International Journal of Engineering Science and Applied Mathematics
Volume.13, Number 12; December-2022;
ISSN: 2836-9521| Impact Factor: 5.78
https://zapjournals.com/Journals/index.php/ijesam
Published By: Zendo Academic Publishing

NAVIGATING THE LANDSCAPE OF PERSONAL DATA PROTECTION: CHALLENGES AND SOLUTIONS

[1]Balakrishnan, S

Article Info

Keywords: personal data, the rapid advancement, identity theft, data significant impact on society.

Abstract

While technology has made life easier and breaches, online privacy, data provided access to various systems and applications, it has also raised security, cyber-attacks, social concerns about the security and privacy of personal data. This paper networking sites, digital age, explores the challenges and issues related to implementing personal data user information, data disclosure protection in the digital age. The increasing number of identity theft risks. cases and personal data breaches serve as evidence that our data on the Internet is no longer safe. Despite these risks, there has been a surge in the number of users willingly sharing their personal information online, often without fully understanding the potential consequences. One major concern is the sharing of private information, such as identity card numbers, contact details, and email addresses, with third-party applications or systems without carefully reviewing the associated terms and conditions. This practice exposes users to the risk of identity theft and misuse of personal data. The value of personal data on the black market is staggering, reaching up to US$200 billion. Furthermore, popular social networking platforms allow users to disclose personal information, including their addresses, dates of birth, and personal photos, which increases the vulnerability of their personal data. Advertisers are particularly interested in accessing this wealth of user information for targeted marketing purposes. Cybercriminals also exploit various tactics, such as malicious software, to deceive users and obtain their personal data for illicit purposes. These attacks pose significant challenges to implementing effective personal data protection measures. This study reviews previous research conducted by students and experts to identify the challenges and issues associated with personal data protection. It provides an overview of personal data protection, discusses methods to safeguard personal data, examines the

[1] School of Computing, University Utara Malaysia, Kedah, Malaysia

different types of attacks used to disclose personal information, and proposes strategies to mitigate data disclosure risks

Introduction

First of all, the advent of technology seems to have a significant impact on society in recent years. As we all know, the development of modern technology has made life easier for everyone. It can be said that these technologies and Internet made easier for each of us to access the system or applications related to medical, transportation, industry and also the education within a second of time. As the result, there are many systems and applications are being developed in order to fulfil the requirements of the users and also with some hidden agendas where the personal information of users being collected. Basically, it can be stated that our data on Internet is no longer safe as there are many identities theft on it. Identity theft or personal data breaches is a current issue that affects everyone who access the Internet [1]. However, the number of users who sharing their personal data online are increasing although the reports regarding information theft are also increasing rapidly.

Nowadays, it can be said that everyone has the access to others' personal information, whether it is a company or any users are able to jeopardize our personal data which we may not have volunteered by ourselves [2]. The main issue is the users are sharing private information such as number of the identity cards, name, contact details, email and others to a third-party software or application or even a system in order to sign up or to get free gifts without reading the terms and conditions applied which will be resulting in identity theft or misuse of personal data. Based on the previous finding, it was said that there will various of consequences such as identity theft or stalking whenever a person shares personal information in an online platform [3]. This is because, users are not aware that their data is valuable. The data can be traded at a high price of US$ 200 billion [2].

Apart from that, social networks or social medias such as Facebook, WhatsApp, LinkedIn, Instagram, Twitter and others allow users to share their personal data such as contact details, address, name, personal pictures, date of birth and others which will be resulting in personal data disclosure. Usually, Social Networking Sites (SNS) are mostly rewarded by advertisers as it has an enormous base of users where they have a specified resource to target the user profiles as there is a higher possibility for the users to reveal the information through this targeting process [4]. There are some activities such as sharing images, updating user profile's information, uploading videos, posting status or story and even commenting on the other person's post could expose one's personal data identity [5]. Moreover, malicious software is being used by cybercriminals to trick or attack the victim to provide their personal data which will be used by them for the identity theft. There were various type attacks being used by attackers which causes a big challenge in implementing personal data protection.

