UNIVERSITY OF READING

Analysis of Obligatory Disclosure Regarding Individual's Privacy

Submitted for the degree of Doctor of Philosophy

School of Systems Engineering

Nurul Amin Badrul

June 2016

Abstract

Disclosure of personal information online has raised concerns about individuals' privacy. In order to protect personal information users undertake measures, such as configuring privacy settings and referring to the privacy policies of the organisation's website before engaging in a transaction. This demonstrates users' concerns with the availability of their personal information online. Besides the individuals themselves, organisations are also exposing the personal information of their staff to the general public by publishing it on their official website. The practice of publishing employees' information on such websites is nominally to offer better services to customers, and it is one of the steps taken to improve governmental transparency. However, there are only limited studies on individuals' (i.e. employees') privacy issues in the context of organisational disclosure, and their internal responses to the relevant factors. To date, far too little attention has been paid to the disclosure of personal information by organisational websites. This research addresses this phenomenon, where the issue of third-party disclosure by an entity that has a direct relationship with the individuals is investigated in the Malaysian context. For this purpose, this research introduces 'obligatory disclosure' as a conceptual framework for this study and adds to the knowledge of privacy-in-public in the context of public administration. The results of the study indicate that while obligatory disclosure was commonly believed to be a normal phenomenon, it creates a vulnerable environment for individuals. The study also found that employees' concerns with privacy were influenced by the specific context. In addition, low levels of privacy concern and lack of privacy awareness regarding this phenomenon were identified. The study recommends that there is a need for a regulatory approach to protect employees' information on organisation websites, and privacy should be incorporated as an important element of obligatory disclosure practice.

Acknowledgement

First of all I would like to thank my supervisors, Professor Shirley Williams, Dr Karsten Øster Lundqvist and Dr Patrick Parslow for their guidance and patience throughout the research. Special thanks are also dedicated to ODIN Lab members for their support and encouragement.

My sincere thanks to my sponsor for supporting me financially. The scholarship awarded by the Government of Malaysia through the Public Service Department has made it financially possible for me to undertake and conclude this research.

I would like also to recognise the contribution of Lucy Whitfield for her proofreading, which has profoundly improved the composition of this thesis.

Last but not least, I would like to express my deepest gratitude to my wife, my two children, my parents, family members and close friends for their unfailing faith and fervour through the entirety of this journey.

Declaration

I confirm that this is my own work and the use of all material from other sources has been properly and fully acknowledged.

List of publications

Badrul, N.A., Williams, S.A. & Lundqvist, K.Ø., 2014. Organisational Disclosure: Threats to Individual’s Privacy? In *5th International Conference on Science & Technology: Applications in Industry & Education (ICSTIE)*. Penang, Malaysia, pp. 321–325.

Badrul, N.A., Williams, S.A. & Lundqvist, K.Ø., 2016. Online Disclosure of Employment Information: Exploring Malaysian Government Employees’ Views in Different Contexts. *SIGCAS Comput. Soc.*, 45(3), pp.38–44.

Otto, F., Badrul, N.A., Williams, S.A. & Lundqvist, K.Ø., 2016. Students’ Perception of Privacy Risks in Using Social Networking Sites for Learning: A Study of Uganda Christian University. In G. Vincenti, A. Bucciero, & C. de Carvalho, eds. *E-Learning, E-Education, and Online Training: Second International Conference, eLEOT 2015, Novedrate, Italy, September 16-18, 2015, Revised Selected Papers*. Cham: Springer International Publishing, pp. 182–190.

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Acronyms

Abbreviation	Meaning
APCO	Antecedents→Privacy Concerns→Outcomes
APEC	Asia Pacific Economic Cooperation
CFIP	Concern for Information Privacy
CAQDAS	Computer-Assisted Qualitative Data Analysis Software
CIO	Chief Information Officer
CMC	Computer-mediated Communication
ECtHR	European Court of Human Right
EGDI	e-Government development index
EPU	Economic Planning Unit
FIP	Fair Information Practices
G2B	Government to Business
G2C	Government to Citizen
G2E	Government to Employee
G2G	Government to Government
HCI	Human Capital Index
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
IIU	International Islamic University
IT	Information Technology
IUIPC	Internet Users Information Privacy Concerns
JPM	Jabatan Perdana Menteri (Prime Minister Department)
JUSA	Jawatan Utama Sector Awam (Super-scaled Grade of Public Sector)
KKMM	Kementerian Komunikasi dan Multimedia (Ministry of Communication and Multimedia)
KPKT	Kementerian Perumahan dan Kerajaan Tempatan (Ministry of Housing and Local Government)
MAMPU	Malaysian Administrative Modernisation and Management Unit
MDeC	Multimedia Development Corporation

MDB	Majlis Daerah Besut (Besut District Council)
MDT	Majlis Daerah Tapah (Tapah District Council)
MGD	Majlis Daerah Gerik (Gerik District Council)
MFPS	Malaysian Federal Public Service
MGPWA	Malaysian Government Portals and Websites Assessment
MITI	Ministry of International Trade and Industry
MoD	Ministry of Defence
MoF	Ministry of Finance
MOSTI	Ministry of Science, Technology and Innovation
MPK	Majlis Perbandaran Klang (Klang Municipal Council)
MPKj	Majlis Perbandaran Kajang (Kajang Municipal Council)
MPM	Manjung Municipal Council
NPO	Non-Profit Organisation
NRE	Ministry of Natural Resources and Environment
OSI	Online Service Index
OSN	Online Social Network
PDPA	Personal Data Protection Act
PI	Personal Information
PSD	Public Service Department
SE	Social Engineering
SSO	Single Sign On
SUK	Setiausaha Kerajaan Negeri (State Secretary Office)
TII	Telecommunication Infrastructure Index
TWG	Technical Working Group
UN	United Nations
UNDESA	United Nations Department of Economic and Social Affairs
UTM	University Technology of Malaysia
WAI	Website Assessment Index

CHAPTER 1

Introduction

1.1 Background

Progressive advances in technology have made it difficult to keep personal information private. Indeed, personal information can be drawn from various sources. The emergence of Web 2.0 in the early 2000s allows more people to publish information on the Internet. Publishing personal information started from personal homepages using HTML code in the early 1990s to weblogs (blogs) in the late 1990s (Bruns, 2013). Users were participating online on their personal blog, and actively producing information.

Transition from personal to social began in 1997 with the birth of the first social network site, known as SixDegrees.com (boyd & Elison, 2007) that allowed users to create profiles, list their friends and browse their friends' lists. Social network sites provided a platform for users to create their own profile and link it with other users with whom they are affiliated. Subsequently, with the emergence of online social networks (OSN), the practice of disclosing personal information has become an online culture with global acceptance. With more than 1 billion users, Facebook is currently at the forefront in social networking sites (Facebook, 2016). OSN users participate actively by posting information about themselves, i.e. their name, date of birth, photos, activities, friends, age, qualification, occupation, feelings etc. Users willingly disclose their personal information to fully experience what the OSN has to offer (Stutzman et al., 2013). In fact, users' personal information is the main commodity of OSNs and thus users' willingness to disclose personal information is important for its sustainability (Joinson, 2008).

With users now being more concerned about their personal information, OSNs provide users with the ability to manage and configure the personal information they make available to other users (Acquisti & Gross, 2006; Dwyer et al., 2007). Users of Facebook were discovered to increasingly keep their personal information hidden from public view (Stutzman et al., 2013). A large-scale study of 1.4 million Facebook users found that there is an increase from 17.2% to 52.6% of users who are keeping their friends list private, and 33% are hiding 14 personal attributes compared to 12.3% in less than two years (Dey et al., 2012).

However, OSNs are not the only sources of personal information. Similarly, non-social networking sites were also found to be leaking personal information to third parties' sites. A study of 100 popular websites discovered that 75% of the sites under study leaked personal information (Krishnamurthy et al., 2011), such as email address, username, full name, zip code, age, gender and sensitive search term.

Personal information was also discovered to be available from organisations via the publication of documents such as excel spreadsheets from their organisation's website. By using a freely available Google search engine, Oh & Chakraborty (2009) demonstrated that they are able to obtain sensitive personal information of university students from four different countries including their financial and guardian information.

In addition, organisations are also exposing the personal information of their staff to the general public by publishing it on their organisation's official website. The practice of publishing employees' information on such websites is nominally to offer better services to customers, and it is one of the steps taken to improve organisational transparency. Information such as an employee's full name, job title and affiliation was found to be available publicly in a sample of 51 states of the United States e-Government websites (including Washington D.C. as a separate extra state) (Zhao & Zhao, 2010).

Gallego-Álvarez et al., (2011) also discovered the personal information of university employees on Spanish universities' websites. Indeed, a piece of research on Spanish universities' websites suggested that publishing contact information is one of the important criteria for assessing website quality (Buenadicha et al., 2001). Based on the Website Assessment Index (WAI), contact information represents more than one quarter of the marks for overall site content category. Contact information that is commonly published on an organisation’s website are employee’s name, e-mail address, organisation’s address, telephone number and fax number.

Additionally, organisations publish information about their activities, events, and reports, either in the form of text, audio or video, and may feature their employees as part of website content. In view of that, employees’ information is one of the main components to be included in organisational websites.

Public organisations, through the e-Government initiatives, publish contact information on their official websites in order to improve communication, transparency, and accountability to the citizen (Evans & Yen, 2006; Zhao, 2010; Welch & Hinnant, 2003). The practice of publishing an employee’s information on an organisation website aims to offer better services to their customers. By providing employees’ information, governments are looking at increasing interaction between the government and the public (Thomas & Streib, 2003; Siar, 2005).

However, the disclosure of employees’ information may also include publishing identifiable information about them. With the recent advances in Internet technology, personal information can be collected, exchanged, shared and used in a simple and easy manner by almost anyone. Furthermore, personal information can be analysed to unveil hidden patterns, inferred and aggregated to reveal other sensitive information. Consequently, personal information can be used beyond its intended purpose and people are open to information abuse (Smith et al., 1996; Dinev & Hart, 2004a).

It has been shown there are real risks in disclosing personal information (Koch et al., 2012). The large amount of personal information available has become a valuable source of information for interested parties who might misuse the information to jeopardise a person. Individuals thus exposed may be at risk and may be particularly vulnerable to threats due to this disclosure. In addition, posting personal information related to employment may put the organisation at risk, regarding sensitive information or internal matters (Furnell, 2010).

According to a report from Symantec Corporation (2016), government and public sector organisations are among the most targeted sectors for online attacks that aim to steal data or confidential information. Attacks that targeted employees increased 55% in 2015. In addition, the report also indicates that the high possibility of attack might be caused by a high online visibility of employees' information.

It is becoming increasingly difficult to ignore the fact that the disclosure of employees' information on public organisation websites inadvertently reveals their personal information, which makes them identifiable whether online and offline. This could raise privacy issues among individuals who are also public service employees. What is not clear is how this disclosure in any way has an underlying privacy consideration for the employees. However, there has been little, if any, research examining the issue of privacy towards public service employees' in the context of organisational disclosure and their internal responses to the relevant factors.

To date, little attention has been paid to the disclosure of personal information by organisational websites. This research addresses this phenomenon, where the issue of third-party disclosure by an entity that has a direct relationship with the individuals is investigated in the Malaysian context primarily towards Malaysian Government websites and the Malaysian public services employees.

Since 2006 the Malaysian Government has actively promoted and implemented government services through the web via the use of ICT. The establishment of the Multimedia Super Coridor (MSC) Malaysia in 1996 and the launch of Public Sector ICT Strategic Plans in 2003 manifested great attention from the Government towards e-Government initiatives (Kaliannan et al., 2009). In order to improve public service delivery through government websites, an annual assessment of various government agencies was conducted to evaluate the standard and content of each agency (refer to section 3.4.1.3). Each agency from the federal, state and local government was evaluated. Besides the online presence, the employees who are the backbone of any government - played a significant role in delivering efficient services. In 2014, the Malaysian public service consisted of 1.6 million employees (Bernama, 2015) and most of the federal agencies and departments are located in the new administrative capital, Putrajaya, which is 25 km from Kuala Lumpur.

