagram, etc. This situation has changed the way people communicate with each other in this modern era. In the past, people were more acquainted and relied on face-to-face interaction to get information.

Facebook, which is a social networking site launched in February 2004 in the United States, has become famous all over the world in recent years. According to official statistics, there are 845 million active Facebook users per month (Facebook, 2012). People can stay connected with friends, relatives, and close associates to share and reveal what is important to them and to discover what is going on in the world on Facebook (Winter K.W. Wong, 2012). Therefore, a person's privacy must be maintained on the site as it concerns the user's data.

Facebook has Terms and Conditions on user privacy, as written in the Facebook Privacy Principles:

> Facebook is built to get people closer; we help you connect with friends and family, find local events, and find groups to join together. We realise that people use Facebook to compare, but everyone wants to share everything with everyone, including us. It's crucial that you have a choice when it comes to how your data is used. Here are principles that guide our approach to privacy on Facebook (Facebook, 2018).

Perhaps if we are careful in creating social media accounts, we must first read the terms and conditions of confidentiality, because we include personal data in the site, such as real name, address, age, occupation, religion, and others.

In Facebook Privacy Principle, there are points about Facebook keeping user's information; in this regard, personal data will be maintained. The end reads as follows:

> We work hard to keep your information safe. We work around the clock to help protect people's accounts, and we build security on every Facebook product. Our security system runs millions of times every second to help capture threats automatically and delete them before they reach you. You can also use our security tools like two-factor authentication to help keep your account a lot safer (Facebook, 2018).

By this point, Facebook has a commitment to its users to keep personal accounts from unauthorised persons, and it must be done by managers of every social media site for the privacy and convenience of users.

Private data is data in the form of identity, codes, symbols, letters or numbers that are associated with a particular person (private). The term data protection was first used in Germany and Sweden in the 1970s, and it involves the protection of personal data through legislation. Obviously, in practice, there have been many violations committed by both government and private parties. However, personal data should not be misused, hence the necessary adjustments related to the problem of personal data (Latumahina, 2014).

In 2016, United States of America held a presidential election, with the major candidates, Hillary Clinton and Donald Trump, campaigning aggressively using various strategies to ensure victory. The winning team (Donald Trump's campaign team) engaged the services of Cambridge Analytica. Cambridge Analytica (CA) was a British political consulting firm that combines data mining, data brokerage and data analysis with strategic communication for election processes (Cambridge Analytica Politica, 2018).

Cambridge Analytica was contracted by the Trump campaign team, and they provided an entirely new weapon for the electoral battle. In addition to using

demographic segments to identify voters, just like the Clinton campaign did, Cambridge Analytica also performed psychographic segmentation. Demographics refers to information related to the class, education, occupation, age, etc., of a group or population. According to Suwarman, psychographics is an instrument used to measure lifestyle; it provides quantitative measurements and is used to analyse extensive data. Psychographic analysis is typically used to look at market segments; it is also interpreted as a consumer research that describes the consumer segment regarding their lives, jobs, and other activities (Suwarman, 2001:58).

In April 2018, a serious case about the unauthorised use of Facebook account data by Cambridge Analytica emerged. The data of as many as 50 million Facebook users from the United States was accessed and used by Cambridge Analytica. Christopher Wylie, former head of research at Cambridge Analytica who becoming the whistleblower in the case, designed the Psychological Operation (Psyop); this is an operating system to convey specific information, affect the user's emotions, motivate, and provide objective reasons. To explore voters, they collect many people's data to build their psychological profiles (kompas.com). Cambridge Analytica made efforts to construct and frame community thinking in determining its choice in the 2016 election in the United States.

At that time, there was an app called "This Is Your Digital Life" on Facebook, and this app could provide exclusive access not just to the personal data of the users of the app, but also the personal data of the network of friends of the app users. The app is able to retrieve the data of users, such as what they like, etc. The app was downloaded by 270,000 Facebook accounts across the United States, but its impact affected the data of about 50 to 60 million users (Kompas.com).