This study is about the challenges and issues in implementing personal data protection based on previous researches done by other students and also researchers. The challenges and issues were identified by analyzing previous papers and also researches done by other students and also experts. Section 1 of the paper will an introduction to the personal data protection. Section 2 will contain the discussion about the protection of the personal data. Section 3 contains the challenges and issues in implementing protection on the personal data. The types of attacks used to disclose personal data will be discussed on Section 4. Section 5 will be explaining the methods to overcome personal data disclosure. Finally, the discussion and conclusion will delineate in the Section6

1 Literature review

Personal Data Protection Personal data refer to any information or data which related to any person which could identify them. Any person who can be identify through the use of a unique identity number, physical, mental, economics or even social characteristics [6]. Apart from that, A legislation or act intended to protect our personal data is known as personal data protection. Everyone, including businesses and governments, should use it to manage our data and safeguard us from data breaches. Moreover, personal data protection known as the personal

information privacy or personal data security where it is a set of principles that regulates on how sensitive data should be acquired and processed [7]. Personal data protection also ensures the data is accessed by those who have the authorization which will prevent it being misused [8]. There were around seven principles that have been used to form Personal Data Protection act in Malaysia. Table 1 summarizes the definition of those seven principles. Moreover, personal data can be classified into two category which are Personal Data and Sensitive Personal Data to [7].

Table 1. Principles of personal data

No	Principles	Definition
1	General Principle	Consumers are not authorized to use other people's private data without users' permission
2	Notice and Choice Principle	The data owner should be notified if the data user's personal data or information will be processed
3	Disclosure Principle	This is to specify the objectives for which personal information will be revealed.
4	Safety Principle (Security)	Data users are required to take specified actions to protect the user's data during the process from being manipulated, lost, misused, or even revealed.
5	Retention Principle	It specifies that personal information only can be maintained for as long as the main intent has indeed been fulfilled. When personal information is no longer required to be processed, it must be deleted immediately.
6	Data Integrity Principle	The data users must make sure that all the data gathered is complete, correct and also up to date in term of data underlying reason for processing and also storing.
7	Access Principle	It allows data consumers to access and amend their information, if it is inaccurate, deceptive, or outdated.

a) Personal Data

Personal data is any information related to a person. It can be a name, ID number, location, address, email, phone number, date of birth, pictures, data held by applications and also video clips. Moreover, credit card, account data, number plate are also considered as personal data. Any data or information which is can be used to uniquely identify a person is known as the personal information. **b) Sensitive Personal Data**

Sensitive personal data is a piece of information any user's personal health. aspect of religion, political views, or religious views. Moreover, and information related to a person's treatment due to their wrongdoing is also considered as the sensitive personal data. Any data related to genetic, biometric data which could identify person is also considered as sensitive personal data. Sensitive personal data needs more security as it is sensitive where it should be processed in a specific method.

2 Challenges and issues in implementing personal data protection

2.1 Industry revolution 4.0

In the year 2011, the concept of Industrial Revolution 4.0 was introduced. Basically, this industry revolution works more with information compared to previous industry revolutions. Personal data is being frequently shared in order to generate Device-to- Device and also Machine-to-Machine communication. There were a lot of security

challenges in this revolution. The privacy of the personal data needs more investigation in the era industry revolution 4.0 [9]. This revolution is exposing maximum personal data that the world has ever seen before. The following are some of the industrial revolutions 4.0 technologies that expose personal data information.

Artificial intelligence. Ai technology, commonly known as machine's intelligence. It is the intelligence represented by machines, nor natural intelligence demonstrated by humans or animals [10]. Basically, Artificial Intelligence or better known as AI is the top challenge in implementing personal data protection. This because Artificial Intelligence will cause privacy risk. For example, real time image processing tools or technology will reveal our identity and at the same time it will also leaks our personal data. They were some big issues of AI were found in term of data privacy such as they are no standard privacy for the AI related technologies resulting in personal data leakage and also inefficiency of gathering data from users with consent [9].

Virtual reality (VR) and augmented reality. Virtual Reality brought the same elements to the next level by creating a completely computer-generated recreation or simulation of a different environment. Next, augmented reality is more efficient than VR as it can accessed by almost everyone with a smartphone. However, both of these technologies becoming a challenge to implement personal data protection. This is because we are required to share some of our personal data in order to enjoy the Virtual Reality and Augmented Reality environment [9]. It can be said each of the application that offers this AR and VR technologies are gathering personal data such as location address and also biometric data which could identify a person easily resulting in personal data leakage.