This study is unique in that it focuses on disclosures of individuals that belong to the organisation in a situation-specific environment. This research adds to the knowledge of privacy-in-public in the context of public administration.

1.2 Motivation

The researcher has been a public sector employee for the past 16 years and has been involved in project management, training management, project development and skills training policy. During the researcher's service with the Government, the researcher has experienced e-Government initiatives, where usage of ICT in government administration is widely implemented. One of the initiatives in e-Government is to establish official website for public agencies, in order to increase delivery of services and citizen's participation. All of the agencies that the researcher has worked with have an official website. In order to facilitate efficient delivery of services, the Government has implemented a strategy of publishing employees' information on the organisation's official website.

During the researcher's service with public agencies, the researcher experienced receiving numerous emails, telephone calls, letters and fax from the public that were not related to the researcher's scope of work. The researcher believes that this might be due to his personal information being publicly available on the official organisation's website, because it is widely accessible by anyone. This experience facilitated the development of the study.

Based on the researcher's observation, most public organisations' websites publish their employees' information publicly. While reports on public disclosure of personal information from organisational websites indicated privacy implications (Scassa, 2014), research from the employees' perspective were scarce. Publication of employees' information on their organisation websites are often overlooked. Instead, this situation could have affected many other individuals where their personal information is disclosed online by their organisation. Interest in exploring obligatory disclosure has a personal statement - an intention to improve the disclosure of individuals (i.e. public employees) by minimising privacy risk.

The disclosure of personal information online may result in conflicting outcomes for public sector employees. Based on above, it is important to explore and understand how employees perceive an official website's disclosure and its relationship with employees' privacy. Such an understanding will help to provide a reduced risk toward employees and increases employees' productivity.

1.3 Research aims

This thesis seeks to explore and understand public sector employees' experiences caused by organisational disclosure, with respect to individuals' privacy. It is interested in understanding how the employees perceive 'obligatory disclosure' and its impact on individuals' privacy.

The research aims of the work are to:

- Examine public organisational websites for potential employees' disclosure.
    - Identify publicly available personal identifiable information caused by organisational websites.
    - Evaluate the disclosure of employees' personal information on organisational websites.
- Analyse the perception of 'obligatory disclosure' from employees.
- Discover the awareness and concerns of employees regarding 'obligatory disclosure'.
- Examine the impact on employees' privacy over 'obligatory disclosure'.

The research was approached from an interpretivist paradigm through a single case study embedded design. This approach is suitable for understanding the phenomena in which people live and work (Creswell, 2013a). Hence, it has allowed for interpretation in an attempt to make sense of the phenomenon. In addition, a case study approach is useful in understanding a complex phenomenon within its context, which is particularly relevant in this study (Yin, 2014).

1.4 Research questions

The research questions have undergone several revisions and improvements. The continuous development and refinement at all stages of inquiry is good practice in developing good research questions (Agee, 2009). In the early stage of study, there were six secondary questions and one sub-question (Appendix A). It was soon discovered that most of the research questions formulated were not open to multiple perspectives to let possible interpretations emerge. Later, two research questions were combined with secondary questions as sub-questions, in order to provide a more focused direction for the questions. As the research progressed, two research questions were considered redundant in combination with the existing research question and were removed. As one question is directed towards suggestions from participants, it was anticipated that this information is better suited to the recommendation section.

Therefore, in order to achieve the aims of this research, the central research question is as follows:

How would public employees describe organisational disclosure and its relation to their privacy?

In order to answer the main research question, several secondary questions need to be answered:

Research question 1: How does obligatory disclosure result in the disclosure of employees' personal information?

- **Sub-question:** What personal information of employees, if any, is publicly available on organisational websites?

Research question 2: What does obligatory disclosure mean to the employees?

Research question 3: How do employees perceive the issue of privacy with regard to obligatory disclosure?

Research question 4: How does obligatory disclosure impact on employees' privacy, if any?

- **Sub-question:** What are the concerns of employees, if any, when their personal information is published on their organisation's website?

1.5 Contribution

This study offers several novel contributions to the area of information privacy and personal information disclosure.

- Identifying and classifying distribution of personal information disclosed in public organisation websites.
- Introducing a more specific conceptual framework for employees' personal information disclosure by its organisation's website.
- Enhancing understanding on the knowledge of privacy in situation-specific environment, i.e. obligatory disclosure.
- Understanding an individuals' privacy management due to information disclosure by a third-party.
- Providing a novel approach to the investigation of public personal information disclosure on websites. The method offers a flexibility framework in adapting to specific personal information research aims and is applicable in other organisations and settings.
- Suggesting several causes of action on policies and website design for obligatory disclosure towards strategies for a 'safer disclosure', without putting aside the objective of the organisation.

1.6 The thesis outline

Chapter one presents an overview of the study, motivations, research aims, research questions, and contributions. Finally, it introduces the outline of the thesis.

Chapter two discusses the literature relevant to the research topic. It starts by introducing a more precise term for organisational disclosure. It discusses the concept of personal information and online disclosure, including different types of disclosure. The chapter moves on to discuss the privacy concepts, characteristics, users' behaviour and risks. Next, the e-Government concepts, implementations and issues are presented. It ends with the theoretical consideration to guide the research framework.

Chapter three describes the investigation's methodology, methods and techniques employed to investigate the research question. It also discusses the data collection, the field work and reflections of strength and weaknesses including the rationale of methodology selected and ethical considerations and the trustworthiness of study.

Chapter four reports on the analysis of this research, firstly on the web content analysis and then on the in-depth semi-structured interviews. It provides a detailed description of the analysis on both techniques.

Chapter five presents the results of this thesis. A taxonomy of personal information found on government websites and themes that emerge from participants are presented.

Chapter six presents the results of the analysis and highlights the key findings of this research. In addition, it presents the words from participants indicating how the data was interpreted and discusses the investigation.

Chapter seven summarises the investigation, including whether it has answered the research questions, the limitations of the study, and presents recommendations on obligatory disclosure as well as suggestions for future research.

CHAPTER 2

Literature Review

The aim of this chapter is to provide an overview of related work and concepts in the area of investigation, including presenting the theoretical framework of this research. The chapter will start by introducing obligatory disclosure as the conceptual framework in the context of research. After defining the concept, this chapter will present the literature regarding the concept of personal information and its disclosure on the Internet, followed by the concept of privacy and e-Government. Finally, the theoretical framework that will guide the research is discussed.

This research explores and understands how public employees perceive and experience organisational disclosure and its privacy implications. It examines the availability of employees' personal information on public sector websites, and identifies common themes and meanings from public employees.

2.1 Obligatory disclosure

This study proposes a more precise term for 'organisational disclosure' that specifically releases personal information of individuals. This term will represent a better description of the investigated phenomenon in seeking a new understanding of disclosure from the individual's perspective. This study introduces 'obligatory-disclosure' as the conceptual framework of the phenomena and it is defined as: "any information about an individual that is shared via any form of communication by an organisation, (in which they are employee or member)". This type of disclosure is not performed by the individuals themselves, but is disclosed by a third party that has an ongoing relationship with the individuals. Figure 2-1 presents the conceptual framework of obligatory disclosure.

Relationships with online organisations were found to influence users upon deciding to share their personal information (Olivero & Lunt, 2004). The relationship between an individual and an organisation has an important influence in information disclosure decisions (Norberg et al., 2007; White, 2004). This research will focus on the employment relationship between an individual and the organisation.

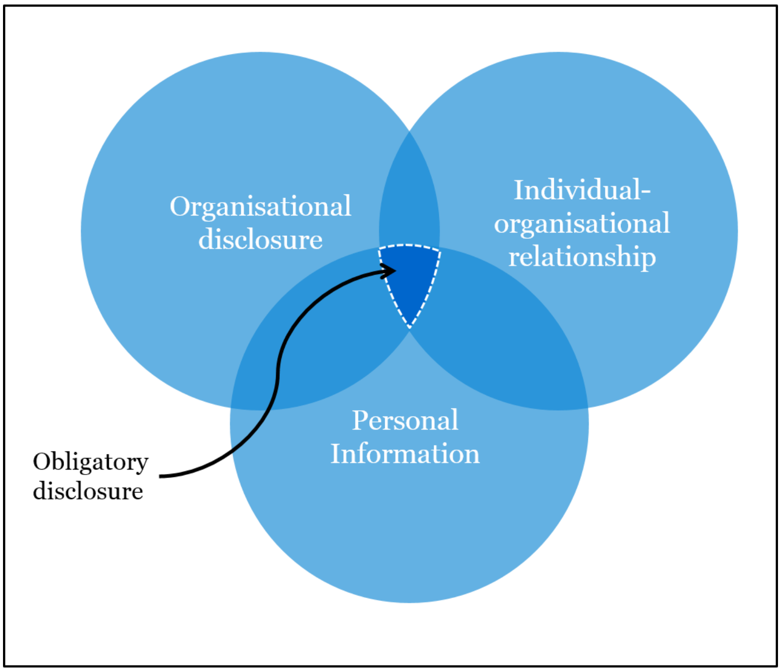

Organisational disclosure
Individual-organisational relationship
Personal Information
Obligatory disclosure

Figure 2-1: Conceptual framework of obligatory disclosure

The organisation discloses employees' information on its websites for various purposes. The disclosure of employees' information is to meet the objectives and demand of stakeholders and customers. Improving delivery of service, transparency and higher efficiency were often highlighted as among the reasons for disclosure (Siar, 2005; Simpson, 2011; Grimmelikhuijsen et al., 2013). Moreover, concerns arise when the information that is published on the website is employees' personal information.

Bannister and Connolly (2011) argued that employees within the public sector have the right to their personal privacy but at the same time fulfil their organisation's goals. Organisations are considered to breach the privacy of an individual when the element of control is not accorded to the individual. According to Hann et al. (2007), "when an organisation in its efforts to pursue the organisation's objectives collects, stores, manipulates or transmits personal information unbeknownst to the individual," (p. 15), it breaches the individual's privacy.

Furthermore, according to Hsu (2006), individuals perceived websites differently according to the different categories they address. Situational factors, such as types of websites, were shown to have an influence on individuals' privacy concerns (Li, 2014). Studies that investigate how a specific website (i.e. government websites) affects the privacy of individuals are limited and this requires more understanding (Belanger & Xu, 2015). As such, this study will further increase understanding on situation-specific privacy concerns where it addresses arguments for a contextual nature of privacy.

Thus, by introducing obligatory disclosure in this study, it provides a coherent context of the phenomenon under investigation from individuals' perspective. In addition, it will stimulate a more focused approach of research in the broad area of disclosure and privacy.

2.2 Personal information

2.2.1 The concept of personal information

Personal information is difficult to define and thus has a variety of definitions (Madden et al., 2007). Even the term 'personal information' itself has at least three different terminologies. Personal information can generally be defined as any factual or subjective information relating to an identifiable individual (Slane, 2000), while personal identifiable information (PII) is defined by Mccallister and Scarfone (2010) from the U.S National Institute of Standards and Technology as:

"any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information" (p. ES-1).

Another related term that is normally used is personal data, which is normally used in the legal fraternity. It is defined as: “information relating to an identified or identifiable natural person,” (Article 2a) by the Data Protection Directives (European Union, 1995).

Commonly, personal information is assumed to be related to an individual’s personal life and movement. However, Stahl (2008) reiterates in the case *Niemietz v. Germany,* 1992, that the European Court of Human Rights (ECtHR) ruled that even professional or business activities are considered personal information. The court acknowledged that during these activities, developing relationships and establishing correspondence with other human beings are within the notion of ‘private life’. Similarly in the EU General Data Protection Regulation Framework (GDPR) which were adopted by the European Parliament in April 2016, extends the coverage of personal data to their private, public and work roles (European Commission, 2016). Hence, personal information can cover a wide range of issues, for example access to information and public documents, protection of personal information, gender, health or identity.