Indonesia, that will hold Presidential elections in 2019, does not have a specific policy and regulation on the protection of personal data. The provisions on this issue are still contained separately in several legislations and only reflect certain aspects of the security of personal data in general. Concerning the protection of private data in developing countries, Indonesia is vulnerable because it is yet to pass the Personal Data Protection (PDP) Act for its citizens. The provisions on this issue are not contained in a single legislation and only covers some aspects of the security of personal data. The regulations include the following: Law Number 7 Year 1971 regarding Principal Provisions of Filing, Law Number 8 Year 1997 concerning Company Document, Law Number 10 Year 1998 concerning Amendment to Law Number 7 Year 1992 concerning Banking, Law Number 36 Year 2009 on Health, Law Number 36 Year 1999 on Telecommunication, and Law Number 23 Year 2006 regarding Population Administration. It is relevant to note that fellow Southeast Asian nations, including the Philippines, Malaysia, and Singapore, have passed the PDP Law, while Brunei, Thailand, and Vietnam are discussing it in their respective parliaments. It is worthy of note that some countries in Africa whose digital infrastructure are not as good as that of Indonesia already have a PDP Act (Kompas.com).

The PDP Act serves to make people in a country feel comfortable in using social media, as it can safeguard their data in such a way that no one except the government may access them. The issue of theft of private data for business interests has occurred in Indonesia, but there has been no civil and criminal law action on the subject. So what if the case of using private data for politics and power interests, which happened in the United States, occurs in Indonesia? This issue is a very sensitive issue in the world today because personal data is basically secret data and only the owner of the account and the site manager should have access to it. This paper will discuss the issue of private data protection in Indonesia ahead of the 2019 Presidential Election. It will also discuss the impact of the dissemination of private Facebook data, which has created a new campaign concept. Countries where the Personal Data Protection (PDP) Act is not yet in force are more vulnerable.

Research Methodology

This research is a descriptive-analytical research. Data collection was done by literature research; library research was done to obtain secondary data, and a literature review of some online media references, such as online magazine sites from several countries.

The concept of reasonable expectation of privacy maintains that the government should ensure that a person's privacy is protected, except in the interest of law enforcement, such as interception of an individual's communication with other people for the purpose of obtaining information related to an investigation. Thus, this concept indicates that privacy is formulated relatively by the government and acceptable to society. This concept is used by judges in the United States to determine in court if a case involves privacy or not by normative generalisation (Riska Nurdinisari, 2013).

Discussion and Research Results

A. Private Data Protection in General

Technological advances have a significant impact on people's social life. Technology presents a wide range of facilities, one of which is the internet. Access to technological advances raises a serious question about the user's right to maintain the confidentiality of his/her personal information. It is common knowledge that due to information technology advances, it is now possible to gather, store, share, and analyse anybody's information at anytime and anywhere, so personal rights must be protected by the state. In general, personal data protection law covers issues about securing a person's data and allowing it to be used by others only with his or her consent.

Privacy is considered a part of human rights, and the personal data of a person is an important right to be safeguarded (Shinta Dewi, 2015). Privacy rights

has become an essential element for individual freedom and self-esteem. Its protection will undoubtedly be a driving force for the realisation of one's sovereignty in all things, such as politics, spirituality and, even, sexual activity. The protection of one's data is also a fundamental human right. Some countries have even recognised the protection of personal data as a constitutional right, i.e., a person is entitled to the protection of his/her data.