2.2 Social networking sites (SNS)

The ever-increasing popularity of the World Wide Web (www) has resulted in an increase in the types of services offered via computer networks. Users of these services have formed a new type of virtual society known as online social media. Social networking sites or often known as social media is a software or applications that allow communications, interactions, content sharing and also community-based input. Most of the websites are available for both computer and also mobile. It can be said that that social media has huge followings or users. There are numerous social networking platforms currently on the market, including Fb, LinkedIn, Instagram, and others. There are least 94 percent of the internet users have one account on social networking sites [11]. Around 74 percent of adults uses social network service [5]. This shows that the social networking is frequently used among us. Almost each social networking site (SNS) is built to allow people to share, read, post, download, and analyse information. Open communication is a typical strategy for attracting people' attention, building social capital, strengthening interpersonal relations, and advancing informational and wisdom societies [12].

Basically, users are required to create a profile in order to use this SNS where they will be sharing their personal information such as name, e-mail address, gender, personal interest and others. At the same time, some of the users are also sharing their information such as photos, videos, family background, stories, and status voluntarily [13]. Moreover, day-by-day the process of sharing personal data on social networks are getting simple. For individuals wanting to publish or disclose their personal information, a variety of social networking platforms are available. The act of personal data to others is known as self-disclosure. It establishes identity by allowing users to create profiles and exchange personal information, emotions, photos, and status updates [12]. Generally, virtual communities are characterized by anonymity among participants, so the information exchange in them works a little different [14]. Data breaches is something not new for us [15]. This is because, although the information sharing is between unknown or anonymous person but the risk of personal data leakage is very high as it might be misused by cyber criminals.

2.3 Internet of Things (IoT)

IoT, a term that refers to a collection of Internet-connected devices where it sends and receives data which is obtained by continuous monitoring of a set of criteria using the sensors [8]. There various type of IoT devices is available in marketing, such as smartwatches, smart door locks, drones, and fitness trackers. All of this device and the application associated with it will process the collected sensor data and use it in order to service the

customer or the users. However, most of the application requires data from users to improve their service. For instance, a smartwatch required to record the hand and leg movement by capturing the angular distance in order to improve the result produced by the smartwatch. Moreover, most of the fitness tracking wrist-band allow the users to share the personal data on social media which will be resulting in personal data breaches by unauthorized person.

The fitness devices, health monitoring device or system, smart home appliances, will boost the gathering, exchange and also the sharing of personal data of the users within the apps [16]. Internet of Things is increasing the risk of the inferential attacks as there are more personal information about individuals and their actions is transferred among the devices. Usually, inferential attacks based on the data mining method where it will try to reveal unknown information to the attacker. Furthermore, one of the most critical aspects of user data disclosure through IoT devices is that it will be used for the security attacks, such as phishing and also bypassing the authentication.

2.4 Lack of awareness among users

Nowadays, users are sharing a higher rate of personal data through online although there are many identity theft issues being reported. This is because the users are lack of awareness on the importance of personal data protection which become a big challenge and issue in implementing personal data protection. Most of the users are unaware of the dangers or threat of posing personal data online [1]. Most users are unconcerned about revealing their sensitive information on the internet since they are unaware that their information could be exposed to data breaches or theft. This is because social media becomes an attraction for everyone which causes their data being exposed without their acknowledgement. User's upload their pictures into social medias such as Facebook, WhatsApp and majority of them thought it acceptable to label the images with their names, the names of their friends, and the place where the shot was taken without realizing they are sharing their personal data to a third person [3]. Another element that leads to this phishing scam is Malaysians' lack of cybersecurity understanding and awareness about phishing [17]. This shows that the lack of awareness is one of the challenges and issues in implementing personal data protection as it causes the users to share their information without knowing the consequences.

