Understanding Employees' Perception towards Personal Data Protection through Their Work Processes in Privacy Enhancing Technologies (PETs) Adoption

May Fen Gan[1], Hui Na Chua[2], Irene Ai Lian Tan[3], Siew Fan Wong[4]

[1,2,4] Dept. of Computing and Information Systems, Sunway University, Malaysia
[3] Centre for Teaching and Learning, Berjaya University College, Malaysia
*Correspondence: 11033420@imail.sunway.edu.my

ABSTRACT

With the increase of consumers' privacy concerns and the government-enforced regulations on data protection, it is necessary for organizations to implement Privacy Enhancing Technologies (PETs) to protect consumers' personal data. PETs refer to any protection in the form of technology. Since employees are the main stakeholders who are directly involved in the PETs implementation and execution process, it is important to understand employees' perceptions especially those daily tasks involving the process of collecting and processing consumers' data. Prior literature showed limited research on the effects of PETs implementation through employees' work process and their perception on the implementation in protection personal data. Hence, the purpose of this research is to explore how PETs adoption affects employees' work process and their perception. A qualitative single case study was adopted in a telecommunications company in Malaysia. Data were collected through in-depth interviews from nine respondents who were involved in data collecting, data processing and data controlling in their daily tasks. The results showed that employees experience difference levels of change depending on their work nature. The affected areas of change in implementing PETs are workload, communication level and data access. Employees also raised their concerns on vendors' accountability. This research provides an insight into employees' perception towards personal data protection based on their experience in implementing PETs. Continuous awareness, updates, monitoring and evaluating of system are perceived as the key to successful PETs implementation in protecting personal data.

Key words: Privacy Enhancing Technologies, Work Process, Perception, Information Privacy, Personal Data Protection, Technology Adoption

INTRODUCTION

With today's technology, data is easily accessible anywhere and anytime. Consumers use their information in exchange for the organization's services. Organizations make use of data in their daily operations, including personal data. There were 3,813 breaches reported from January to June 30, exposing over 4.1 billion personal data records (Risk Based Security, 2019). The advancement of technologies and the interconnectivity of networks providing unprecedented methods of collecting, analyzing and disseminating personal information on individuals increases and thus, consumer's concern of invasion of data privacy and the potential of invasion increases (Hinde and Ophoff, 2014). Numerous countries including European, America and Asia regions have adopted data protection act, such as European General Data Protection Regulation (GDPR) (General Data Protection Regulation, 2016), Freedom of Information Act 2000 (Freedom of Information Act 2000, 2019) and Singapore Personal Data Protection Act 2012 (Personal Data Protection Act 2012, 2019). In Malaysia, the government has enforced Personal Data Protection Act in 2013 to protect consumers' personal data in any commercial transaction process (PDPA, 2013). Despite the government enforcement and mandated adoption by organizations, it is reported that the rate of data breach increasing over the years (Verizon, 2019).

Privacy Enhancing Technologies (PETs) are adopted by organizations to serve as a data protection tool for protecting consumers' personal data. PETs refer to any security and privacy protections in the form of technology. In addition, technological developments create more regular and accurate reporting of

information, increased automation of control which provides further assurance on compliance and decrease in human errors (Gozman and Currie, 2015). PETs are often referred as a combination of several technologies to protect data and enhance privacy. However, many organizations do not implement PETs extensively despite the advantages of PETs. This might be due to insufficient support from current regulations (Borking, 2011), and lack of user availability and user-friendliness (Borking, 2011; Phillips, 2004). Furthermore, prior research showed little attention has been given to how PETs adoption influence employees' working processes.

Prior studies indicate that there will be a change in the organization during new technology adoption. Vakola (2014) shows that employees have different perception towards organizational change. Employees need to adopt the new technology and familiarize with it. With the changes in working processes, there are almost no systematic investigation on the impact of technology on employee job characteristics (Venkatesh, 2006).

Past researches (Foth, 2016; Ifinedo, 2012) showed that employees' behaviour positively affects employees' compliance. Therefore, it is important to understand employees' perceptions towards data protection through their work process in PETs adoption as they are the main stakeholders who are directly involved in the personal data protection implementation and execution process of protecting consumers' data (Bulgurcu et al., 2010). Hence, the aims of this research was to answer two research questions, (1) How does the PETs adoption affect employees' working processes? and (2) How do employees perceive personal data protection through PETs adoption? The findings of this research provide insights that urge organizations to formulate more efficient work processes and sustainably effective PETs management system for personal data protection.

2 Literature Review

2.1 Personal Data Protection (PDP)

Personal data protection (PDP) is the process of protecting personal data in collecting, disseminating, processing and storing of personal data (PDPA, 2010). Organizations collect consumers' personal data in exchange for their services. Consumers' privacy concerns will
lead to their willingness to disclose personal information (Xu et al., 2011). Moreover, consumer loyalty can be easily lost when an organization experience privacy breach (Choi et al., 2016). Both organizations and government officials are responsible for ensuring consumers' personal data are safe and secure (Thompson et al., 2015). Organizations introduce accessible privacy policies (Wu et al., 2012) and organizational self-regulation (Xu et al., 2011) to overcome individuals' privacy concerns and gain individuals' trust. Governments in different countries enacted personal data protection act such as the Personal Data Protection Act (PDPA, 2010), the European General Data Protection Regulation (General Data Protection Regulation, 2016) and the USA Federal Trade Commission's Fair Information Practice Principles (Federal Trade Commission, 2000) to protect personal data.

The use of technology can help to solve consumers' privacy concern and ensure that personal data is protected (Van den Hoven et al., 2014). Examples of these are the Privacy Enhancing Technologies, platforms for privacy preferences, access control and tracking systems (Borking and Raab, 2001). Hence, effective organizational data protection can be achieved by taking people, process and technology into consideration.

2.2 Privacy Enhancing Technologies

The European Commission defines Privacy Enhancing Technologies (PETs) as "a coherent system of Information and Communications Technology measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or desired processing of personal data, all
without losing the functionality of the information system" (Economics, 2010). In PETs, technology is used in achieving compliance with data protection legislation.