In the context of online privacy, Irani et al. (2011) defines it as: “information which can be used to distinguish or trace an individual’s identity,” while Krishnamurthy & Wills (2009) elaborated further as: “information which can be used to distinguish or trace an individual’s identity either alone or when combined with other public information that is linkable to a specific individual.” Collectively, these definitions while explicitly mentioning identifying individuals - also cover the possibility of processing any information that can be used to identify an individual. Thus the concept of ‘identifiable’ appears to be prominent in the meaning of personal information, that reinforces the idea that any identifiable information that can be associated to an individual is accounted for as personal information regardless of the intention whether it is for professional or personal purposes, which is in line with Krishnamurthy and Wills (2009) definition to which this research is subscribing. For the sake of clarity and consistency, this study will use the term “personal information” to include all definitions.

2.2.2 Personal information on the Internet

Previous research into the online environment discovered different types of personal information widely available on the Internet. The spread of Internet usage and increasing adoption of online communication has generated an explosion of personal information.

With the technological advancement of the Internet, identifying individuals is much easier. Furthermore, the explosion of users' generated data has resulted in a tremendous amount of personal information available on the Internet. Even if the information is made up from fragments scattered across the Internet, as long as it is possible to identify an individual either by linking or aggregating information from different sites, it is relevant with the definition stated above and considered as personal information.

A number of authors have reported that various attributes of personal information were discovered online. For example, photographs (Aguiton et al., 2009; Wang et al., 2010) and gender (Wang et al., 2010) were found to be an important element in the computer-mediated environment, while an individual's full name, email address, postal address, location, contact information, age, gender and occupation (Krishnamurthy et al., 2011; Lam et al., 2008; Aguiton et al., 2009; Wang et al., 2010; Lederer et al., 2003; Mccallister & Scarfone, 2010) were also categorised as attributes of personal information. Even the question of whether IP addresses can be considered as personal information caused controversy (Lah, 2008). Furthermore, an individual's friends were also identified as personal information, especially within the OSN environment (Nosko et al., 2010). In the interest of clarity, researchers often grouped these attributes into similar functions such as identity, location, activity, nearby people and profile (Lederer et al., 2003).

Additionally, different types of personal information were found to have different degrees of sensitivity (Rohm & Milne, 2004; Metzger, 2004; Hawkey & Inkpen, 2006). The same personal information may be sensitive to some individuals but not to others. Some researchers have shown that some personal information is typically more sensitive than others, e.g. personal identifiers, financial information and medical information (Ackerman et al., 1999; Phelps et al., 2000; Metzger, 2007). The sensitivity of information may also depend on the context where it is observed. Nissenbaum (2004) argued that when information is transferred outside of the intended context of collection, it loses contextual cues and may increase its sensitivity and subsequently lead to privacy issues.

This led researchers to consider sensitiveness as another category of personal information. For example, an e-commerce investigation classifies personal information into identification information; sensitive information; and general habits (Andrade et al., 2002) while Aïmeur and Lafond (2013) characterise personal information as identifying information, buying patterns, navigation habits, lifestyle, sensitive data, and biological information in few different Internet domains. Researchers tend to differentiate between sensitive and non-sensitive personal information when investigating users' behaviour when disclosing personal information (Joinson et al., 2008).

Within the OSN environment, Nosko et al. (2010) further suggest three different categories of personal information: personal identity information; sensitive personal information; and potentially stigmatising information. Personal identity information refers to basic identifying information that most people are willing to disclose in daily activities, e.g. city/town, address, profile picture. Sensitive personal information refers to information that could be used to threaten or endanger individuals in terms of identifying or locating an individual, e.g. employer, job position. Thirdly, potentially stigmatising information involves information that could portray specific characteristics of an individual e.g. birth year, photos, interests.

From the perspective of personal information protection, recently there have been calls to not differentiate personal information into sensitive and non-sensitive information, because non-sensitive information can be manipulated into revealing individuals' sensitive information (Corbett, 2013). In general, sensitive information can be suggested as information that users are less willing to disclose while non-sensitive information refers to information that users have a high willingness to disclose. Thus, for highly sensitive information, individuals may object to it being made available online moreover to have it published publicly on websites.

2.3 Disclosure of personal information

When participating in online activities, there are times when users are required to disclose personal information to fully experience what the site has to offer. Example of this are social networking sites, e-commerce sites, Internet banking sites and official government's sites. The more users are involved in online activities, the more personal information is contributed online and as such, this content is searchable, traceable and can be used to track their digital footprints (Madden et al., 2007). However, there are also times when it is not users who disclose their personal information, but others might do it for them. Even when the personal information was not disclosed actively (by any individuals), it can be collected without the user's knowledge when participating in online activities (e.g. web browsing) (Krishnamurthy et al., 2011).

Sources of personal information online may come from the individual themselves where they voluntarily disclose their information, or their friends or others may have done it for them. They can consist of either information that is: a) disclosed by the person themself i.e. self-disclosure, b) disclosed by third parties - their friends, other individuals or entities, or c) disclosed without the individual's awareness or knowledge i.e. leakage. This section will discuss how personal information has been found to be available online.

2.3.1 Self-disclosure

Research in self-disclosure roots from social scientists in the area of mental health (Jourard & Lasakow, 1958), and was defined as: "the process of making the self known to other persons," (p. 91) which covers wide-ranging views of disclosures. In the context of relationships, Collins and Miller (1994) describe it as "the act of revealing information about oneself to another," (p. 457), while Cozby (1973) loosely refers to it as verbal sharing of information. Without setting aside the basis of self-disclosure which is about disclosing information to another person, it is important to note that these definitions were developed when computer-mediated communication did not exist. Thus the context was more towards interpersonal communication.

With the rise of the Internet, and computers becoming an important mode of communication, Joinson and Paine (2007) when discussing disclosure in computer-mediated communication (CMC) define it as: “the telling of previously unknown so that it becomes shared knowledge,” (p. 235). They added that disclosure could occur between individuals, within groups, or between individuals and organisations, and is dependent on the context.

Users disclose their personal information consciously as a way of communicating with others. In early CMC research, Internet users were more willing to reveal their information due to lack of identifiability and visual anonymity (Joinson, 2001; Tidwell & Walther, 2002). The amount of personal information disclosed by CMC was higher compared with face-to-face interaction (Tidwell & Walther, 2002; Joinson, 2001), as perceived anonymity can lead users to feel less inhibited. These studies put forward the importance of the concept of anonymity in understanding online self-disclosure.

The explosion of online social networks (OSNs) has created a new interest for researchers to understand more about self-disclosure in OSN. Moreover, in OSN, the identity of participants is often revealed and at the same time the communication is under reduced social cues.

In order to discuss self-disclosure in OSN, it is therefore important to understand why people decided to participate in OSN. People’s decision to participate in OSN sites is normally based on several considerations. Studies on Facebook suggested that the use of Facebook is for social searching and social browsing (Lampe et al., 2006). Social searching in this context refers to finding information about people that they have met offline using Facebook, while social browsing is the act of finding someone with the intention of meeting them in the real world (Lampe et al., 2006). Their findings were further supported by Joinson (2008), where keeping in touch and social surveillance were the most often cited reasons by participants for using Facebook. Besides, other motives for Facebook use were to procrastinate or waste time or for entertainment (Sheldon, 2008; Hew, 2011). Similarly, a Malaysian study found five main motives for using Facebook and the primary reason was because of the social factors (Balakrishnan & Shamim, 2013). Although most of these samples focus on students, it is obvious that the usage of Facebook was mainly for social interaction (Sheldon, 2008).

In fact, a workplace study that focused on employees' usage of OSNs found similar findings. The two most widely used OSNs found within the workplace studies are LinkedIn and Facebook (Skeels & Grudin, 2009; Stopfer & Gosling, 2013). LinkedIn is a professional networking site that focuses on an individual's professional information, and is the world largest professional OSN (LinkedIn, 2015). As LinkedIn targets professional individuals, the usage of LinkedIn in workplace environments is expected. On the other hand, employees were found using Facebook for both personal and professional purposes (Skeels & Grudin, 2009). For instance, employees were using it as formal organisational tool, managing team activities and spaces for self-promotion (Mangold & Faulds, 2009).

A survey of more than 1,600 corporate information technology and information system managers and computer end users across North America, United Kingdom and Europe discovered that while OSN usage is common at work for both work and personal use, Facebook usage is mainly by employees for personal reasons (Facetime Communications, 2008). It was reported that 35% of employees used Facebook for personal reasons and only 18% for professional purposes.

2.3.1.1 Motivations for self-disclosure

Researchers discovered that OSN users shared their information to gain certain benefits associated with self-disclosure. Several studies have revealed motivations for self-disclosure in OSN (Krasnova et al., 2010; Waters & Ackerman, 2011; Ellison et al., 2006). Through a mixed-method study comprising focus groups and an online questionnaire, Krasnova et al. (2010) identified three motivational factors for self-disclosure in OSNs: convenience of maintaining relationships, relationship building and enjoyment. While Krasnova et al's sample consists of two OSN platforms (StudiVZ and Facebook), Waters and Ackerman (2011) focuses specifically on active Facebook users. Building from Lee et al. (2008), they argued that a user's motivation to disclose comes from the following reasons: sharing information, storing information and using it for entertainment, to get updated about trends and showing off. Equally important, SNS users were found to manage self-presentation on their profile (boyd & Ellison, 2007). In an online dating context, Ellison et al. (2006) discovered that users carefully constructed their online profile to generate positive impressions of themselves. Interaction in the OSN environment can facilitate relationship building (boyd & Heer, 2006; Joinson & Paine, 2007) and increase trust (Tidwell & Walther, 2002; Joinson & Paine, 2007) for relationship development. On the whole, the main reasons that people would disclose their personal information in OSNs is for building and maintaining relationships and online self-presentation (Waters & Ackerman, 2011; boyd & Ellison, 2007). These are the benefits that can be derived from information sharing and impression management from the usage of OSNs (Beldad & Koehorst, 2015; Waters & Ackerman, 2011).

2.3.1.2 Antecedent of self-disclosure

As an information-sharing platform and a communication tool, OSNs enable users to produce ideas, messages, and interaction by presenting themselves via their individual profile (Krasnova et al., 2010; Külcü & Henkoğlu, 2014; boyd & Ellison, 2007). However, within the context of OSN, users are less anonymous compared with traditional CMC environments, as users often know their communication partner. Furthermore, the ‘real names’ policy embedded within the Terms of Service of the most popular social media, i.e. Facebook (Facebook, 2015), caused a high number of Facebook users to provide their full name on their profile (Debatin et al., 2009; Tufekci, 2008; Young & Quan-Haase, 2009).

Research around OSNs discovered that many users are disclosing their personal information online (Acquisti & Gross, 2006; Nosko et al., 2010). Several authors provide a more detailed insight into what types of information were disclosed. Findings from 601 students’ profiles (on Facebook and Myspace) found that full names were the most disclosed piece of personal information on a social media profile (Tufekci, 2008). Similarly, Young and Quan-Haase (2009) reported a high number of full names disclosed in user’s profiles. In addition, self and friends’ visual images, birth dates, school name, current city/town and email address were disclosed by more than 80% of participants. A more comprehensive study in examining possible types of personal information that are present on Facebook profiles identified up to 97 different types of personal information that were shared by Facebook users (Nosko et al., 2010). The majority of their Canadian sample (more than 50%) disclosed 26 types of personal information, which included birth date, gender, profile photos, photo albums, friends, groups joined and education information publicly. These findings showed that Facebook and other OSN users divulged a lot of personal information.

In an attempt to further understand people's disclosure behaviour, studies found that people are willing to disclose their personal information when the expected benefits far outweigh the risk (Gross & Acquisti, 2005; Chellappa & Sin, 2005). Perceived ownership has been identified as one of the factors that influences information disclosure (Sharma & Crossler, 2014). Nguyen et al. (2012) found that factors such as type of relationship, mode of communication and context of interaction suggest differences in the degree of disclosure. In addition, trust was argued as an important factor for users to self-disclosure (Christofides et al., 2009; Beldad et al., 2011). Demographic properties such as gender were also found to have influenced information disclosure behaviour (Schrammel et al., 2009). Schrammel et al. (2009) presented that men are more willing to disclose information to their friends than women. However, some authors did not find any significant effect on gender (Malheiros et al., 2013; Young & Quan-Haase, 2009; Metzger, 2004) regarding disclosure behaviour.