Article 1 of ASEAN Human Rights Declaration explicitly recognises an individual's right to his/her data. It should be emphasized that more than 75 countries have made laws for the protection of private data (Greenleaf, 2011). The right of privacy is understood as a form of confidentiality; it is the power of a person to disclose or conceal information about himself. Besides, there are differences in the scope, purpose, and content of privacy protection and data protection. Explicitly, data protection means protecting non-core values of privacy and is related to provisions for processing, approval, legitimacy, and non-discrimination of a person's personality. The expression of the concept of data protection is closely related to respect for the personal and family life of an individual. Private data protection is the key to many business and economic problems in today's modern era. Issues related to data protection has now extended into the political sphere. Current business practices often involve data manipulation, such as customer data segmentation, which is also applied in political campaigns. Data mining, data retrieval, creating individual profiles, consolidating global data processing, and other processes are currently used by businesses and politicians to gain advantage in their respective activities.

B. Protection of Private Data in Indonesia

Ahead of the presidential election to be held by Indonesia in 2019, political elites have registered as candidates for head of state. Therefore, it is expected that a serious competition to gain power would occur. The general election will take place simultaneously in all regions of Indonesia, and the presidential candidates will use every means at their disposal to win the hearts of the people, so that the people will choose them. In this digital era, the campaign is no longer done face to face or using picture and video images only. Politicians now have the option of using social media in the electoral battle.

Indonesia is one of the primary target markets of world-famous social media companies like Facebook, Twitter, Path, Instagram, etc. In this regard, Indonesia is included in the top 5 countries that have high numbers of social media users. Also, Indonesia became the country with the 4th highest number of Facebook users, with about 130 million users, and is estimated to hold about 6% share of the Facebook market, the same with Brazil (Kompas.com). The presidential candidates who will compete in the presidential election would go to any length to win the battle to become the ruler of Indonesia for a period of 5 years, until the year 2024. The existence of these social media channels and other technological advancements

offer opportunity to those who are interested to seek other people's data, thereby changing an old community system into a new community system with the use of digital channels.

The issue of data harvesting in the Facebook data scandal by Cambridge Analytica during the campaign period of the 2016 presidential election of the United States further exposes the urgency of the Personal Data Protection Act (PDP Act), even for Indonesia. However, Indonesia does not yet have a legal umbrella that covers the misuse of one's private data by social media companies, such as Facebook and others. So, it could be an easy task for an unscrupulous person to access and manipulate the personal data of Facebook users in Indonesia.

The fact that indonesia dose not yet have a Personal Data Protection Law (PDP Act) has a significant impact, as many people have recently talked about following the issue of data leakage in the process of prepaid SIM card registration. Moreover, after the incidents of theft of Facebook users' data, Americans were horrified, and this also impacted the people of Indonesia (Kompas.com). The PDP Bill was actually drafted in 2014, but there has not been a sense of urgency in the process of making it a law.

The applicable ITE Act in Indonesia does not yet contain specific privacy protection rules. Implicitly, this law provides for a new understanding of the protection of general and personal electronic data or information. However, in order to compliment the ITE Law with regards to elaborating on the issue of personal electronic data, Government Regulation No. 82/2012 on the Implementation of Electronic Transaction Systems and Transactions (GR no. 82/2012), which covers protection from unauthorised use, protection by electronic system providers, and protection from illegal access and interference, came into force.

Regarding the protection of personal data from unauthorised use, Article 26 of the ITE Law states that the use of any personal data in an electronic medium shall be subject to the consent of the owner of the data concerned. Any person who violates this provision may be sued for the damages incurred. Article 26 of the ITE Law states as follows:

1) The use of any information through electronic media concerning the personal data of a person shall be made with the consent of the person concerned.
2) Anyone whose rights are violated as referred to in paragraph (1) may file a lawsuit for damages incurred under this Act.

Article 26 of the ITE Law states that personal data is a part of a person's rights. However, the definition of personal data can be seen in Article 1 of GR no. 82/2012 is defined as specific individual data that is stored, maintained, and kept pure and protected by confidentiality. The definition of personal data by Article 26 of the ITE Law does not adequately explain what is included in an individual's data. Therefore, it is still necessary to reference the definition of personal data in other laws and regulations. For example, Article 84 of the Population Administration Act

(Adminduk Act) describes the personal data of the population that should be protected to include the following:

a. KK (Family Card) Number,
b. NIK (Population Identity Number),
c. Date, Month Year of birth,
d. Description of physical and mental disability,
e. NIK Biological mother,
f. NIK Father, and
g. Some critical event notes contents.