PETs were implemented for different data protection purposes which may include either or both privacy and security protection features. According to Chan et al. (2016), PETs include technology protection for both personal and non-personal data. Thus, PETs contain both privacy and security protection features. The implementation of PETs is not limited to specific techniques as it can be a new technology or an improvement of existing technologies (Van Blarkom et al., 2003). Examples would include networks and firewalls (Olivier, 2003), cryptographic systems (Phillips, 2004), credential system (Shen and Pearson, 2011) and Context and Identity Management (Danezis and Gürses, 2010).

Past research on PETs mostly focused on the design and implementation of the technology such as biometric authentication framework (Yanikoglu and Kholmatov, 2004), blockchain (Zyskind and Nathan, 2015) and morphing based method (Korshunov and Ebrahimi, 2013). Many studies (Cha et al., 2018; Curzon et al., 2019; de Roode, 2016; Huang, 2019; Piras et al., 2019) focused on the designing and implementation of PETs based on GDPR.

Companies such as Google, Facebook and Microsoft Office are committed to complying with data protection laws such as GDPR, Health Insurance Portability and Accountability Act (HIPAA) and California Consumer Privacy Act (CCPA) (Brill, 2018; Facebook, 2019; Google, 2019). Microsoft provides several PETs such as data breach notifications, compliance manager and GDPR control mapping to support GDPR accountability (Microsoft, 2019). In Malaysia, there is a limited number of PETs studies in complying to PDPA. This may be due to the lack of awareness of PDPA (Chua et al., 2018).

Organizations can ensure data protection by applying PETs and streamlining personal data processing (Borking, 2011). For example, Privacy and Identity Management for Europe (PRIME) project has developed user-centric privacy-enhancing and transparency enhancing technologies (Fischer-Hübner and Hedbom, 2008). The importance of adopting PETs include compliance with data protection legislation, increase consumers' trust, increase competitive advantage and increase security (Fischer-Hübner and Hedbom, 2008).

2.3 Employees' Perception & Attitude towards PDP

The execution of PDP depends strongly on employees as they are the ones who collect, process, store and disseminate personal data. Human factors are one of the weakest links in attempts to secure systems and networks (Imgraben et al., 2014). Desjardins Group, a large Canadian financial institution, experienced roughly 2.7 millions data leaked due to an employee improperly collected information about customers and shared it with a third party outside the financial institution (Shingler, 2019). Although employees are considered the weakest link in data protection, they are also responsible for reducing personal data risk (Bulgurcu et al., 2010).

Past researches have shown that individuals' behaviour on protecting privacy is affected by psychological factors using behavioural-related theories such as Theory of Planned Behaviour (Ajzen, 1985), the Protection Motivation Theory (Mady and Gupta, 2017; Rogers, 1975), the Theory of Reasoned Action (Bulgurcu et al., 2010; Fishbein and Ajzen, 1975) and the General Deterrence Theory (Williams and Hawkins, 1986).

Previous studies have examined that attitude toward PDP has positive influence on employees' intention to comply (Foth, 2016; Ifinedo, 2012; Pahnila et al., 2007). Blythe et al. (2015) conducted a study that aimed to identify the motivators and barriers of employees' security behaviour. The results showed that response evaluation, threat evaluation, knowledge, experience, security responsibility, personal and work boundaries, and security behaviour explained why employees engage in security action. An introduction of a new workload increases employees' stress level and subsequently impacting employees' decision to comply (Lee et al., 2016). Moreover, employees choose to ignore information security policy practices when they are not able to cope with their daily job routines (Post and Kagan, 2007).

2.4 Impact of Employees' Work Process on Technology Adoption

During technology adoption, the organization's procedure and employees' working routine will be affected. A successfully implemented technology should not overlook employees' factor (Ko et al., 2016). Employees perceived that technologies affect them positively and negatively. For example, employees think that information and communication technology can improve their ability to do their job, to share ideas with co-workers and have more flexible working hours (Madden and Jones, 2008).

In a qualitative research on the impact of information and communication on technology on employees conducted by De Wet et al. (2016) showed that employees perceived technology as a medium to increase effectiveness and productivity at work, increase their availability, provide easy access, save time, help them to establish and maintain virtual access, increase competitive advantage of organization, facilitate obtaining and sharing of information and support globalization. The negative effects that employees perceived are increasing work demands and hours, increase in stress levels and the difficulty of disconnecting from work when at home (Madden and Jones, 2008). Additionally, employees think that information and communication technology adoption increased pressure and acted as an excuse to avoid direct communication (De Wet et al., 2016). The consequences of adopting new technology includes change in job responsibilities, added workload, additional training and personnel (Delaney and D'Agostino, 2015).

3 Methodology

This research adopted a single qualitative case study method to investigate the research questions. The rationale of choosing a qualitative case study approach is based on the following justifications:
Firstly, it allows researchers to understand and discuss the situation of the problem on the ground through the support of the qualitative data generated from the perspectives and experiences of the participants (Merriam, 1998; Ticehurst and Veal, 2000).

Secondly, qualitative case study is used to develop a fully rounded understanding of an un-investigated case (Silverman, 2013). Therefore, this approach was chosen for our research subject that is less understood and has been less investigated in the past (McGivern, 2006). Thirdly, using qualitative single case study enables researchers to understand the nature and complexity of the process that is taking place and gain an in-depth understanding of the phenomenon through case study (Cao et al., 2014). Fourthly, it explains an intervention or phenomenon and the real-life context in which it occurred (Merriam,
1998; Yin, 2013).

In this research, there are several reasons that a qualitative single case study is a suitable method:

- This research allows us to explore the importance of PDP through employees' perception and experience.
- The enforcement of PDPA is considered new and the organization is undergoing the process of adopting PETs to comply with the act.
- There is a lack of rich, in-depth, qualitative understanding on how employees adapt to the new environment in Malaysia.
- Employees' work process in implementing PETs adoption is an area which has been less understood and less investigated in the past.