2.3.2 Third party disclosure

Another type of disclosure that also reveals personal information is disclosure by a third-party. This disclosure occurs when an individual's personal information is not disclosed by the individuals themselves but by others, for example by friends (Gundecha et al., 2011), acquaintances, family members, colleagues, websites or anyone who has collected that particular information. The person or entity armed with a user's personal information may later disclose that particular information to another party, unaware that it might create an inconvenience to the individual.

In OSNs, examples of third-party disclosure can normally be observed by friends' information sharing practices. Since OSNs allow others to interact actively, quite often friends have the ability to post text, photos and links on an individual's wall. Comments left by friends on a user's Facebook account were found to affect impressions towards profile owners (Walther et al., 2008). They explored public photos and messages on a user's wall posting that were placed by their OSN friends, which could suggest attractiveness and the behaviour of the profile owner. Although these messages comprise only a small part of the overall information on the profile, it illustrates that disclosure of personal information by others affects the evaluation of an individual's persona.

Another example is by tagging photographs (Pesce et al., 2012; Besmer & Lipford, 2010). Users tag photos to promote higher interaction, and this acts as a feature to inform a person about what others have posted about them. Tagging photos in OSNs was found to create problems when the user doesn't want certain information to be connected to them (Wisniewski et al., 2011). Furthermore, photo tagging increases the possibility of predicting user's personal information such as gender, current city and current country (Pesce et al., 2012). By combining two different types of information (i.e. username and tags), it was demonstrated that users can be identified across different OSNs, and their strategies can be achieved with up to 80% accuracy (Iofciu et al., 2011).

Along the same lines, Gundecha et al. (2011) argues that friends in OSNs can spread personal information indirectly even without posting information. According to them, vulnerable friends are those that might place a user at risk by not having sufficient privacy and security settings to protect the entire network of friends. The authors further suggest that users should unfriend vulnerable friends to reduce the vulnerability of a user.

Another way of disclosure is from the OSN's service provider itself. This approach was demonstrated by Krishnamurthy and Wills (2009). They discovered that users' personal information was transferred to the third party servers via the OSN itself without the knowledge of users. In analysing a sample of 12 OSNs, four types of leakages were identified. OSN identifiers of a user were transmitted to third parties via OSN and external applications, users' personal information to third party servers and users were linked with other fragmented information. This information was used to track user behaviours such as browsing activity and online shopping for improved targeted advertising (Wilkinson & Thelwall, 2011).

Besides OSNs, other websites were also found to be disclosing users' personal information (Krishnamurthy et al., 2011). Krishnamurthy et al. (2011) discovered that 75% of 120 samples of popular commercial websites disclosed users' personal information to a third party site. By analysing HTTP requests and responses, they discovered that among the personal information that was disclosed are addresses, home phone numbers, email addresses, full names, health searches, age, zip codes, jobs, gender, activities, city, employers and travel searches.

2.3.2.1 Organisational disclosure

However, OSNs and commercial websites are not the only sources of personal information. Instead, organisations are also exposing the personal information of their staff to the general public by publishing it on their organisation's official website. Organisations may disclose personal information on their websites either intentionally or unintentionally. In fact, Facebook was initiated based on organisational disclosure. It started from the practice of Harvard University to issue a student directory to undergraduates that contains personal information together with photographs. Later in 2004 it was transferred to an Internet site by a group of undergraduates, initially under the name Thefacebook (Craik, 2009).

Researches on organisational disclosure were largely found in the accounting discipline and the term 'corporate disclosure' was normally being used to represent disclosure by an organisation (García-sánchez et al., 2013). The disclosure largely focuses towards organisational factors from an organisation's perspective such as policies, financial, accounting or corporate social reporting (Williams & Ho Wern Pei, 1999; Dutta & Bose, 2007; Ettredge et al., 2001). Nevertheless, studies which specifically examine an organisation's website disclosure towards personal information are very limited.

Organisations, such as universities, were found to be disclosing information about their employees' on their websites (Gallego et al., 2009) in order to improve their relationship with users (Gallego-Álvarez et al., 2011). A study by Gallego et al. (2009) found that most Spanish universities publish employees' information. More than 96% of all 70 Spanish universities in the report published the email address, postal address and telephone number of their employees. Moreover, the staff directory was evident in 59% of the websites. Information about the university's top management was published in 67% of the websites. The information was categorised as: 'description of individual governing positions' (p. 173) with 23% of universities revealing their Pro-Vice Chancellor's curriculum vitae. In addition, they reported that 14% of universities disclose their organisation chart. In addition to the Spanish version, more than three-quarters of the universities provided an English version of their websites.

Another recent study focusing on university lecturers in three countries was able to evaluate the strength of accounting faculty members based on the employees' information available on official websites (Samkin & Schneider, 2014). In this study, the authors were able to identify significant differences between Australian, New Zealand and South African academics' qualifications and research performance by examining the information disclosed on organisational websites. Vital to their research is the availability of personal information of academics on the faculty websites. They listed name, job title, gender, professional and academic qualifications, contact information, publications, biographical information and professional membership as information that was found during their data collection. This information could serve as a career development strategy for the academic in the sense of promoting themselves to internal and external stakeholders.

In order to address efficiency and transparency, non-profit organisations (NPOs) are guided by recommendations on the principles and best practice of website disclosure (Lee & Joseph, 2013). They recommended a minimum requirement, six types of information on NPOs websites: mission/vision; performance goals and outcomes; success stories/testimonials; broader community impacts; staff list; and board list. In a web content analysis of 154 Northeast United States NPO websites, 62% websites disclosed their board members and 75% published a list of staff. Although Lee and Joseph (2013) did not present the type of information about staff and the board, it is most likely that the employees' and board members' personal information was made available on most NPOs' websites.

Research on public organisations' disclosure of personal information was limited. A preliminary study on 16 public organisation websites from six countries examining employees' personal information disclosure identified that more than 80% of websites publish names, occupations and photographs of employees (Badrul et al., 2014).

An earlier study investigating e-Governance strategy focused local Government websites from the Philippines, and discovered content related to employees' information. From a total of 102 Philippines city websites, the author reported 35% of the websites publish heads of departments while 11% disclose organisation structure (Siar, 2005). Similarly, the personal information of employees was present in the United States websites. In a study of 51 states of the United States e-Government websites (including Washington D.C. as a separate extra state), Zhao and Zhao (2010) identified that employees' information, such as full names (47%), job titles (6%) and affiliations (0.5%) were available. They further stated that no information about employees' salary and residence was published. While their results revealed that some employees' personal information was available on United States Government websites, it was measured by using the site's internal search tool. Only six types of personal information were tested using the site's search tool, which meant that their findings on types of personal information are not comprehensive since other types of personal information were not evaluated.

2.3.3 Consequences of personal information disclosure

With the abundance of sources of personal information on the Internet, researchers have looked into privacy issues, perception and behaviour of individuals. Revealing personal information online attracts unnecessary implications towards a user's privacy. Users are exposed to privacy risk due to the potential of negative consequences (e.g. identity theft, phishing) (Choo, 2011).

Since the concept of OSN sites involves self-representation to others, it is common for users to share their personal information for online interaction and communication. Gross and Acquisti (2005) started looking into the disclosure of personal information by Facebook users and its privacy implications. Personal information that is made available may put Facebook's users at risk of threats, either physically or online. The authors listed potential threats that may arise due to geographical information, visual identification, and unique personal attributes (e.g. social security number, birthdate and phone number). Nevertheless, Facebook users can minimise the threats by configuring their privacy settings to limit the visibility of information according to different categories of people. The privacy settings offer users control over their personal information by being able to determine who could access their content and which pieces of content are accessible (boyd & Eszter, 2010). Early studies on Facebook's privacy settings suggest that users were not concerned with restricting their profile visibility. A year after Facebook was introduced, a very small number of undergraduate users were utilising the privacy settings (i.e. 1.2% of 4,540 users) (Gross & Acquisti, 2005). Three years later, 11% of 464 students were found to be limiting access to their profiles (Kolek & Saunders, 2008), suggesting that the awareness of privacy had increased although it was still at a minimum.

Recently, Facebook users are found to be more concerned about their personal information. A longitudinal study of 1.4 million New York City Facebook users from March 2010 to June 2011 discovered that users appear to have more awareness about their privacy as they are changing their default privacy settings (Dey, Jelveh, et al., 2012). Users' practice of configuring nine attributes from public to private saw an increase from 12.3% in March 2010 to 33% in June 2011. As an example, friends lists were hidden by 52.6% of users, up from 17.2% in 2010. They discovered that the increase in awareness appears to stem from media attention and Facebook's privacy page redesign. Similar findings by Stutzman et al. (2013) also highlighted the upward trend of users keeping their data private between 2005 to 2011.

However, OSNs privacy settings can be easily compromised and personal information can be uncovered even though limited information is disclosed. Although users might employ strategies to protect their personal information on OSN, it was demonstrated that additional information from a specific individual can be disclosed by implementing several techniques. This stream of research explored the possibilities of revealing the identity of an individual based on the limited personal information that was posted. Among the techniques that were discussed are information reference algorithms (Gross & Acquisti, 2005); de-anonymisation algorithms (Wondracek et al., 2010); and re-identification algorithms (Yang et al., 2012).

He et al. (2006) further demonstrate that even by only sharing common attributes with friends, users' other personal information can be revealed by performing the Bayesian inference approach. A Bayesian network is a graphical model of joint probability distribution among variables of interest. Mislove et al. (2010) managed to infer personal information with up to 80% accuracy, even with very little information from the individual while Zheleva and Getoor (2009) focus on inferring user personal information from groups that individuals joined. For example, by analysing friendship associations, Jernigan and Mistree (2009) were able to predict sexual orientation and Dey et al. (2012) demonstrated a method for predicting users' age by analysing friends' information. Therefore, while personal information in OSNs can be restricted, it is still possible to infer or aggregate that information by implementing some techniques in order to explicitly identify an individual.

While disclosure in OSNs has attracted concern on the disclosure of personal information, similar concern has surfaced when personal information is disclosed on other platforms. Shopping online means that personal information is also transacted. Concern about individuals' privacy was identified as one of the major challenges in consumers adopting e-commerce (Brown & Muchira, 2004). For example, in e-commerce studies supplying personal information was one of the main barriers identified for participating. (Liebermann & Stashevsky, 2002). This was due to the knowledge that marketing and advertising companies are collecting personal information in order to understand their customers better (Aïmeur & Lafond, 2013). Researchers began to investigate how e-commerce should handle the personal information of its users or consumers. Recently, the issue of personal data retention was raised to increase protection for consumers' privacy (Corbett, 2013). She argued that e-commerce companies who hold consumers' personal information should be allowed a limited timeframe to store it. The author further suggests a standard international level of regulation to the privacy of individuals given the fact that personal information can be copied, transferred, misused and collected easily in the online environment.

In a piece of US research, 27% of those employed stated that their personal information e.g. biography, contact information, and photo are available on their company's or employer's website (Madden et al., 2007). Meanwhile, in the public administration domain, a preliminary study by Badrul et al. (2014) focusing on employees' personal information found that all of their 16 sample government websites from six countries disclose personal information of their employees. In contrast to OSNs, personal information on organisations' websites are publicly available for users. By using public information, Kozikowski and Groh, (2011) were successfully able to infer additional personal information of OSN users. Thus, with 'official' public information at hand, this information can be used to identify individuals and may invite malicious threats to government employees. For anyone to launch an attack, they must first discover the true identity of the target (Yang et al., 2012). Government websites may serve this purpose comfortably as it is an easy source for anyone looking for a specific person's information. As demonstrated in the OSNs study, additional information can be inferred by using the few pieces of personal information available to construct a more detailed and rich picture of an individual (He et al., 2006; Mislove et al., 2010). Besides, OSN users have a certain element of 'control' over their personal information while individuals in the obligatory disclosure might not.