Concerning the protection of personal data by the Operation of Electronic Systems, Article 15 Paragraph (2) of GR no. 82/2012 stipulates that if an electronic system organiser fails in maintaining the managed personal data, they are required to provide written notice to the owner of the personal data. Article 15 Paragraph (2) of GR no. 82/2012 states as follows: "In the event of a failure in the protection of personal data being administered, the operator of the electronic system shall notify the owner of the personal data in writing."

This article does not specify the nature of the failure in question, but in general, the fault can be categorised into two: first, procedural confidentiality and security failures in data processing and, second, system failure from the aspects of reliability and security of the system used and the aspects of the operation of the electronic system as appropriate. Furthermore, the occurrence of system failure can also be caused by internal and external factors. One of the most common external factors is cybercrime. Judging from the type of activity, cybercrime can be hacking, cracking, phishing, identity theft, etc. The losses that arise include leakage of personal data, data manipulation, privacy violations, system damage, etc.

In other cases, with respect to the security of a person's data, the ITE Law provides legal protection against electronic interference and unlawful access. Any unlawful act by accessing electronic systems with the intention to obtain electronic information or documents by violating the security system is considered a criminal offence according to Article 46 and Article 30 of the ITE Law. This act is punishable by a maximum imprisonment of 6 to 8 years and/or a fine of not more than IDR 600.000.000,00 to IDR 800.000.000,00. Article 30 of the ITE Law stipulates as follows:

(1) Any person who knowingly and without right or unlawfully accesses others' computer and electronic systems in any way.
(2) Any person who knowingly and without right or illegally accesses the computer and electronic system in any way to obtain electronic information and electronic documents.
(3) Any person who knowingly and without right or illegally accesses the computer and electronic system in any way by violating, breaching, surpassing, or breaking the security system.

Article 46 of the ITE Law reads as follows:

(1) Any person who meets the elements as referred to in Article 30 Paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and a maximum fine of IDR 600,000,000.00 (six hundred million rupiah).
(2) Every person who fulfills the elements as referred to in Article 30 Paragraph (2) shall be punished with imprisonment for a maximum of 7 (seven) years and a maximum fine of IDR 700,000,000.00 (seven hundred million rupiahs).
(3) Everyone who fulfills the elements as referred to in Article 30 Paragraph (3) shall be punished with imprisonment for a maximum of 8 (eight) years and a maximum fine of IDR 800,000,000.00 (eight hundred million rupiah).

With regard to the protection of personal data in the form of electronic documents and electronic information, Article 32 of the ITE Law provides for the prohibition of a person from interfering in any way (such as modifying, adding, subtracting, transmitting, destructing, removing, transferring and hiding) with electronic documents or electronic information without rights and in a way against the law. Article 32 of the Law on ITE reads further as follows:

(1) Everyone who intentionally and unlawfully in any way alters, adds, subtracts, transmits, damages, removes, transfers, conceals any electronic information or electronic documents belonging to others or publicly owned.
(2) Every person who intentionally and without right or unlawfully by any means transfers electronic information or electronic documents to other unauthorised electronic systems.
(3) Acts as referred to in paragraph (1) shall be acts that result in the opening of electronic information or electronic documents with confidential nature becoming publicly accessible in an improper manner.

The threat of punishment is regulated in Article 48 of the ITE Law which reads:

(1) Everyone who fulfills the elements as referred to in Article 32 Paragraph (1) shall be punished with imprisonment for a maximum of 8 (eight) years or a maximum fine of IDR 2,000,000,000.00 (two billion rupiah).
(2) Any person who fulfills the elements as referred to in Article 32 Paragraph (2) shall be punished with imprisonment for a maximum of 9 (nine) years or a maximum fine of IDR 3,000,000,000.00 (three billion rupiahs).
(3) Every person who fulfills the elements as referred to in Article 32 Paragraph (3) shall be punished with imprisonment for a maximum of 10 (ten) years or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).