3 Type of attacks on personal data

3.1 Phishing attacks

Phishing is one of the most destructive, damaging, or widespread challenges to people's personal information. When an attacker pretends as a trustworthy contact, the victim is persuaded to click on a phishing link, download a malicious file, or provide sensitive personal information, bank account information, or passwords. Basically, the attackers will make sure that they create a good relationship with the victim until they believe them. The goal is to make it as simple as possible for victims to disclose their personal information such as passwords, usernames or even credit card numbers. There are more than 100 reports being done to PDRM per day regarding this phishing where most of the cases are Vishing where the phishing is conducted through phone calls, Smishing where it is done via Short Message Service (SMS) and lastly Spear Phishing [17]. All the contact details were gathered by the attackers through the social medias, IoT applications used by the victims.

3.2 Malware

Malware is one of the most significant hazards to the personal data. Initially, the malware was developed to discover the machine's vulnerability [18]. But now there are wide range of malware which covers a big range of cyber-attacks, including viruses and also trojans. In general, it is a set of harmful code developed by hackers in order to get access to a network or system, steal sensitive data, or even corrupt or wipe records from a system. Usually, malware will be spread by malicious links, spam emails or malicious downloads. According to [19], there was a fake coronavirus email which is known as "Trick Bot Malware Byte" emerge as a spam campaign during the pandemic Covid-19. Hackers are now using this strategy because it allows them to send emails

containing harmful code in order to attack user personal information. Most of the social media users a tends to be the victim of this malware as there are a lot of malicious links on it. For instance, most of the users click the malware links that pretend to be a "Free Giveaway Links" on social media and insert their personal data in order to win the gift without realizing it is a malware link. At the end, their personal data will be misused by some unauthorized person for their own benefits.

3.3 Ransomware

Every year, hundreds of individuals are affected by ransomware. Ransomware is a form of malware that intercepts user files and related assets utilizing security measures like cryptography and then demands currency in return for the information [20]. Ransome malware is a sort of malware that infects computer that prevents a user from accessing the systems or files and demands ransom in return. Nowadays, ransomware is another emerging trend that targets a user's personal information. The attackers are targeting users by demanding big amount money as the ransom, or else their personal data will be published. Individuals will be facing a difficult decision: pay the ransom or risk losing a significant amount of money and also their personal data. This form of attack is getting more prevalent as the majority of individuals accessing technology via the internet rises every day.

4 Methods to implement personal data protection

4.1 Set up stronger password on devices

First of all, users should set up a for the devices such as laptops, handphones, iPad, and tablets as it is easily to be lost or stolen by someone. So, it will be easier for the thief to access the information in the devices if we didn't set up a password to login into our devices. Most of the users have a habit of repeatedly using same and simple password as it is easy to be remembered. However, this is bad behavior because it's not difficult for cybercriminals to gain access to additional of the users' accounts once they figure out a password. Strong, long and random passwords are the most secure, where the users should set up password with at least 8 to 16 characters of password with the complex combination of uppercase, lowercase, numbers, and also symbols. To create and manage passwords, users should consider utilizing a password management tool as it will store the users' passwords securely. Moreover, users should avoid to use their personal information that other people knows or it is stated in their social medias as the password. For example, their name, birthday date, children's names as it is easy to be guessed.

4.2 Avoid opening unnecessary emails from unknown resources

Spam mails is becoming a trend today. Users should not open any emails from an unknown source or person. Apart from that, users also should not click any of link or file attached to the emails as it might be a malicious link that collect personal data of the users. Users also should not open any emails that contains files with the extension of ".exe" as its executable file which will works once it is been clicked. Users should delete it and avoid forwarding it to others if they are not sure with the content of the email or files. This is because most of the files might contains phishing software. Phishing emails are among the most popular ways for hackers to obtain personal details, as they trick the user into unconsciously handing over their login information to savings accounts, bank cards, as well as other accounts, enabling them to obtain additional information, end up making unauthorized purchases, or perhaps even defraud their authenticity. Targeted users by phishers in the hopes that they will click on harmful links containing viruses and malware. The best course of action is to avoid clicking on the link to avoid unnecessary personal data breaches.

5 Conclusion and recommendations

Personal data is data is any data that solely related to an individual. Data protection and privacy are inextricably linked. Individuals require the correct tools and skills to implement personal data protection and to protect their data from being misused by unauthorized person. It's also critical that those processing data understand their responsibilities so that they can take steps to preserve the users' personal data. Basically, this paper has discussed the challenges and issues that rise in implementing personal data protection, followed by a set of type of attacks

on personal data. This studies also has discussed some method to implement personal data protection in daily life. Finally, it is anticipated that this paper would assist future researchers in their studies on the subject.