In addition, the revelation of personal information by the employees' organisation may have a higher impact on the employees themselves. This is because individuals often identify themselves by referring to their membership of organisations and their profession (Johnson et al., 2006), including university and government employees (Van Knippenberg & Van Schie, 2000). As such, an individual's relationship with an organisation may exert influence on their job-related attitude and behaviours (Van Knippenberg et al., 2007). Thus, subjective knowledge about an individual was exposed to public view via identification of an organisation.

2.4 The concept of privacy

Privacy is a complex concept and it is difficult to define (Joinson & Paine, 2007). Among the earliest published research to define privacy occurs within the law discipline with Warren and Brandeis (1890) considering it as the right to be let alone from the perspective of US Constitution and the common law. Privacy as a fundamental right is a concept that flows along with the idea of Warren and Brandeis. They argued that each individual has the right to decide to whom and how his thoughts, sentiments and emotions shall be communicated. In order to preserve the privacy rights of an individual, the legal and policy approaches commonly focus on regulating how organisations (or companies) process personal information (Bennet, 2000). Among the measures implemented are the introduction of data protection laws. The law seeks to balance privacy issues against other interests relating to the use of personal information. As an example, privacy statements should address users' consent for how their information collected and disclosed while at the same time provide a legal way for it to be processed. However, this definition of privacy was deemed too broad and vague as it didn't provide much indication on the value of privacy against other interests, such as free speech or effective law enforcement (Solove, 2002).

Another concept of privacy is that of 'limited access to the self', and to some extent this overlaps with the definition above as it recognises the individual's desire to determine concealment and being set apart from others (Solove, 2002). This concept argues that privacy should covers physical access, mental and informational access (Allen, 1988). It tends to look at privacy from the perspective of personal property, one's physical body and personal information. However, some privacy scholars argue that the notion of 'limited access' failed to inform substantive matter of access that would implicate privacy, since not all situations pertaining to limited access are private (Rossler 2005; Solove 2002).

With the advancement of the technological and digital landscape, privacy issues are on the rise as a result of disclosure of an individual's personal information. Interestingly, the concept of control over personal information has drawn attention into privacy research, conducted prior to the pervasiveness of the online environment we have today. Westin (1967) introduced a key definition, saying: "Privacy is the claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others... [It is] the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others." (p. 7). He identifies privacy as four states: solitude, intimacy, anonymity and reserve. Solitude is a state of physical withdrawal and is not observed by others, intimacy is where an individual is secluded with at least one other person, anonymity is when the individual is in a public sphere without being identified or under surveillance, and reserve is a psychological barrier against unwanted intrusion. Westin's definition argues that privacy is about the ability to control information available to others, and under chosen circumstances.

Another legal scholar, Altman (1975) defines privacy as: "the selective control of access to the self" (p. 24). This definition suggests that the need for privacy is dynamic across time and situation, and the element of control is characterised by defined boundaries of regulation. Thus, it portrays that privacy, environment, and the person has an important link when studying privacy (Margulis, 2003). Interestingly, both definitions stress the element of information control in their definitions. Similarly, several authors concur that privacy is related to issues of disclosure, personal information and how to control it (Joinson & Paine, 2007; Altman, 1977).

From the discussions above, privacy can be applied to various concepts, such as informational perspective to privacy (Altman, 1975; Petronio, 2002), privacy as a right (Warren & Brandeis, 1890; Westin, 1967) and physical and expressive properties of privacy (Altman, 1975; DeCew, 1997).

Due to the highly complex nature of privacy, attempts have been made to define it by describing its dimensions as an alternative approach. For example, Burgoon et al. (1989) put forward four dimensions namely: the physical dimension, the interactional dimension, the psychological dimension, and the informational dimension - while DeCew (1997) proposed the informational dimension, the accessibility dimension and the expressive dimension. These descriptions consist of the idea of control and access considerations as presented above, and also recognises the importance of an informational dimension when discussing privacy.

However, as a result of technological developments, a pragmatic approach to privacy has been suggested that focuses on privacy issues and its harmful consequences, according to a particular context (Solove, 2002; Hughes, 2015). Solove claims that privacy issues involve disruptions to specific practices including activities, norms and traditions. His taxonomy specified four basic groups of harmful activities to the individual: information collection, information processing, information dissemination and invasion (Solove, 2006). Similarly, Nissenbaum (2004) argues that there are norms specific to a particular situation that regulate the gathering and distribution of personal information. Privacy invasions occur when these norms are violated (see section 2.12). Therefore, it is the particular context rather than type of information that makes information privacy sensitive, which could be the reason why individuals seek privacy entitlements over non-sensitive information.

Of direct relevance to this research is the information dimension which relates to the ability of individuals to control and decide who has access to their personal information. This was further defined by Clarke (1999) when discussing the concept of information privacy:

“Information privacy refers to the claims of individuals that data about themselves should generally not be available to other individuals and organisations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use” (p. 60).

With these definitions of privacy, general emphasis is put on the importance of personal information, with the ability to control it from unintended parties and unauthorised usage. That said, this research is exploring public disclosure of personal information by a particular entity that has a direct relationship with the individual, and its relationship towards individuals’ privacy in an online environment (e.g., a specific website or organisation).

Thus, with the increased use of the Internet, a large amount of personal information is being disclosed online. In the online environment, while there is a lack of physical space, higher interactions are conducted through the web. Personal information that was published on the Internet will last indefinitely into the future. Moreover, information is available to a significantly large and invisible network of information seekers (Dinev & Hart, 2006). As a result, Internet users are concerned with the availability of personal information online (Madden & Smith, 2010).

2.5 Privacy concerns

Most privacy studies suggest that generally Internet users are concerned about their privacy when they are online. Privacy concern refers to the: “beliefs about who has access to information that is disclosed when using the Internet and how it is used,” (Dinev & Hart, 2006 p. 65). In general, privacy concern is related to the collection and use of personal information, which may arise from different perspectives. Worth noting is that privacy concern was regularly selected by privacy researchers as the proxy of privacy when measuring or defining privacy (Xu et al., 2008).

Early studies investigating privacy concerns focused on consumers in three different countries (i.e. United Kingdom, United States and Germany), and showed that more than 68% of consumers in each of the countries believed that they have lost control over how their personal information was used and collected by companies (IBM, 1999). Similarly, a study on privacy concerns using a telephone interview survey reported an overwhelming 84% of adult American Internet users were concerned that their personal information can be collected by companies and strangers (Fox et al., 2000). The consequences resulting from the availability of their personal information online, such as identity theft and access to and distribution of personal information, were of primary concern for Internet users (Paine et al., 2007). Another study of 1,698 Internet users reported that almost one-quarter (24.6%) were concerned about their personal information online and more than half are concerned with active searching for others' personal information online (Mesch, 2012). A recent study by Pew Research Center found that more than a half of US Internet users were worried about the availability of their information online, compared to 30% in 2009 (Rainie et al., 2013).

To better understand information privacy concerns, several authors have conducted research on this issue. Smith et al. (1996) identified the four primary dimensions of individuals' privacy concerns about organisational information privacy practices as *collection, unauthorised secondary use, improper access* and *errors,* and this resulted in the development of the Concern for Information Privacy (CFIP) scale. Specifically, *collection* refers to the concern of a massive amount of data being collected. *Unauthorised secondary use* describes the concern that information is being collected for one purpose but is being used beyond its intended purpose. *Improper access* relates to the concern that information held by an organisation is readily available for those who are not authorised to view or work with it. Finally, e*rrors* refer to the concern that protection of data is inadequate against accidental and deliberate errors. Building on this, Stewart and Segars (2002) found their result was consistent with Smith et al. (1996) and they further suggest enhancement for measuring the dimensions following advances in technology and research. They proposed a higher-order construct with the same dimensions and items as Smith et al. (1996). Malhotra et al. (2004), discovered three dimensions of privacy concern: *control* (over personal information), *awareness* (of privacy practices of organisations collecting personal information) and *collection* (of personal information) on general Internet context. They developed a multidimensional scale of Internet users' information privacy concern while Dinev & Hart (2004a) suggested *abuse* and *finding* when individuals are participating online. *Abuse* refers to the misuse of personal information while *finding* are concerns about being monitored and the availability of personal information on the Internet.

On individual perspectives, personal information that was disclosed to organisations may put this particular personal information in danger of misuse. Similarly, in this context of study, personal information of employees disclosed by public organisations on websites may expose employees to privacy implications, as this information may be collected easily by any website users/visitors. According to Solove (2006), the collection of personal information is considered a harmful activity. Once collected, employees' personal information may be used beyond its intended purpose. For example, it may be sold to and used by a third party without authorisation, i.e. for marketing purposes. Information abuse, such as creating fake profiles, may raise employees' concerns. Fake profiles of employees can be created based on information published on organisational websites and these profiles are later used to launch an attack. Thus, this tarnishes the image of employees and subsequently the civil service. As a civil servant, it is the responsibility of the employees to uphold the reputation of the civil service.

In addition, information that is published should be free of errors (Smith et al., 1996). Erroneous employees' information may lead to misidentification of the employee, unreachability and misperception of individuals. An employee that claimed to be working at a particular organisation may discover that his status as an employee is publicly questionable when inaccurate information about him is published, as the public may not able to reach or contact him.

As a comparison, disclosure of personal information on OSN is largely conducted by the individuals themselves. While the OSNs offer users the ability to decide and manage the disclosure of their personal information (Dwyer et al., 2007), similar means are less observed with obligatory disclosure. The impacts of personal information disclosure were discussed in section 2.3.3.

Individuals are seen as having lost control over their personal information when it is published on an organisation's website, as personal information of employees can be collected without their knowledge. Employees are not able to decide for themselves how their information will be used and this may lead to negative consequences.

2.5.1 Privacy concern measurement

Since online privacy concerns started drawing high interest from scholars, several authors have attempted to conceptualise and operationalise privacy concerns in more detail. The two most widely used scales are the Concern for Information Privacy (CFIP) scale by Smith et al. (1996) and the Internet Users Information Privacy Concerns (IUIPC) by Malhotra et al. (2004). Dinev & Hart (2004a) argued the importance of envisioning users antecedents when measuring privacy concern, and Buchanan et al. (2007) suggested an unidimensional scale to measures specific privacy concerns.

The APCO model (Smith et al., 2011) presents privacy concerns as a proxy when measuring privacy. By way of illustration, this model was later adopted by Miltgen & Peyrat-Guillard (2014) when discussing factors and the outcome of privacy concerns. These factors are classified as individual factors, contextual factors, macro factors and privacy outcomes (belief and behaviours). Individuals' privacy concern was found to affect individual's psychological and privacy-related behaviour (Dinev & Hart, 2004b; Malhotra et al., 2004; Stewart & Segars, 2002).

2.5.2 Antecedent of privacy concern

A number of authors have investigated individual factors that influence privacy concern. Demographic factors, such as gender, have shown that relatively men were less concerned about their privacy than women (Joinson et al., 2010; Youn, 2009; Janda & Fair, 2004; Hoy & Milne, 2010; Fogel & Nehmad, 2009; Liebermann & Stashevsky, 2002), while no significant effects were found by Ji & Lieber (2010). In addition, age (Janda & Fair, 2004; Joinson et al., 2010; Laric et al., 2009; Nosko et al., 2010), race

(Laric et al., 2009), and income and education (Zukowski & Brown, 2007; Liebermann & Stashevsky, 2002) were found to have a significant impact on individuals' privacy concern. Another piece of research on adult Internet users reported that married users perceive higher risks on the Internet than single users (Liebermann & Stashevsky, 2002).