The provisions of several articles of the ITE Law, Adminduk Law, and GR no. 82/2012 are still quite fragile in their implementation because they only regulate the person's data being hacked by violating PSE's security system. In addition, there is a restriction if incidents of abuse of private Facebook data occur in Indonesia. There are legal issues between users and Facebook in accordance with the Statement of Rights and Responsibilities that have been approved by users and Facebook as the organisers of the electronic systems; the user agrees to submit all affairs or legal action of personal jurisdiction attached to any kind of legitimate subject, whether an individual or a legal entity, to a state or federal court located in the Santa Clara County. Subsequently, all disputes are to be resolved subject to the laws of the state of California, United States of America, irrespective of any legal contradiction (Facebook, 2018).

On the urgency of the problem of misuse of personal data, the Indonesian government must immediately pass the PDP (Privacy Data Protection) Act to ensure the safety of all its citizens both regarding physical security and the safety of private data. The alignment and uniformity of law should also be taken into account between the purposes of the PDP Law of the Ministry of Communication and Information and the Adminduk Law under the Ministry of Home Affairs; the Adminduk Law regulates the personal data of the population. There is a discussion component in the Adminduk Law that intersects with the PDP Law and must be aligned to avoid overlap.

The privacy of personal data is the recognition and protection of fundamental human rights under international, regional and national laws. Protection of personal information is a fundamental right mandated by the Constitution of the Republic of Indonesia. To protect the rights of individuals within the community, the privacy of personal information is a necessity. Adequate protection of privacy concerning personal data will increase public confidence to provide personal data or information to enhance public interest, with the belief that their private rights will not be infringed.

C. New Campaign Concept

A campaign is a communication activity aimed at influencing others to have insight, attitude, and behaviour in agreement with the will or desire of the dispenser or informer (Cangara, 2011: 223). The advancement of internet technology has generated a lot of interest, particularly the interest of politicians, with regards to employing it in the organisation of campaign communication strategy. Campaign activities such as money politics, campaign rallies, posters, and billboards are gradually been replaced in recent times. This concept of employing advanced technology in political campaigns first emerged after Barrack Obama's victory with the help of the social networking service Twitter. This new concept became the center of attention of several researchers of political marketing in all corners of the world, and Indonesia was not an exception. Political campaigns that initially only

talked about how a politician running for office should distribute economic gains to the electorate have moved on to a more advanced way of educating voters about the candidate's figure with the help of the internet as a new medium.

The internet and politics are interrelated. As the political scientist Roelofs says, "politics is a matter of speech or rather political activity is speech." Thus, in every political activity, there will always be a process to communicate. Humans make effort to interact with others to meet their needs. Activities on social media can provide an advantage for politicians to campaign for free and more efficiently. However, they must have excellent communication management for the drive to materialise. The numerous activities in the virtual world is the reason why politicians use the internet as a campaign medium. The creation of a society network, i.e. a social structure of society, in the early 21st century was made possible by digital network communication.

The network itself is a social structure formed from vertices (which are generally individuals or organisations) tied to one or more specific types of relationships, such as values, vision, ideas, friends, descendants, and others (Barnes, 1969). Therefore, the person who successfully holds full power over the communication within a network is in control of the conversations that occur within the system. In social media, it is not only the politicians that have an essential role in marketing their party or prospective leaders who will compete in the general election, but the public also contributes by responding to the political situation. Apart from commenting on political issues, with the use of social media, the community can organise its activities better. Public actions in responding to political issues on social media are a way of making bold statements and making the voices of the people and their aspirations louder.