3.1 Sampling

3.1.1 Sampling Criteria

The recruitment of respondents is based on purposeful sampling (Palinkas et al., 2015). There are several criteria in selecting the respondents. As a single case study, this research investigated employees from a large mobile telecommunications service provider organization (denoted as TELCO). The respondents are TELCO's employees who work in the telecommunication industry before and after PETs implementation for data protection regulation compliance. Moreover, the respondents are employees who are involved in the process of personal data management, i.e., collecting, processing and controlling personal data using PETs. Telecommunication industry was targeted because it processes a large amount of data in everyday transactions. The respondents were chosen with the rationale of discovering the impact of employees' working processes on PETs implementation.

3.1.2 Respondents Recruitment Protocol

A rare and favourable opportunity was given to study employees' working processes on PETs implementation through a senior manager from the Data Science Solution department in the TELCO company. The senior manager recommended several names that were thought to fit the study. The potential respondents given by the senior manager was contacted through phone call, which included a short description of the research and its purpose. The respondents that accepted the interview were then arranged for a face-to-face interview. More respondents were recruited through snowball approach.

3.1.3 Sample Size Justification

Researchers like Thomson (2011) is of the view that there is no fixed amount of sample size in conducting qualitative research. Marshall (2013) believes that in a review of qualitative research sample size, it shows no apparent effort in sample size justifications even with the citation of recommendation from qualitative methodologists. According to Lancaster (2017), those who turned down interview invitation were due to their unavailability or concern of exposing their organization's information where recruitment with purposive criteria for this case study shared the challenges in getting access to the targeted respondents.

3.1.4 Respondents' Demographic

The criteria were selected in order to ensure recruited respondents have experience in using PETs and were involved in the implementation. Out of the 20 employees who met the recruitment criteria, 9 of them participated in this research. The respondents' demographic can be found in Table **1**. The participation was voluntary and the respondents were ensured of anonymity.

Table 1: Respondents' Demographic

Respondents	Position	Department	Work experiences (years)
R1	BI Development	Business Intelligence	16
R2	BI Dashboard Developer	Business Intelligence	6
R3	Big Data Engineer	Data Science Solution	4
R4	Big Data Analyst	Data Science Solution	7
R5	Manager	Data Science Solution	4
R6	BI Development Lead	IT	5
R7	Data Engineer	IT Transformation Enabler	15
R8	Zoom Analytics	Strategic Analysis	7
R9	Governance	Security Governance	11

3.2 Data Collection

The method of collecting data in this research was interview. Interview was chosen because it provides researchers in gaining insights, understanding of opinions, attitudes, experiences, processes, behaviours, or predictions (Rowley, 2012).

The interview questions were semi-structured as it allows other related questions to be raised and explored during the interview. Each interview session lasted with an average duration of 1 hour and 30 minutes. Research ethics application was approved (Sunway University Research Ethics approval code: SUREC2016/020) before conducting the interview. The benefit of conducting a face-to-face interview is to collect responses provided by the respondents and seek clarification of questions instantly (Ryan et al., 2009).

During the interview sessions, all data were audio-recorded with the permission of the interviewees. All the transcribed audio and the data were kept off-line and only accessible by the researchers that were involved in this research. Besides that, all the interview responses remained confidential and were not discussed with any fellow interviewees. The data will be deleted after the completion of this research.

3.3 Data Analysis

In this research, thematic analysis (TA) is adopted (Braun and Clarke, 2006) to analyze the data due to its flexibility in combing through rich and detailed yet complex data (Nowell et al., 2017). The following Figure 1, adapted from Braun and Clarke (2006), shows the TA method phases.

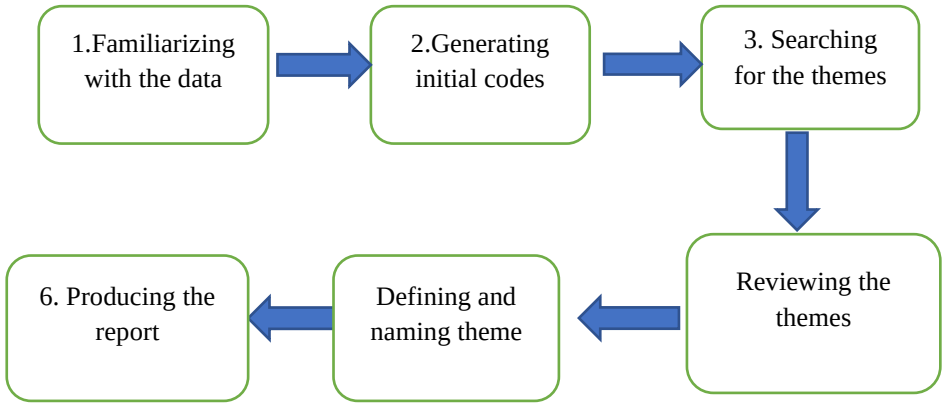

Figure 1: Six phases of thematic analysis (Braun and Clarke, 2006)

Several phases of data analysis in Figure 1 were employed. The first phase started by transcribing the interviews manually and performed several times. When there is an uncertainty of the content of statements, the audio was played several times to ensure that the statements were transcribed accurately.Next, two researchers conducted open coding individually. Both researchers met several times to share their analysis results.

Changes were made to the codes on reaching consensus between them. After that, two researchers collated the codes and put them into potential themes and sub-themes. For example, the codes are mindset, personal right, trust, honesty, the need of act, governance process, security team responsibilities and company responsibilities. These codes are merged to employees' attitudes, government and organization responsibility as sub-theme. The final theme is the different parties involved in protecting personal data. Both researchers discussed and agreed on the themes and sub-themes identified. Each theme and sub-themes were then defined.

3.4 Trustworthiness of the study

Several strategies were used to ensure the trustworthiness and rigor of this study. Lincoln and Guba (1985) defined the concept of trustworthiness by introducing four criteria in qualitative research: credibility, transferability, dependability and confirmability.