Research suggests that personal knowledge and experience (Smith et al., 1996) triggers stronger concerns about privacy. This is true with individuals that have direct experience with invasion of privacy (Bansal et al., 2010). However, Internet knowledge is particularly interesting as it was found to have a mixed effect on individuals' privacy concern. Dinev and Hart, (2004b) found that Internet literacy had a negative impact on privacy, and similarly Bellman et al. (2004) and Metzger (2004) presented the same result for Internet experience. Higher web usage was found to have a higher impact on privacy (Zviran, 2008), whereas experience and skills in using the web did not have any impact (Zviran, 2008; Janda & Fair, 2004). However, inconsistent findings were discovered for Internet fluency and Internet diversity (Yao et al., 2007) and this could suggest that Internet knowledge is complex and multifaceted (Li, 2011).

A number of authors empirically tested psychological and social-psychological factors and the results are in accordance with the expectations. Personal beliefs were found to influence individuals' privacy concern (Yao et al., 2007). Individuals were found to have the same ideas and values regarding privacy both online and offline. Individuals who were optimistic in their capabilities and cognitive resources were found to negatively impact their privacy concern (Yao et al., 2007) while perceived vulnerability (Dinev & Hart, 2004a) and perceived control (Xu, 2007; Xu et al., 2008) were shown to be important in affecting privacy concerns.

In addition to individuals' factors, cultural values can influence privacy concern (Dinev et al., 2006; Bellman et al., 2004). Culture can be divided into two aspects, which is at the macro level (e.g. society, country) and at the micro level (organisational or corporate). Most privacy research is focused at the macro level of culture. For example, Bellman et al. (2004) investigated consumers' privacy concerns from 38 countries, and reported that cultural values influence privacy concerns which is in line with findings from Milberg et al. (2000). Milberg et al. (2000) studied information system auditors from 28 countries and suggested that cultural differences affects individuals' privacy concern. Therefore studies from culturally diverse countries exhibited a consistent picture, such as between Italy and the United States (Dinev et al., 2006) and the United States and China (Lowry et al., 2011). Also, these findings were in line with Milberg et al.'s (1995) results in their survey of 30 different countries that observed privacy concern differ across nationalities.

At the organisational scale, culture describes the shared beliefs of employees based on current practice and the norms of the organisation in meeting the organisation’s objectives (Stahl & Elbeltagi, 2004). Hence, the action and perception of employees will be guided by their organisational culture (Stahl & Elbeltagi, 2004).

Numerous studies were found to address cultural differences by adopting the classic dimensions of culture by Hofstede (2001). Hofstede identified five main dimensions of culture that may explain the differences in perceptions of privacy across countries: individualism/collectivism (interest of the individual versus society), power distance (acceptance of unequal distribution of power), masculinity (gender roles distribution), uncertainty avoidance (the extent of uncertain condition) and long-term orientation (difference in thinking). In relation to information privacy, individualism/collectivism was identified as playing the key role in cultural dimensions affecting privacy (Bellman et al., 2004; Milberg et al., 2000; Cullen, 2009).

In addition to cultural values, regulatory structure was also found to impact individuals’ privacy concerns (Milberg et al., 2000). Users in unregulated countries were found to have higher concerns than people in countries with privacy regulations specifically regarding security of online transactions and error in databases (Bellman et al., 2004).

2.5.3 Mitigating privacy concern

A number of studies have been interested in organisational practices and its role in influencing Internet users’ privacy specifically to their customers. Most of them have focused on the privacy policies of websites and information practice structure. Organisations mitigate users’ privacy concerns by displaying a privacy statement or policies regarding the handling and use of personal information. In addition, Lwin et al. (2007) suggests that organisations should strengthen their privacy policy by allowing it to fit in with other regulatory and governmental policies. Another way of doing this is by displaying a privacy policy with third party assurance or seals of approval (Wirtz et al., 2007; Wang et al., 2004; LaRose & Rifon, 2006; Nam et al., 2006). Another area of organisational practice is investigating adherence to Fair Information Practices (FIP) principles. FIP is a guideline to protect the privacy and security of personal information in online environment (FTC, 2000). Similarly, the reputation of an organisation is found to reduce privacy concerns (Andrade et al., 2002), while trustworthiness plays an important role in influencing consumers' willingness to engage in online transactions (Yousafzai et al., 2009).

Trust plays a key role when discussing privacy. It was found to have a mediatory effect between privacy and disclosure (Dinev & Hart, 2006; Metzger, 2004), shown as antecedent to privacy (Bélanger & Crossler, 2011) and a consequences of privacy (Bansal et al., 2010; Malhotra et al., 2004). Having trust in an institution/organisation is often based on the knowledge and reputation that individuals have acquired about an organisation. Trust in the institution refers to a set of beliefs or expectations that: "the institution is competent, fulfils its obligations, and acts in responsible ways," (Devos et al., 2002, p. 484). In this research context, trusting an organisation will imply that individuals believe that that organisation will undertake appropriate measures in processing their personal information. Online trust is more complex than offline trust as the Internet itself is considered an insecure environment, and hence trust is difficult to achieve (Friedman et al., 2000). In fact, there is a low correlation between online and offline disclosure of personal information in interpersonal communication, which means that they differ in trust according to different environments (Mesch & Beker, 2010).

2.6 Privacy behaviour

Prior research into examining privacy behaviour has regarded that an individual's privacy decision making is a rational process. This process is guided by the weighing of anticipated costs (or risks) and perceived benefits (Culnan & Armstrong, 1999; Dinev & Hart, 2006). This privacy trade-off, which is also known as 'privacy calculus', refers to the decision the individual made to disclose personal information, and is determined by the outcome of the privacy trade-off. In a simple way, it means that information disclosure is a trade-off between benefits and risks (Dinev & Hart, 2006). It is posed that individuals undertake the decision in an expected and rational weighing of risks and benefits upon deciding to disclose personal information or conduct transactions (Malhotra et al., 2004; Xu et al., 2009). Individuals disclose information when the perceived benefits surpass the expected losses.

Those benefits can be tangible or intangible. It could be in the form of economic value where organisations are willing to offer something to their customers in return of their personal information (Hann et al., 2007). Furthermore, people are willing to give up their personal information by signing up to become member of an online networking site in return for connecting with other members, or with a webmail service just to have an email account. Thus, the findings highlight the benefits that Internet users are calculating against the impact of disclosing certain personal information. Henceforth, it is not clear what form of benefits and risk might be involved when personal information of employees is disclosed on the Internet.

However, the rational decision model in privacy calculus has been challenged by several authors. Acquisti & Grossklags (2005) suggest that rational considerations may be limited by the knowledge that they had (related to privacy) and capability to process all information relevant to the cost-benefit-ratio. In a mobile applications study, individuals' decision-making was affected by considerations of time frame for risks. Both short-term risks and long-term risks may increase the risk perception and be consequently reflected on the disclosure intention (Keith et al., 2012). A possible explanation as the notions of 'bounded rationality' was put forward to suggest that individuals' ability to acquire and process information are limited and thus rely on what they know (Smith et al., 2011; Acquisti et al., 2015; Keith et al., 2012).

In addition, as argued by some authors (Li et al., 2010; Wilson & Valacich, 2012), the risks and benefits in privacy calculus are strongly related to the situation-specific environment. Kehr et al. (2015) put forward that considerations of a situation-specific assessment may dominate attitudes in disclosure intentions. Concerns of specific risks on mobile applications were suggested to outweigh their general privacy concerns in disclosing their registration information (Keith et al., 2013).

The privacy calculus raises the complexity of privacy decision-making online. Personal information that enters the Internet is accessible to an unlimited audience. Privacy calculus may shed some light upon the fact that people’s willingness to surrender their privacy is based on perceived risk and benefit. Certainly, information that is shared on the Internet albeit by others, should be explored within its specific context. Thus privacy decisions are also based on a set of contextual and heuristically defined preferences (Kehr et al., 2015). This study furthers existing research by conducting the study in a public organisational context. In this regard, the present research is exploring privacy issues in situation-specific assessments (i.e. e-Government websites).

Furthermore, while privacy calculus has been examined in a different context, such as e-commerce (Acquisti, 2004), the Internet (Dinev et al., 2012), OSNs (Gross & Acquisti, 2005), Internet of Things (Kowatsch & Maass, 2012), and mobile applications (Xu et al., 2009), limited research was conducted in respect of the constituencies of government.

2.6.1 Privacy paradox

Researchers who studied privacy concerns found users who claimed to have high concern about their privacy often did not translate it towards their privacy behaviour. People showed differences between their stated privacy attitude and their actual privacy behaviour (Acquisti, 2004; Metzger, 2006; van de Garde-Perik et al., 2008). This attitude-behaviour gap, also known as the ‘privacy paradox’, refers to discrepancies between the reported privacy attitude and actual privacy behaviour (Norberg et al., 2007; Kokolakis, 2015).

Norberg et al. (2007) compare disclosure willingness to actual disclosure in their two-phased study. During phase one, a sample of graduate students were asked about their willingness to disclose specific pieces of information. Several weeks later, in the second phase, the subjects were asked to disclose the same kind of information to a market researcher. The research reported that individuals reveal significantly greater amount of personal information than their stated intention indicated. They attributed this to the effect of risk perception that plays a stronger role in the willingness of disclosure.

Another research in the OSNs domain reported that there is little or no relationship between online privacy concern and self-disclosure behaviour (Tufekci, 2008). Participants' concern about privacy on Facebook and their posting behaviour were also found to have little correlation (Reynolds et al., 2011).

In trying to explain this, Acquisti et al. (2015) suggested that privacy attitude and privacy behaviour shouldn't be assumed to be closely related due to the illusory characteristic of the paradox. Indeed, the weak link between attitude and behaviour was acknowledged by Ajzen and Fishbein (1977) in their work in the late 70s. Further, Acquisti et al. (2015) cautioned that the paradox should also account for the contextual element of the situation, and the weighing of costs and benefit analysis has to include the misperceptions of the costs and benefits in decision making.

2.7 Information sensitivity

Individuals were found to have different levels of sensitivity towards certain types of information (Rohm & Milne, 2004). Li (2011) categorised these as information contingencies and further divided it into types of information and information sensitivity.

Weible (1993), has defined information sensitivity as: "the level of privacy concern an individual feels for a certain type of data in a specific situation" (p. 30). In short, information that is relatively insensitive has a lower privacy concern to be disclosed.

It has been observed that different types of personal information impact individuals' privacy concern in different ways (Ji & Lieber, 2010). In contrast, personal information requests demonstrate lower privacy concerns compared to financial information requests (Ward et al., 2005). This suggests that it can mean different things to different people and it has to be contextually analysed. Acquisti (2004) poses that when discussing privacy the context must be defined to offer more accurate findings on privacy issues.

2.7.1 Contextual nature of privacy

It has been argued that privacy differs across cultures according to its rules and social norms within cultures (Westin, 1967). Thus privacy may exist in different forms under different societies. Since privacy is neither static nor objective in nature, this is highly contextual (Margulis, 2011). The concepts of boundaries in privacy are subject to certain rules, and is subject to change depending on context (Petronio, 2002). Several studies have explored the contextual nature of privacy. A study examining individuals' behaviour in disclosing personal information suggested that the amount of personal information disclosed differs according to the context (Emanuel et al., 2014). A total of 148 participants from two UK universities were required to disclose themselves under four different contexts: in private (as a baseline), face-to-face (offline), a generic online context and a specific online context (i.e. dating or job-seeking). Participants were willing to disclose more information face-to-face compared to the online platform. With regard to online space, a generic online space assists in more disclosure compared to context-specific online spaces. The authors argue that contextual factors greatly influence an individual's disclosure behaviour, which is in line with findings from van Dijck (2013). Further, understanding the receiver of the information is another reason for what individuals choose to disclose online (boyd, 2004).

Li et al. (2010) provided an example that situational factors at a specific level, e.g. specific online websites, influence privacy-related perceptions of individuals. They discovered that monetary benefit may undermine information disclosure if the information requested is deemed of out of context. Additionally, individuals' perception towards different categories of websites influences their decision on disclosing their personal information (Hsu, 2006).