Through the internet, we can know what the real responses from the community are about individuals who will participate in the elections. The internet also offers many benefits to politicians, among which are free publications through online social media services, such as Facebook, Twitter, and Instagram, as well as affordable tariff publications on websites. With these, the selling power or image of a politician can be quickly established. However, the effectiveness of internet use as a campaign medium is considered to still be relatively low. This is because the use of the internet as a campaign medium is still relatively new, and political parties as institutions that should provide civic education are considered to priorities conventional media, such as billboards and campaigning through specific groups of people.

However, it is possible that if the use of social media continues to evolve as a new political campaign concept, its effectiveness will increase. If we look at the issues around Trump's victory in the United States, it can be concluded that social media offers a new way for politicians to conduct their political campaigns by Psychological Operation (Psyop).

The Facebook scandal involving the use of private data without consent in the United States highlights this new campaign method, which contributed to the

victory of Donald Trump. This method could be applied by candidates involved in the political struggle for power in Indonesia. Cambridge Analytical, which was engaged by Trump's campaign, made efforts to build and frame voter opinion in making their choice through the use of social media, taking into consideration the class, education, religion, and age of prospective voters. The psychographic concept applied by Cambridge Analytical contributed to Trump's victory in the US presidential election in 2016.

The Psychological Operation (Psyop) created by Wylie made some people change their political tendency in the last US elections of 2016, because to change someone's political view, one must change the culture attached to him, since politics flows in the literature, as said by Steve Bannon. In economics, psychographic concept is typically used to look at the market prospects of firms, but with the development of the times, this concept has been adopted by political consultants to campaign for clients through online media.

Rogers and Storey (1987) define campaign as a set of planned communication actions to create a specific effect on a large number of audiences and is sustained over a period. Some communication experts recognise that the definition given by Rogers and Storey is the most popular and acceptable among communication scientists. So basically, a campaign is commonplace in the society. However, in some cases, the implementation of campaigns is not in line with the regulations that have been mutually agreed.

By using psychographic analysis to determine market trends, the tendencies of social media users in choosing candidates can be predicted if the personal data of the users have been accessed. Personal data could be obtained by distributing questionnaires to prospective voters through social media and looking to see where their political tendencies lie, but it is done in a way that social media users are not aware of the motive. This new campaign concept will be of interest to candidates in Indonesia, considering that Indonesia is a country with high use of social media.

Conclusion

Indonesia has not passed the PDP (Personal Data Protection) Law. However, the government has a responsibility to ensure the safety of all its citizens, be it physical safety or safety of private data. The draft of the PDP Act is still in progress since 2014, and till now, the development of the discussion is unclear. As we approach the 2019 Presidential Election, Indonesia could be vulnerable to cyber media-based campaigns, as there is no legal umbrella protecting the private data of Indonesians. The new concept of campaign using psychographic method is very promising for politicians, and they are likely to take advantage of the vacuum in law with regards to the protection of personal data.

Recommendation

Communities need to be educated to enhance their literacy in the use of social media; this will make them more careful in providing data to social media applications, like Facebook, Instagram, Line, WhatsApp, and other social media sites. The Ministry of Information and Communication together with the People's Legislative Assembly should accelerate the passage of the Personal Data Protection Act, which has been designed since 2014 but has not been realised to date. The government should also look at the alignment between existing laws and the laws that will be made. Due to the urgency of the problem ahead of the 2019 presidential election, all relevant parties, including Election Watch Institution (Bawaslu), Police Department, and other concerned bodies, should further improve their oversight of cyber media. The Indonesian people should learn from the US case and should, therefore, not be in a haste to share personal information, such as telephone numbers, addresses, etc., on the internet because the increasing sophistication of technology makes information more accessible.***

References

Barnes, J. A. 1969. Social Networks in Urban Situation: Analysis of Personal Relationships in Central Africa Town. Manchester: University of Manchester Press.

Cangara, Hafied. 2011. *Komunikasi Politik Konsep, Teori, dan Strategi* (Political Communication, the Concept, Theory and Strategy). Jakarta: PT. Raja Grafindo Persada.