The trustworthiness of this research is achieved by applying researcher's triangulation and member checking. The second researcher checked the audio transcriptions that were transcribed by the first researcher to ensure that the correct transcriptions were recorded. Also, the two researchers performed their respective data coding and interpretation independently before meeting to discuss the differences and ensured that a consensus was reached on the final interpretation. For member checking, the transcription and a summary of the transcription are sent to the respondents and to confirm the accuracy of the data.

The purpose of case study research is not generalizability, but rather transferability. Transferability shows how and in what ways understanding and knowledge can be applied in similar context and settings (Bloomberg and Volpe, 2018). In this research, the case study does not represent the whole population of the telecommunication industry. However, it serves as a guide for future researchers to apply this method in another telecommunication industry or other sector. In addition, thick description is applied for establishing transferability (Trochim, 2006).

4 Results

In the process of discovering employees' work process, their work nature has been identified. The changes in employees' working processes vary from one another based on their work nature. We identified and categorized three groups of employees who have either direct or indirect access to consumers' personal data.

They are data user (R3, R6) – an employee who request data from data processor and data controller to perform work such as customer profile understanding and marketing; data processor (R1-R2, R4-R8) – an employee who has access to the customer' database and process data user request; and data controller (R9) – an employee that is responsible for defining data protection procedures and handling personal data request from data user.

4.1 Employees' perception on personal data protection through PETs adoption

The data analysis resulted in the identification of four themes:
(a) awareness of personal data protection,
(b) parties involved in protecting personal data stakeholder,
(c) effectiveness of personal data protection, and
(d) sustainability of personal data protection.

Each theme contains several sub-themes as shown in Table 2. The theme and sub-themes discovered employees' perception on PDP through their experience.

Table 2: Identified themes and sub-themes

Themes	Sub-themes
Awareness of personal data protection	Internal awareness factors
	External awareness factors
Parties involved in protecting personal data	Government (to enforce personal data protection regulations)
	Employees' attitudes (towards personal data protection)
	Organization responsibility (in implementing data protection)
Effectiveness of personal data protection	Justice need to be served - Employees' reflection (through own and others' experience)
	Organization support
	Self-efficacy
	Technologies' functions (to protect data)
	Holistic data protection process
Sustainability of personal data protection	Internal protection (continuous updates, monitoring & evaluation)
	External protection (vendors' accessibility control)

4.1.1 Awareness of personal data protection

This theme consists of two sub-themes that identified employees' awareness on PDP. The sub-themes showed how employees received information from different areas.

4.1.1.1 Internal awareness factors

Employees received information about PDP through email (R5, R9), and briefing (R7). However, many of them were not aware of PDP information until their work was involved (R1, R2, R4) or through their co-workers (R3, R6).

4.1.1.2 External awareness factors

Other than TELCO, employees also gained PDP knowledge from the media and banks (R2, R5, R8).

4.1.2 Parties involved in protecting personal data

This theme shows the need for different parties in PDP. These sub-themes illustrate three essential parties that are responsible for PDP.

4.1.2.1 Government (to enforce personal data protection regulations)

Employees shared their thoughts on how having PDPA can prevent privacy breach. Employees also think that ensuring PDP is part of government process. The law will intimidate the employees not to violate PDP. Different employees commented that:

> *"But now they treat it [technology requirement] other than common sense, they treat it as something that is governance process."* (R5)
>
> "*We can have rules then they are a bit afraid to give things to others. So, we can avoid that to happen."* (R7)
>
> *"It [PDPA] can protect us."* (R8)

4.1.2.2 Employees' attitudes (towards personal data protection)

Employees think that individuals' security behaviours are essential in PDP. Employees perceived values such as honesty (R1, R3), trust (R1, R7), greed (R2), individual responsibility (R2, R4, R5, R8, R9). Besides that, the trust between consumers and TELCO can be built by ensuring PDP (R4, R7). As the respondents commented:

"It's your customer information, you should protect it. With and without PDPA, it's your customer, you shouldn't let your customer information to go out." (R5)
"They [customer] will trust us more than previous… Because they [customers] know previously anybody can get their information right, they feel more secured." (R7)

4.1.2.3 Organization responsibility (in implementing data protection)

Organization is responsible in maintaining their PDP systems. In TELCO, they have a security department who handles all security and privacy-related issues. The department is responsible for maintaining their systems such as updates on anti-virus, firewall and encryption (R9). However, some of the employees (R1, R2, R3, R6) are not aware of the system updates or new technology for better PDP. Relevant comments:

"For the current system, we just make sure it is patch, we make sure that the system we use is protected. Meaning that, we do patching, update antivirus, firewall to prevent hacking or any threats." [R9]
"There is no change [on the system] since the implementation of the system" (R1)

4.1.3 Effectiveness of personal data protection

This theme is defined by a cluster of sub-themes that relate to employees' perceptions on the effectiveness of PDP. These sub-themes illustrate the importance of having an effective PDP.

4.1.3.1 Justice need to be served - Employees' reflection (through own and others' experience)

Employees shared their experience of PDP in TELCO and other organizations. In TELCO, they have experienced personal data leak caused by employees. Employee (R2) compared that the security level in previous organization is tighter than TELCO. With the current PDP policies and PDPA, employees are less likely to make a mistake again. Employees commented that:

"You have a friend inside [TELCO] that can have access to our system. So, the friend check and the person involving get to know and the person complain to [TELCO]. [TELCO] checked and find out that [TELCO] staff [does it] and the staff is being dismissed." (R1)
"With [PDP] enforced, it's not easy for those people to repeat the same mistake anymore." (R5)

4.1.3.2 Organization support

TELCO supports PDP by introducing new security department, providing new processes and guideline, providing data protection application approvals and training for employees. Overall, employees perceived that management fully supports PDP. Employees commented that:

"Management plays a big role which they actually allocate resources to do the data protection things" (R1)
"They [management] are supportive because PDP is a big concern for the company" (R9)
"[Training] for different system, yes. A training about the process also." (R3)

4.1.3.3 Self-efficacy

Employees perceived that their job scope would affect their competency in performing PDP task. The change of employees' work process impact employees based on different data groups. Different data group employees commented:

"Ya [increase workload]. First time, first second time, I think why have to go through all this? Because it's like burden. But, we have to understand la, all this implementation, there might be some reason right. We just follow, we just try to adapt." (R3)
"Easier for me to handle the requestor because half of it have been handled by the security team. If not, requestor, they actually don't know what they need also, but they just put whatever information that they want. So easier for us, when we have this kind of things, already filtered out and we just do our work." (R7)
"Same team same task. Just when this security comes in, so I have additional workload. Do governance work as well." (R9)

4.1.3.4 Technologies' functions (to protect data)

TELCO has implemented several technologies to protect personal data. The technologies include both physical and online protection. Employees think that having PETs are a useful tool in PDP. The list of technologies implemented for PDP is shown in Table 3.