Because privacy is highly contextual, Nissenbaum (2004) argues that since the flow of personal information is entrenched in a specific context, it is governed by context-specific norms. Nissenbaum proposes contextual integrity theory to explain why certain communicated information leads to an invasion in privacy and some does not. Discussion on this theory is presented in section 2.12.

Thus, privacy scholars have noted the importance of addressing situation-specific concerns instead of general privacy concerns, due to the contextual nature of privacy (Margulis, 2003). Privacy concerns focus on situation-specific concerns investigate individual's perceptions on a specific website, and found that an individual's attitude and belief in a website-specific situation may have a higher influence on privacy concern than general Internet situation (Li, 2014). As such, the contextual emphasis of privacy into situation-specific parameters is investigated in this study by focusing on public organisations websites.

2.8 Privacy risks

With the Internet becoming a fertile ground for personal information hunting, preserving Internet users' privacy from emerging user threats are becoming more important (Bélanger & Xu, 2015). Internet users are exposing more of their personal information online, including sensitive information with the increase in online commerce transaction and social media uptake (Jang-Jaccard & Nepal, 2014). Furnell (2010) listed implications and risks that relate to the availability of personal information online which is snooping, cyber stalking, social engineering, identity theft and identity fraud, while Schrammel et al. (2009) made it clear that publishing online contact information (i.e. email, instant messaging) facilitates online stalking. Personal information is also used as an authentication mechanism by many web systems, as in online banking and email password recovery. In an organisational context, several studies have revealed risks associated with the release of personal information such as selling of personal data (Corbett, 2013; Culnan, 1993), unauthorised access and theft (Rindfleisch, 1997), and sharing information with government agencies (Dinev & Hart, 2006; Smith et al., 2011). Thus, the availability of personal information online increases the risk of individuals to various privacy and social engineering attacks.

Social engineering (SE) is a technique used to manipulate people into divulging confidential information to compromise information systems through influence and persuasion (Krombholz et al., 2015). Within organisations, employees were often being targeted and manipulated to extract confidential information (Brody et al., 2012). According to Allen (2006), there are four steps in SE attacks namely: 1) information gathering; 2) relationship development; 3) exploitation; and 4) execution. The first step is vital in launching a SE attack. Information can be easily gathered from publicly-accessible websites and this information could be the personal information of employees (Luo et al., 2011). Then the SE attacker tries to establish trust with the employees, with the intention to persuade them into desired actions and finally carry out attacks. Thus publishing employees' information on the website increased the risk of a SE attack through the employees.

Social engineering attacks are varied from technical to non-technical means. They are categorised into physical, technical, social and socio-technical approaches (Krombholz et al., 2015). Among SE attacks towards employees are dumpster diving, reverse social engineering, search engines, baiting, pretexting and phishing. Despite the different approaches of attack, a common important substance is an employee's personal information.

Displaying personal information (e.g. full name, phone number, address and date of birth) can be potentially harmful to individuals, specifically relating to the possibilities of identity theft (Nosko et al., 2010). In the same way Irani et al. (2011) acknowledged that attributes such as name, gender, date of birth, hometown and location pose a potential password recovery attack. This attack requires the attacker to produce personal information in answering related questions to recover passwords. By knowing these attributes, an attacker is able to answer password-recovery questions and gain access to the targeted account. In the Sarah Palin case (Stephey, 2008), her personal information such as postcode, date of birth and high school were found on Wikipedia. The attacker used this information to reset the password of her Yahoo email account. Similarly, a conventional SE attack - such as dumpster diving, that searches for specific information through an organisation's trash bins or dumpsters - can be shifted to the online platform by searching on the Internet. Thus organisations (as well as employees) need to be more aware of publishing personal information on their organisation's website.

Furthermore, a single full name was shown to be able to successfully infer the ethnicity and religion of an individual (Mateos, 2007; Mateos et al., 2011; Webber, 2007; Nanchahal et al., 2001). Thus, revealing personal names will increase the risk of inferring additional personal information of an individual.

The vulnerability of publishing actual names becomes more apparent when it is linkable with an OSN profile. A study from Young & Quan-Haase (2009) found that 99.35% of users from a university use their full name as their profile name. This result reflects earlier research by Acquisti and Gross (2005) that discovered a high amount of personal information disclosure on OSN.

Public profile information from online social networks were shown to be able to identify more complete range of individual’s attributes by aggregating it. Completeness of up to 83.3% was discovered on average, compared to each profile from different services (Abel et al., 2010). Although this technique has been shown to reveal more information about specific users, there is a possibility that users may reveal inaccurate information to protect their privacy. In contrast, personal information from organisation websites are known to publicly reveal information that is accurate, credible and updated. It is believed that aggregating both information from OSNs and organisation websites will paint a complete and accurate profile of individuals.

With sufficient information of an individual, an attacker can perform a pretexting technique, which is creating a well-furnished scenario to persuade a targeted employee to voluntarily reveal sensitive information or perform actions (Luo et al., 2011). An attacker may impersonate a senior or high ranking employee of an organisation, to manipulate junior employees in disclosing information, which is often conducted through telephone conversation.

Furthermore, personal information of individuals gathered from organisation websites can be used to create fake profiles in OSN. The fake profile is then used to send falsified messages which may jeopardise the original user. An Indian ambassador to Saudi Arabia was a victim of a fake profile on Facebook, which used both his real and false information (Mengle, 2016). Since the official holds a high position in the Government, the fake profile could damage and humiliate the ambassador’s reputation and image.

Publishing emails to the outside world can also pose a privacy threat. The email address is another attribute of personal information. There are officials email and personal emails. However, by knowing either of the email addresses, any outside party is able to establish contact. Users might receive unsolicited emails, popularly known as spam emails. Employees considerably use their time managing spam emails and also checking their spam folders to avoid losing genuine emails that were mistreated by the anti-spam filters (Bujang & Hussin, 2013; Caliendo et al., 2008). As a result, employees’ productivity was affected (Moustakas et al., 2005). Furthermore, spam also assists cyber-crime. Spammers can collect publicly available email addresses and construct phishing emails. Phishing is a technique where someone pretends to be from a legitimate entity, such as banks or companies, to deceive employees into revealing sensitive information. Halevi et al. (2013) demonstrated simple phishing attacks to students. Before the attack commenced, they needed to collect the email addresses of their targeted samples. This shows that an important step for beginning a phishing attack is knowing the email address of the victim. As an example, a US Government agency had to be closed down for few days due to a phishing attack where 57 of the targeted 530 employees fell victim to opening an email that installed malware on their computers (Wlasuk, 2011).

A complete full name will assist in launching a spear-phishing attack. This technique is a targeted attack aimed at specific individuals or groups with a clear objective, such as stealing information, infiltrating target networks, financial gain or trade secrets (Caldwell, 2013). Normally this kind of attack requires the attacker to send a clever and convincing e-mail to the recipient. To make this happen, the attacker will use personal information of the recipients' such as a full name, to make it appear convincing and trustworthy. During their eight months of monitoring spear-phishing attacks, the government sector was identified as the prime target (Trend Micro, 2012). They further suggest this could due to the availability of pertinent information on the website, such as contact information and staff. In the first quarter of 2016, 41 organisations were victimised by spear-phishing attacks (Ragan, 2016). Most of the attacks used spoofed emails to impersonate the top management, executives or employees themselves. The disclosure of location information raises privacy concerns (Schilit et al., 2003). Research on location privacy mostly centred on mobile networks, databases and ubiquitous computing in protecting the location privacy of users (Shokri et al., 2011). When location information falls into the wrong hands, it could cause financial harm, personalise spams, harassment, and alter reputation as well as inviting threats to the real world where users' physical whereabouts are known (Schilit et al., 2003; Schrammel et al., 2009).

Photos with a facial image enable an individual's recognition. Photos can provide an indication of a person's age and gender. In addition, group photos convey information of their family, friends or colleagues. This has been shown by (Acquisti & Gross, 2005) that discovered 80% of profile photos from 4,540 Facebook accounts were sufficient for identification.

Posting personal information related to employment may put the organisation at risk on sensitive information or internal matters (Furnell, 2010). A study on phishing awareness of employees within an organisation at the University of Plymouth found that 23% of staff attempted to download a software update within the 3.5 hours after the email was sent. The attack was based on information that was publicly available from the organisation’s website (Furnell & Papadaki, 2008). In their Facebook case study, Nosko et al. (2010) categorise employment information as sensitive personal information which could be exploited to harm individuals.

A study by Symantec consistently reported that employees were targeted through the availability of their personal information on their organisation’s website. In 2012, there was a 42% rise in targeted attacks that focused on employees (Symantec Corporation, 2013). The increasing trend of attacks targeting employees was evidently reported in their recent study (Symantec Corporation, 2016). In 2015, the number of attacks increased by 55% compared to a year before.

2.9 Privacy protection behaviour

Internet users were aware of online threats focusing on individuals (personal), such as stalking, online harassment, trolling, flaming, identity theft or spam (Kang et al., 2013). When faced with situations that are potentially intrusive to users’ privacy, Internet users undertake a few measures to control it. In view to this, they chose to protect themselves by being anonymous online (Kang et al., 2013). Being anonymous intends to limit identifying information from being identifiable. Other than withholding information about an individual, Internet users hide their identity by providing false information, amending identity and simply ignoring or deleting any unwanted presence - for example, emails, pop-ups and online chat request (Chen & Rea, 2004; Kang et al., 2013).

When dealing with disclosure of personal information by others, individuals resorted to conduct self-search (also known as ego-search or vanity search) in order to locate information about them on the Internet (Madden et al., 2007). In a US study, individuals searching for self-information was found to increase from 47% in 2007 to 57% in 2009 (Madden & Smith, 2010). This suggests that individuals are more aware and concerned with the availability of their information online. By using their name as the search query, individuals were able to gather information that was published about them on the Internet. Individuals were concerned when information about them were found to be inaccurate (Madden et al., 2007). Marshall and Lindley (2014) suggested that individuals who conduct self-searches to manage their online presence may cause by specific personal information that they did not want to appear. Individuals are concerned by certain types of information about them that may violates their privacy. Other motivations for self-search are self-search for discovery, self-search for re-finding (information seeking), self-search for entertainment, and for its archival value (Marshall & Lindley, 2014).

Studies in privacy protective behaviour normally utilise protection motivation theory (Rogers, 1975) as their framework (Youn, 2009) in order to understand individual's risky behaviour. Thus, to understand an individual's risky behaviour, privacy researchers utilise protection motivation theory (Rogers, 1975) as their framework (Youn, 2009). According to the theory, the higher privacy concerns that individuals have, the more likely they will be to exhibit privacy protection behaviour (Youn, 2005). This will assist in explaining how individuals cope with potential threats when their personal information was disclosed and available on the Internet. This theory will be discussed further in section 2.12.

However, many users have limited knowledge and capability in protecting their privacy (Acquisti et al., 2015), moreover when they are not in a position to take relevant measures as the disclosure is conducted by a third party. Thus, a 'privacy by design' approach was suggested where privacy requirements are taken into account from the beginning of a system development (Cavoukian, 2012). It enables an organisation to approach privacy as a prevention rather than compliance in order to recognise the privacy values of stakeholders. This approach listed seven key principles towards achieving its objective to minimise information privacy risks through technical and governance controls (Cavoukian, 2009). These principles are 1) proactive not reactive; preventive not remedial, 2) privacy as the default, 3) privacy embedded into design, 4) full functionality

– Positive sum not zero-sum, 5) end-to-end lifecycle protection, 6) visibility and transparency, and 7) respect for user privacy. As a result, a privacy-friendly system that promotes privacy protection and mitigate privacy concerns can be developed.