Cambridge Analytica Politica, WITA (https://ca-political.com/casestudies/case studydonaldjtrumpforpresident2016). Retrieved on April 21, 2018, at 15:28 WITA.

Christopher Wylie, Student Disclosure of Facebook User Data Leakage, https://tekno.kompas.com/read/2018/03/23/10010067/christopher-wylie-mahasiswa-pengungkap-kebocoran-data-user-facebook. Retrieved on May 1, 2018, at 14.38 WITA.

Dewi, Sinta. 2015. "Privacy of Personal Data: Legal Protection and Form of Arrangement in Indonesia". Journal of De Jure, Vol. 15 Number 2, June 2015.

Facebook Privacy Principles, (https://www.facebook.com/about/basics/privacy-principles). Retrieved on April 18, 2018, at 18:56 WITA.

Greenleaf, Graham. 2011. "Global Data Privacy in a Networked World". https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1954296&rec=1&srcabs=2280877&alg=1&pos=10. Retrieved on May 1, 2018 at 16:35 WITA.

Kompas.com. "Indonesia, 4th Most Facebook User in the World", https://tekno.kompas.com/read/2018/03/02/08181617/indonesia-user-facebook-terbanyak-ke-4-di-world. May 1, 2018, at 15:57 WITA.

Kompas.com. "Indonesia Lost from Africa on Personal Data Protection Consciousness", https://tekno.kompas.com/read/2018/04/10/16185017/indonesia-kalah-of-afrika-soal-adaran-perience-perpection-data-personal. accessed on 2 May 2018, at 20:42 WITA.

K.W. Wong, Winter, 2012 "Discovery-SS Student E-Journal Vol. 1, 2012, 184-214 (http://ssweb.cityu.edu.hk/download/RS/E-Journal/journal9.pdf). Retrieved on April 18, 2018, at 16:25 WITA.

Latumahina. R. Elsina. 2014. *Aspek Hukun Perlindungan Data Pribadi Di Dunia Maya* (Legal Aspect of Private Data Protection in Cyberspace). Jakarta, Universitas Pelita Harapan.

Law of the Republic of Indonesia Number 19 Year 2016 About Amendment To Law Number 11 Year 2008 About Information And Electronic Transactions.https://web.kominfo.go.id/sites/default/files/users/4761/UU% 2019 % 20Year% 202016.pdf. Retrieved on May 2, 2018, at 10:05 pm.

Law of the Republic of Indonesia Number 23 Year 2006 concerning Population Administration. Source: http://www.dpr.go.id/dokjdih/document/uu/UU_2006_23.pdf. Retrieved on May 2, 2018, at 22:55 WITA.

Nimmo, Dan. 2014. *Komunikasi Politik (Komunikator, Pesan, Media)* Translate Edition: Political Communication (Communicator, Message, Media). Bandung, PT. Remaja Rosdakarya.

Nurdinisari, Riska, 2013 "Legal Protection Against Privacy and Personal Data of Telecommunication User in Telecommunication Operation Specifically in Receiving Spamming Promotion Information, University of Indonesia (http://lontar.ui.ac.id/file?file=digital/20334335-T32602-Rizka%20Nurdinisari. pdf). Retrieved on 21 April 2018, at 17:15 WITA.

Nurudin, 2001. Propaganda Communication. Bandung: PT. Youth Rosdakarya.

Rogers, E. M., & Storey J. D. 1987. Communication Campaign. Dalam C. R. Berger & S.H. Chaffe (Eds.), Handbook of Communication Science, New Burry Park; Sage.

Suwarman, Ujang. 2001. Consumer Behavior Theory and Its Application in Marketing, Ghalia Indonesia, Jakarta.

Zuckerberg Finally Lift Talk about Data Leak Facebook (https://tekno.kompas.com/read/2018/03/22/09070997/zuckerberg-first-lift-talk-soal-febocoran-data-facebook). Retrieved on 21 April 2018, at 18:52 WITA