Table 3: PETs

Technologies Used	Purpose	Before PDPA enforcement	After PDPA enforcement
Change of default password (R5)	The system password in the company	remain default password	change of default password
Encryption (R1-R7)	To encrypt personal information in the database.	No	!
Multicast File Transfer Protocol (MFTP) (R1)	To transfer data to the requestor	No	!
SSH File Transfer Protocol (SFTP) – Accellion (R7)	To transfer data to the requestor	No	!
Data Loss Prevention System (R9)	To track the use of network	No	!
ITCR Systems (R1-4, R6-R9)	For data request application	No	!
Access Control (R1-R7, R9)	To access the system	!	!
Video Surveillance (R5)	For security purposes	!	!
Anti-virus System (R8)	To safeguard computer from malware	!	!
Firewall (R6, R9)	To keep the computer safe and block intrusions	!	!
Virtual private network (R8, R9)	For employees who work from home and access company network	!	!
Access Control to server room (R1-R9)	For security purposes	!	!

4.1.3.5 Holistic Process for Data Protection

Although TELCO has implemented various methods in PDP, there are flaws in the current process. The current process monitors the use of personal data and the number of persons accessing the personal data after the application has being approved. Besides, external protection is as vital as internal protection. Employees shared their concern on external threats such as vendor accessibility as well. Relevant comments:

> *"They don't have, what we call that, system for monitor for all this kind of data movement. So, the most important is how to monitor this data movement."* (R6)

> *"Some vendors, they can have access, full access. [TELCO] is like this, the business in [TELCO], you have to always fast, very fast. If the boss say, tomorrow I want launch this product. Okay. You must implement. Ask vendor to execute now. For this, they have to get the full access. You cannot control. That is the problem. Right?"* (R3)

4.1.4 Sustainability of personal data protection

This theme consists of two sub-themes that relate to the sustainability of PDP. These two sub-themes demonstrate the need for both internal and external protection for PDP sustainability.

4.1.4.1 Internal protection (continuous updates, monitoring & evaluation)

TELCO has implemented several measures in protecting personal data. However, employees shared their thoughts on TELCO limited effort in maintaining PDP. Employees perceived that there is a lack of continuous awareness, monitoring, evaluating, tracking and updates. The employees commented:

> *"If, let's say, they [data users] want to keep it [requested personal data] for more than 3 months also I think, the security [team] also didn't check.* (R1)

> *"I don't think there is anyone who is responsible in evaluating or monitoring how's the system."* (R8)

> *"To improve the existence system, somebody has to be like moderator la… I mean, to check, there is somebody who own the system and track actually are we doing the correct, the right thing. There is no like moderator for that."* (R3)

4.1.4.2 External protection (vendors' accessibility control)

There is a need to sustain PDP from different areas. Employees mentioned that the monitoring and evaluating of vendors were lacking. Employees pointed out that TELCO protects personal data from vendors through non-disclosure form only. Employees shared their thoughts:

> *"[Vendors have] all the access, all the database control"* (R2)
> *"In most of our project, we engaged to the vendor. We engaged with the vendor. No one else like monitor what actually vendors access, permissions…"* (R3)
> *"All vendors are exposed to the raw data actually. They can see everything. But then I think vendor also sign NDA when they want to work with us."* (R4)

4.2 The impact of PETs adoption on employees' work process

This section identified the themes and sub-themes that are important in understanding employees' work process for different data groups before and after PETs adoption after PDPA enforcement.

4.2.1 Work process for different data groups

4.2.1.1 Data User

First, it shows that data users need to go through more processes in getting approval for data requests. Previously, data users could make direct requests to the data processors that they were familiar with. For example, they could write an email request (R6) or they could pick up the phone to call the data processors directly (R3, R6) to make a request. After PETs adoption, there is an introduction of the security team (i.e., data controller). The purpose of security team is to validate and filter the data requests (R9). Hence, the process of requesting data is more tightened as before.

In addition, as the process flow of requesting data increases, data users might delay in executing their tasks. The time taken for data users to complete their task is increased. Second, the company has introduced an additional computerized system in data request procedure. Third, the access control of the system. Each user has their own username and password to log in to the system. This allows data controller to track data users' activities in the system.

4.2.1.2 Data Processor

Before PETs adoption, data processors can send it via email, shared folder or external hard disk. According to the interviewee, the external hard disk can be either a personal hard disk or company hard disk. After 2013, the company improved the method of sending data by allowing only the data processor to send the data through shared folder and secure email. However, it is untraceable on how the user uses the obtained data.

Besides that, the data processor received less user request due to the filtering process by security team. Previously, data users can easily obtain any data from data processors if the data request is approved only by their supervisor. After the PDPA enforcement with PETs adoption, there is a constraint which security team will evaluate the needs of the data request. However, although data processor receives less request, it increases their communication workload because some data users do not understand the new process and demanding for the data.

4.2.1.3 Data Controller

Data user who needs data that involve personal information needs to go through the security process. When data controller receives the request, they checked all the information and the reasons for requiring all the specific data such as email, age, and address. If the specific type of data does not match the purpose of requesting the data, the data controller will give the necessary data only unless data user provides a better reason to data controller.

After PDPA enforcement, security department adds one more unit which caters for PDPA related issues in the company. This unit is responsible for approving requests from data users. This is an additional unit created based on the existing employees.