6 Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by University Utara Malaysia.

REFERENCES

Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. Online Journal of Applied Knowledge Management, 3(1), 180–207.

Kamleitner, B., & Mitchell, V. (2019). Your data is my data: A framework for addressing interdependent privacy infringements. Journal of Public Policy & Marketing, 38(4). https:// doi.org/10.1177/0743915619858924 Rafique, G. M. (2017). Personal information sharing behavior of university students via online social networks. Library Philosophy and Practice (e-journal).

Shibchurn, J., & Yan, X. (2015). Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective. Computers in Human Behavior, 44, 103–117. https://doi.org/10.1016/j.chb.2014.10.059

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2016). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. New Media & Society, 20(1), 141–161. https://doi.org/10.1177/1461444816660731

Dokuchaev, V., Statev, V., & Maklachkova, V. (2020). Classification of personal data security threats in information systems. T-Comm, 14(1), 56–60. https://doi. org/10.36724/2072-8735-2020-14-1-56-60

Baskaran, H., Yussof, S., Bakar, A. A., & Rahim, F. A., (2020). Blockchain and the Personal Data Protection Act 2010 (PDPA) in Malaysia. In 2020 8th International Conference on

Information Technology and Multimedia (ICIMU) (pp. 189–193). https://doi.org/10.1109/ ICIMU49871.2020.9243493

Romansky, R., & Noninska, I. (2019). Cyber Space Features – Security and Data Protection Requirements. 2019 International Conference on Information Technologies (InfoTech). https://doi.org/10.1109/InfoTech.2019.8860880

Onik, M. M. H., Kim, C. S., & Yang, J. (2019). Personal Data Privacy Challenges of the Fourth Industrial Revolution. 2019 21st International Conference on Advanced Communication Technology (ICACT). https://doi.org/10.23919/ICACT.2019.8701932

Mohammed, Z. (2019). Artificial intelligence, definition, ethics and standards. Electronics and Communications: Law, Standard and Practice, 1–10.

ALQadheeb, B. E., & Alsalloum, O. I. (2021). Self-disclosure in social networking sites in Saudi Arabia. International Journal of Business and Management, 13(10), 1–96. https://doi. org/10.5539/ijbm.v13n10p96

Sharif, A., Soroya, S. H., Ahmad, S., & Mahmood, K. (2021). Antecedents of self-disclosure on social networking sites (SNSs): A study of Facebook users. Sustainability, 13(3), 1Meshi, D., Mamerow, L., Kirilina, E., Morawetz, C., Margulies, D. S., & Heekeren, H. R. (2016). Sharing self-related information is associated with intrinsic functional connectivity of cortical midline brain regions. Scientific Reports, 6(1), 1–11. https://doi.org/10.1038/ srep22491

Kim, J., Lee, C., & Elias, T. (2015). Factors affecting information sharing in social networking sites amongst university students. Online Information Review, 39(3), 290–309. https:// doi.org/10.1108/OIR-01-20150022

Riedy, M. K., & Hanus, B. (2016). Yes, Your Personal Data Is at Risk: Get over It. SMU Sci. & Tech. L. Rev., 19,

3.

Torre, I., Koceva, F., Sanchez, O. R., & Adorni, G. (2016). A Framework for Personal Data Protection in the IoT. 2016 11th International Conference for Internet Technology and

Secured Transactions (ICITST). https://doi.org/10.1109/ICITST.2016.7856735 [17] Balakrishnan, S. (2020). Phishing Related Crimes In Malaysia: Challenges & Solutions.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.

Cristea, L. M. (2020). Current security threats in the national and international context.

Journal of Accounting and Management Information Systems, 19(2), 351–378. https://doi. org/10.24818/jamis.2020.02007

Alshaikh, H., Ahmed, H., & Ramadan, N. (2020). Ransomware prevention and mitigation techniques. International Journal of Computer Applications, 177(40). https://doi.org/10.5120/ijca2020919899