4.2.2 Task Management

Employees go through different process in completing their tasks depending on their work nature. The sub-themes describe different employees' workload and time taken for them to complete their tasks.

4.2.2.1 Workload for different data groups

For data users, their workload increases because they are required to go through several additional application processes for personal data requests. Moreover, they have extra PDPA applications for data requests to apply. With the PDPA application for data requests, they need to justify the reason for having the personal data. R1 stated:

> *"The user should tick, if let's say they are requesting sensitive information, there is a page to fill in; who is the one who requesting the data, who will use the data, how long will the data be used, where are they keeping the data, sort of information."*

For data processors, their workload decreases because they receive a lower number of data request applications. This is due to the security department that filters the application. With this, the data request application is lower and subsequently lesser data extraction to do. R2 and R7 explained:

> "*Because they have to check tightly to ensure that this data is being protected careful by the requestor. At the same time, I can attend to other requests. Like last time, request come in coming out… Lesser workload because user cannot simply request the thing right. So, whenever they want to request thing, they should provide the purpose, what is the result, what is the outcome, what is the post analysis kind of thing"* (R2)
> *"Easier for me to handle the requestor because half of it have been handled by the security team for the PDPA things. If not, requestor, they actually don't know what they need also, but they just put whatever information that they want."* (R7)

For data controllers, it is a new team created based on the existing security team. The team now has additional work on handling data request application. Hence, it increases data controller workload.

4.2.2.2 Work completion time for different data groups

The time taken for data user to apply personal data increases because they need to go through several application levels. Data user needs to justify the reason of having personal data in the application form and go through different levels of approval. Thus, the waiting time for data application increases. R9 mentioned that, "they need approval from their head, from this boss, that boss. It takes time.". Besides that, R3 expressed that, "It just constrains us la. In a way, we have to be like, okay, we have to be like, this process, we have to go to A B C instead of just go to C."

For data processor, it doesn't affect their work completion time as the time taken for them to extract the data remains the same. Their work mainly is to extract data from the database. R1 commented that, "It doesn't affect the duration to extract".

For data controller, they are responsible for filtering data requests. As the filtering task is additional workload from their existing work, it increases their time to complete their task. Moreover, when the application is unclear, data processors needs to get back to data user for further verification. R9 stated: "My task when I am reviewing the form is that we have to review first and then advise the user if anything.. If applicable can proceed."

4.2.3 Communication workload

Data users who are not aware of the new process will follow the previous practice which they send requests to data processor. When the application is not processed, they will go through data processor to find an explanation. As the waiting time is longer for data application, data users who urgently require the data will directly request from data processor. R2 mentioned that, "At the end user side right, it's kind of like when can I get the data when can I get the data.". This requires the data processor to explain the flow to data user. Data user feels that the communication is not going down from the top organization. R3 suggested that, "we have to introduce like communication systems of all the, I mean stakeholders of the system.".

As some data users are not aware of the new application process, they send the request directly to data processor. Data processor will need to explain to them that they need to go through the proper channel for data application. R1 stated that, "Some of the users didn't aware of the PDPA. They didn't know. Happens to know when we reject their SR and ask them to go to security first. Then only they know.".
Moreover, some of the requests passed directly to data processor without PDPA approval. R4 recalled that, "Sometimes there is miscommunication or mis-check, the request goes to us without the PDPA approval. So, we will tell them and pass back...". Data processor will need to communicate with data user about getting the PDPA approval. The data application filtering process is newly implemented in TELCO. Data controller needs to work closely with data user for the justification of the application. They will need to communicate with each other more frequently to understand the reason of applying the data. R9 mentioned:

"I need to see my boss, then I have to explain to my boss why the user needs the data... It doesn't look correct la, because I wouldn't know why. I can answer certain questions but if the head of security ask other questions, I cannot answer la... So need to get back to the user.."

5 Discussion

Firstly, the findings show that employees have limited PDP knowledge as there is a lack of awareness in TELCO. Employees do not perceive PDP as necessary due to their insufficient knowledge about PDP. Hence, it is important for organizations to reduce employees' resistance by providing basic security knowledge through education (Furnell et al., 2002).

Secondly, all parties are responsible for PDP. Government enforcement on PDPA will mandate the implementation to ensure PDP. Previous research highlighted that individuals choose to engage in protective information security behaviours due to perceived fear (Warkentin and Siponen, 2015). Employees' attitudes toward PDP, work process, PETs will affect their intention to protect personal data. If employees think that they are responsible for PDP, their intention of performing PDP action increases (Blythe and Coventry, 2018). Organizations should equip employees with all the resources to ensure PDP. Organizations should provide employees with information security training that would provide a full understanding of the threats from data breaches and hacking (Bulgurcu et al., 2010). Education and precautions through internal campaigns can create employees' positive attitudes in PDP (Hentea, 2005).

Thirdly, the effectiveness of PDP can be achieved through organization support, employees' self-efficacy, technologies and a holistic PDP process. Besides, justice need to be served for data leak cases to strengthen the perception of PDP effectiveness that leads to attitude change due to the own/others experience. Employees' competence in performing their tasks will affect their PDP intention. Researches have shown that in healthcare industry, nurses are more likely to engage in protective behaviour when they perceived that they are capable of protecting the data privacy (Ma et al., 2015). Technologies such as PETs are useful in ensuring PDP. For a holistic process for PDP, process flaws need to be identified to enable organization to solve the issues by understanding the cause and problems. PETs can be applied for protection against various forms of unlawful processing of personal data, including unlawful kinds of collection, recording, storing, disclosure (within or between organizations), and matching or sharing (Borking and Raab, 2001).

Fourthly, there is a need to sustain PDP in the long run as protecting personal data is not a one-time event. Organizations should continuously monitor, update and evaluate employees'/vendors' accessibility and PETs. The implementation of security education, training awareness (SETA) programmes and computer monitoring are needed to prevent misuse of personal data (D'Arcy et al., 2009). It is vital for organizations to establish a security culture environment that accounts for internal employees and external threats (Hu et al., 2012).

The findings of this research show that the changes in employees' working processes vary from one another based on their work nature. The employees experience different impacts in their work process. Employees' workload should take into account as overloaded employees will affect employees' compliance (Lee et al., 2016). In addition, the methods used to share data is restricted. Moreover, the mode of interaction between employees are not only through email, phone call, face to face but using the system. These changes are to provide a more tightened control and protect personal data. Based on the previous work process, the employees used a manual approach in their work. Now, there is a computerized system and the work is more organized and systematic. Hence, the employees' working processes are affected positively and negatively depending on their work nature. This is supported by existing research that the influence of information and communication technology affect individuals positively and negatively (De Wet et al., 2016).

The purpose of this research is not aimed to generalize, but to provide a deep understanding of employees' perception and experience. This understanding can help organizations to manage the employees in data protection setting. By managing employees well, organizations' security in protecting personal data increases and subsequently increases consumer trust.

Additionally, through in-depth interview of qualitative method, this study provides an insight into how environmental factors subsequently impact the responses of employees towards their perception and attitude of data protection. With this insight, organizations should invest in building a conducive security culture environment, including continuous awareness fostering and involving security experts for knowledge/skill development as the foundation of supporting subsequent data protection practices.

Whereas continuity in monitoring, evaluating and updating data protection system process is considered as the backbone to ensure the sustainability of the data protection implementation process. The research findings from this study are previously unexplored in prior studies which mainly focused on quantitative methods (Moody et al., 2018) to identify factors that effecting protection behavioural attitude.

6 Conclusion and future work

6.1 Key Findings

The key findings of this study are:

Awareness of personal data protection

As the importance of PDP needs to be constantly reminded, organizations, policymakers and media should discuss relevant topics more often through company internal communications and public media respectively. This can boost employees' memory of the importance of PDP periodically.

Effectiveness and parties involved in personal data protection

The responsibility to protect personal data should be a team effort from government, organizations and employees. Organizations should provide a supportive environment for employees to implement data protection process while governments should take serious action in the penalty of incompliance to intensify the enforcement.

Sustainability of personal data protection

Protecting personal data should not be a one-time execution, it requires continuous effort and monitoring to protect personal data at all time. Organizations should evaluate PDP implementation from time to time to ensure that all the mechanisms are up to date. Further, personal data protection in an organization requires a holistic approach that encompasses a data handling process starting from data collection, maintenance and deletion. Operation and systems that control the data handling process should be periodically audited to ensure the functions of data protection are up-to-date and audited. Those parties involved in the process such as employees and vendors who access to personal data should be tracked with monitoring systems to minimize the loophole for personal data leak.

6.2 Research limitation & Future work

There are several limitations in this research. Firstly, this research only focuses on a single case study in telecommunication industry. Future research could examine different sectors that implement PETs. The comparison can be pursued to obtain more insights on employees' perceptions in PDP through PETs adoption. Multiple case studies can be applied to compare and contrast the result.

Secondly, there is an imbalance amount of identified data groups in the results. Future studies could examine more respondents from each data group. Comparisons between different data group can be made to identify the similarities and differences among their perceptions. As the results showed that there is limited control on vendors, future research could explore the role of vendors and investigate a more secured data handling process by vendors to minimize potential threats to data security.

Acknowledgements

Funding: This research was supported by the Malaysian government FRGS grant [FRGS/1/2015/SS03/SYUC/02/1].

References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39): Springer.

Bloomberg, L. D., & Volpe, M. (2018). *Completing your qualitative dissertation: A road map from beginning to end*: Sage Publications.

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in human behavior, 87*, 87-97.

Blythe, J. M., Coventry, L. M., & Little, L. (2015). *Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors.* Paper presented at the SOUPS.

Borking, J. J. (2011). Why adopting privacy enhancing technologies (pets) takes so much time. In *Computers, privacy and data protection: an element of choice* (pp. 309-341): Springer.

Borking, J. J., & Raab, C. D. (2001). Laws, PETs and other technologies for privacy protection. *Journal of Information, Law and Technology, 1*, 1-14.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.

Brill, J. (2018). Microsoft's commitment to GDPR, privacy and putting customers in control of their own data. Retrieved from https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Cao, Q., Jones, D. R., & Sheng, H. (2014). Contained nomadic information environments: Technology, organization, and environment influences on adoption of hospital RFID patient tracking. *Information & Management*, *51*(2), 225-239.

Cha, S.-C., Hsu, T.-Y., Xiang, Y., & Yeh, K.-H. (2018). Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal*, *6*(2), 2159-2187.

Chan, J. M. J., Chua, H. N., Lee, H. S., & Iranmanesh, V. (2016). *Privacy and Security: How to Differentiate Them Using Privacy-Security Tree (PST) Classification.* Paper presented at the 2016 International Conference on Information Science and Security (ICISS).

Choi, B. C., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, *33*(3), 904-933.

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, *34*(4), 157-170.

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of Employees' Demographic Characteristics on the Awareness and Compliance of Information Security Policy in Organizations. *Telematics and Informatics*.

Curzon, J., Almehmadi, A., & El-Khatib, K. (2019). A survey of privacy enhancing technologies for smart cities. *Pervasive and Mobile Computing*.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Danezis, G., & Gürses, S. (2010). A critical review of 10 years of privacy technology. *Proceedings of surveillance cultures: a global surveillance society*, 1-16.

de Roode, M. (2016). Privacy Enhancing Technologies.

De Wet, W., Koekemoer, E., & Nel, J. A. (2016). Exploring the impact of information and communication technology on employees' work and personal lives. *SA Journal of Industrial Psychology*, *42*(1), 1-11.

Delaney, R., & D'Agostino, R. (2015). The Challenges of Integrating New Technology into an Organization.

Economics, L. (2010). Study on the economic benefits of privacy enhancing technologies (PETs). *Final Report to the European Commission DG Justice, Freedom and Security, London*.

Facebook. (2019). What is the General Data Protection Regulation (GDPR)? Retrieved from https://www.facebook.com/business/gdpr

Federal Trade Commission. (2000). Privacy online: Fair information practices in the electronic marketplace: A report to Congress. *Federal Trade Commission, Washington, DC*.

Fischer-Hübner, S., & Hedbom, H. (2008). Benefits of privacy-enhancing identity management. *Asia Pacific Business Review*, *4*(4), 3-13.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, *25*(2), 91-109.

Freedom of Information Act 2000. (2019). CHAPTER 36 ARRANGEMENT OF SECTIONS.

Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5/6), 352-357.

General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Official Journal of the European Union (OJ)*, *59*(1-88), 294.

Google. (2019). Compliance. Retrieved from https://privacy.google.com/businesses/compliance/

Gozman, D., & Currie, W. (2015). *Managing governance, risk, and compliance for post-crisis regulatory change: A model of IS capabilities for financial organizations.* Paper presented at the 2015 48th Hawaii International Conference on System Sciences.

Hentea, M. (2005). A Perspective on Achieving Information Security Awareness. *Issues in Informing Science & Information Technology*, *2*.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Hinde, C., & Ophoff, J. (2014). *Privacy: A review of publication trends.* Paper presented at the 2014 Information Security for South Africa.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660.

Huang, C.-C. J. (2019). *Privacy Implication and Technical Requirements Toward GDPR Compliance.* Paper presented at the Proceedings of the Future Technologies Conference.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Imgraben, J., Engelbrecht, A., & Choo, K.-K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology, 33*(12), 1347-1360.

Ko, C.-H., Pei, L., & Tsai, Y.-H. (2016). A study of employees' perception of information technology adoption in hotels. *International Journal of Organizational Innovation, 8*(3), 231-238.

Korshunov, P., & Ebrahimi, T. (2013). *Using face morphing to protect privacy.* Paper presented at the 2013 10th IEEE International Conference on Advanced Video and Signal Based Surveillance.

Lancaster, K. (2017). Confidentiality, anonymity and power relations in elite interviewing: conducting qualitative policy research in a politicised domain. *International Journal of Social Research Methodology, 20*(1), 93-103.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59*, 60-70.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry.

Ma, C.-C., Kuo, K.-M., & Alexander, J. W. (2015). A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC medical informatics and decision making, 16*(1), 13.

Madden, M., & Jones, S. (2008). *Networked workers: Most workers use the internet or email at their jobs, but they say these technologies are a mixed blessing for them*: Pew Internet & American Life Project.

Mady, A., & Gupta, S. (2017). Behavioral Approach to Information Security Policy Compliance.

McGivern, Y. (2006). *The practice of market and social research*: Pearson Education UK. Merriam, S. B. (1998). *Qualitative Research and Case Study Applications in Education. Revised and Expanded from" Case Study Research in Education."*: ERIC

Microsoft. (2019). Support for GDPR accountability. Retrieved from https://www.microsoft.com/en-ww/trust-center/privacy/gdpr-accountability-documentation

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS quarterly, 42*(1).

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1609406917733847.

Olivier, M. S. (2003). A layered architecture for privacy-enhancing technologies. *South African Computer Journal, 2003*(31), 53-61.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07).

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544.

PDPA. (2010). Laws of Malaysia, Act 709, Personal Data Protection 2010.

Personal Data Protection Act 2012. (2019). Republic of Singapore Government Gazette Acts Supplement.

Phillips, D. J. (2004). Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media & Society, 6*(6), 691-706.

Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Crespo, B. G.-N., . . . Sanz, A. C. (2019). *DEFeND Architecture: a Privacy by Design Platform for GDPR Compliance.* Paper presented at the 16th International Conference on Trust, Privacy and Security in Digital Business-TrustBus 2019.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*(3), 229-237.

Risk Based Security. (2019). *2019 MidYear QuickView Data Breach Report*. Retrieved from Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*(1), 93-114.

Rowley, J. (2012). Conducting research interviews. *Management research review, 35*(3/4), 260-271.

Ryan, F., Coughlan, M., & Cronin, P. (2009). Interviewing in qualitative research: The one-to-one interview. *International Journal of Therapy and Rehabilitation, 16*(6), 309-314.

Shen, Y., & Pearson, S. (2011). Privacy enhancing technologies: A review. *HP Laboratories, 2739*, 1-30.

Shingler, B. (2019). What you need to know about the Desjardins data breach. Retrieved from https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-explain-1.5185163

Silverman, D. (2013). *Doing qualitative research: A practical handbook*: SAGE publications limited.

Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government information quarterly, 32*(3), 316-322.

Ticehurst, G. W., & Veal, A. J. (2000). *Business research methods: A managerial approach*: Addison Wesley Longman.

Trochim, W. M. (2006). Web center for social research methods. *Retrieved September, 10*, 2008.

Vakola, M. (2014). What's in there for me? Individual readiness to change and the perceived impact of organizational change. *Leadership & Organization Development Journal, 35*(3), 195-209.

Van Blarkom, G., Borking, J. J., & Olk, J. E. (2003). Handbook of privacy and privacy-enhancing technologies. *Privacy Incorporated Software Agent (PISA) Consortium, The Hague, 198*.

Van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2014). Privacy and information technology.

Venkatesh, V. (2006). Where to go from here? Thoughts on future directions for research on individual-level technology adoption with a focus on decision making. *Decision Sciences, 37*(4), 497-518.

Wang, Y.-S., Li, H.-T., Li, C.-R., & Zhang, D.-Z. (2016). Factors affecting hotels' adoption of mobile reservation systems: A technology-organization-environment framework. *Tourism Management, 53*, 163-172.

Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS quarterly, 39*(1), 113-134.

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society Review*, 545-572.

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior, 28*(3), 889-897.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798.

Yanikoglu, B., & Kholmatov, A. (2004). *Combining multiple biometrics to protect privacy*. Paper presented at the Proc. ICPR-BCTP Workshop.

Yin, R. K. (2013). *Case study research and applications: Design and methods*: Sage publications.

Zyskind, G., & Nathan, O. (2015). *Decentralizing privacy: Using blockchain to protect personal data.* Paper presented at the 2015 IEEE Security and Privacy Workshops.