2.10 Data protection

As stated in section 2.4, privacy as a fundamental right and data protection law are interrelated but different issues. Data protection refers to the regulation of personal data processing of individuals. In the EU, the data protection framework is created for the protection of individuals with regard to the processing of personal data and free movement of data. The EU directive requires all member states to implement privacy legislation (European Union, 1995) in each country, whereas a recent proposed regulation - namely the General Data Protection Regulation (GDPR) - aims to harmonise current data protection laws across EU member states (European Commission, 2016). Thus by implementing the same legislation, the protection of an individual's information privacy can be enforced effectively in light of the Internet's non-territorial nature and cross-border transfer of data.

Different data protection regimes among countries should be minimised in order to adequately protect an individual's information privacy nationally or internationally (Wu 2014). In the context of e-Government, Wu (2014) found that although the data regulation of three countries (i.e. United States, China and Germany) demonstrate similar commonalities in general data protection principles, the implementation differs from one another. For example, German law (and Chinese draft law) covers both the public and the private sectors but the US adopted a more 'sectoral' approach. Another difference is the scope of law protection, where Germany protects an individual's personal data irrespective of the nationality, while the US only protects its citizens & permanent residents. In Malaysia, the Personal Data Protection Act (PDPA) 2010 was enforced in November 2013. The act is modelled after OECD Guidelines, the EU Directive, UK Data Protection Act, Hong Kong Personal Data (Privacy) Ordinance and New Zealand legislation (Hassan, 2012). However, the PDPA was criticised as its scope is limited to the private sector in respect of commercial transactions (Greenleaf, 2013). According to

Greenleaf, even if a government entity is carrying out ‘commercial activities’ the PDPA will likely not apply to them. Thus this act does not protect personal data from the public sector, which raise questions on the protection of personal information on Malaysian public organisations websites.

2.11 e-Government

Introduction

Governments around the world have embraced e-Government initiatives in order to provide better services to their citizens (Carter & Bélanger, 2005). In this research context, the e-Government initiative is focused on government websites where an abundance of information and services are made available on the Internet for public view.

Definition of e-Government

The e-Government initiative was introduced to transform government services by encompassing wide usage of ICT within all public service sectors, in order to enhance, and deliver high quality and improvements in terms of access, information, services and improvement of citizens, businesses and civil society at all levels. ‘e-Government’ is often broadly defined as the utilisation of information and communication technology (ICT) by government agencies to better delivery of government services to citizens, business and other agencies. With the prevalent influence of the online environment, some researchers have highlighted the Internet as the principal single point of access in the e-Government (Willoughby et al., 2010).

Several studies have proposed categorisation of e-Government’s interaction according to stakeholders’ involvement in implementing e-Government initiatives (Stamoulis & Georgiadis, 2000; Ndou, 2004). These categories have been identified as: Government-to-Government (G2G), Government-to-Citizen (G2C), and Government to Business (G2B) (Stamoulis & Georgiadis, 2000). However, some authors suggested including government employees as another category and propose this as Government-to-

Employee (G2E) (e.g Ndou, 2004). These categories place emphasis on specific stakeholders' relationship with the government.

Government to Citizen (G2C) is described as providing citizens access to interaction with the government, in particular through electronic service delivery. Citizens have direct access to information and services, for example applying for a driving license, registering schools, births, and filing tax returns. Such interaction is achieved by establishing a single site providing accurate information, fast delivery and better government services (Bonham et al., 2001; Heeks, 2000; Seifert & Petersen, 2002). The government can later improve services by offering personalised interactions to individuals on the availability of their personal information.

Government to Government (G2G) is where inter-governmental agencies co-operate and communicate online, based on information sharing on their databases. Integrated architecture is required to support a seamless communication environment (Loukis & Kokolakis, 2003). In doing so, it has an impact on efficiency and effectiveness of government services.

Government to Business (G2B) is another category of e-Government interaction where governments facilitate business sector services, such as registering companies, procurement, taxation or business license applications. Companies are able to deal directly through online channels and receive a faster response.

Government to Employees (G2E) supports online interaction between a government and its employees. Among other benefits, this provides employees with online training opportunities and facilitates knowledge sharing as well as allowing employees access to their information (Ndou, 2004). Employees are also empowered to assists citizens quickly and in a proper manner. In addition, this promotes efficiency, has a faster response time, reduces administrative cost, and reduces bureaucracy.

2.11.1 e-Government function

ICT usage is clearly important in order to improve service delivery across all stakeholders (Carter & Bélanger, 2005). Innovation in ICT provides opportunities for government in increasing interaction between governments and citizens. Nam (2014) summarised five types of e-Government use as: service use (using service provided); general information use (information seeking); policy research (searching information about government policies); participation (online decision-making); and co-creation (involvement in developing policies). Although scholars identified five types of e-Government usage, the major purpose of e-Government implementation is basically to refer to the information and services offered by the government (Nam, 2014). The main function of e-Government is to facilitate communication between the government and its citizens via information communication technology, including online presence (Evans & Yen, 2006). Instead, the earlier and basic form of e-Government refers to service delivery to fulfil public needs (Zhao, 2010). The implementation of e-Government has brought an improved quality of service delivery in terms of timeliness, responsiveness and cost-effectiveness.

One of the strategies for delivering e-Government initiatives to the public is by creating a website as an official contact point. Organisational websites are established to present themselves on the web, either for marketing, image building and reputation or to improve services to their customers. A government’s website strengthens its commitment to flourish online, and add new styles of governance in a new dimension (Jaeger, 2003). Generally, this strategy is listed as one of the four major criteria of e-Government as suggested by (Anonymous, 2000).

2.11.2 Government websites

Government websites have become the focal contact point between the government and the public. The main purpose of establishing a government website is to extend its services through online channels (Teo et al., 2009). One of the benefits for the government by providing a website is reducing operational cost while increasing revenues. This is possible because government services and transactions are conducted though the website instead of more conventional means - which is manually and on paper.

However, it is the citizens who will benefit most by the establishment of a government website, as the main objective is to improve the quality of service delivery to citizens (Germanakos et al., 2007). Likewise, information published on government websites should be accurate, relevant and regularly updated to attract users into considering adopting e-Government services (Gilbert et al., 2004).

Eschenfelder (2004) views websites as channels to educate the public, promote transparency and stimulate economic activities. This is why research on government websites is often deeply citizen centric, as it focuses on serving the citizens (Evans & Yen, 2006).

2.11.3 Trust in e-Government

It is important for the government to maintain their website effectively in order to gain higher trust from the public. Trust is another factor that affects the use of e-Government (Gefen et al., 2005). Belanger and Hiller (2006) highlight issues related to trust in e-Government adoption. A study from Teo et al. (2009), suggests users' trust in government is positively related to government websites.

The credibility of a government's website depends on trust and confidence by citizens (Huang & Benyoucef, 2014). Sources are seen as credible when it is 'trustworthy' and 'believable' (Fogg & Tseng, 1999). Low credibility of government websites raises users' concerns regarding security during transactions and unauthorised use of their personal information (Bélanger & Carter, 2008).

However, trust in government websites varied between different countries. A study of four different countries (the United States, the Netherlands, China and Taiwan) and their attitudes towards government websites suggested that Asian countries have a higher level of trust compared to their western counterparts (Hsu, 2006). Less personal information was disclosed by the US and Dutch respondents when interacting with their government websites, while Chinese and Taiwanese people disclosed more about themselves to government websites. Furthermore, Hsu (2006) ascertained that government websites were considered to be the most trusted category of websites (except for the United States) compared to health, commercial, non-profit, or community website categories. Thus higher trust in the government led to higher disclosure of personal information from the citizens. On another note, information and knowledge of government processes and performance were found to increase citizens’ trust in the government and led to an increase in transparency (Cuillier & Piotrowski, 2009; Bertot et al., 2010).

As discussed in section 2.5.3, having trust in an organisation/institution was found to influence individuals’ privacy concerns. In the e-commerce environment, higher trust leads to higher willingness to disclose personal information and engage in online transactions (Yousafzai et al., 2009). Individuals believe that their privacy will be protected by the organisation. Thus individuals depend on the trustworthiness perception to reduce their privacy concerns. However, employees’ trust of their organisation and its relation to their privacy were less explored. Trust of employees towards their organisation (in this case government agencies) and trust of citizens towards their government may be different as it was seen from two different perspectives.

2.11.4 Transparency

The use of ICTs is one approach to promoting efficiency and transparency concurrently (Von Haldenwang, 2004). Through government websites, information can be channelled directly to the citizens. As a result, the public are more informed of any process or decision of the government. In turn, they are able to make better decisions based on the information provided. Dissemination of government information and greater access to that information is embedded within the notion of transparency (Grimmelikhuijsen, 2010; Bertot et al., 2010). For instance, Grimmelikhuijsen et al. (2013) suggests transparency as: “the availability of information about an organisation or actor allowing external actors to monitor the internal workings or performance of that organisation” (p. 576).

Transparency is also regarded as a strategy for fighting corruption (Cuillier & Piotrowski, 2009). For example, by providing information about policy-making and service delivery processes, it prevent government employees’ corrupt behaviour because process and procedure are available on the websites for public view (Shim & Eom, 2008). Consequently, it will reduce unnecessary interventions by government employees in that they felt they were under the watchful eyes of the public (Shim & Eom, 2009). In fact some countries, such as South Korea, Japan, Peru and Brazil, have reported to have shown evidence on controlling corruption (Shim & Eom, 2008).

Transparency on government websites is commonly referred to as the presence of information available on a government's website including information about the organisation, level of accessibility, knowledge of processes and level of attention to citizens' response (Welch & Hinnant, 2003). Researchers on government websites widely used a Website Attribute Evaluation System (WAES) when focusing on transparency issues (Pina et al., 2007; La Porte et al., 2001; La Porte et al., 2002). According to the WAES, disclosing relevant information on the website is considered as one of the criteria for transparency (Demchak et al., 2000). Transparency consists of five elements: a) site ownership; b) contact information; c) organisational or operational information; d) citizen consequences; e) freshness.

Therefore, by disclosing organisational structure, officials and staff e-mail addresses, or the visions of senior officials will improve governmental transparency. These factors were listed in two out of five elements as shown above. Thus, the public will have knowledge of the person behind the management of an organisation, its organisational structure, and be able to directly contact them, and even recognise their visual appearance (Odendaal, 2003).

Siar (2005) points out that among the purpose of disclosing names of staff and organisation structure is an aim to promote citizens' awareness and understanding of the organisation.

While evaluating Greek public hospital websites, Patsioura et al. (2009) suggested that direct communication with government employees is one of the important criteria for hospital's websites. In addition, citizens were found to seek contact information when visiting a government's website (Thomas & Streib, 2003). Publishing contact information on the website is intended to promote the relationship between the government and their citizens (Siar, 2005).

Email is one of the channels available to interact with the government, alongside the traditional methods - by telephone, letter, fax or face-to-face (e.g. counter). Citizens might prefer this mode of communicating (i.e. through the web) due to the ease and speed compared to traditional communication (Thomas & Streib, 2003). Contacting the government through email either to request a service, feedback or lodge a complaint can be done anywhere as long as there is an Internet connection available. With the widespread availability of the Internet, this approach may be a selected choice among citizens. In addition, local government organisations are also making annual reports available on their websites for public viewing or download in an effort to improve transparency (Salin & Abidin, 2011). However, transparency is not without criticism. Possible risks - such as security, legislation, proprietary information and personal privacy - were often put forward as reasons to withhold the information (Piotrowski & Van Ryzin, 2007).

What seems to be dominating research into e-Government websites is a heavy focus on evaluation, usage, and content of the website from the citizen's perspectives. Among the six evaluation criteria for public websites (Karkin & Janssen, 2014), all criteria focused towards the website users including one criteria that specifically focuses on the citizen. The citizen engagement criteria assess the available features that may assist citizens in communicating and participating with the government. Whilst those studies have been largely citizen-centric and have considered organisational aspects (Evans & Yen, 2006; Alcaide-Muñoz & Rodríguez Bolívar, 2015; Weerakkody et al., 2013), few, if any, studies have considered the concept from the employees' perspective.

Personal information of employees that was disclosed on the websites may invite privacy risks to the employees. As discussed in section 2.8, various privacy risks arise where individuals can no longer control their personal information. The practice of disclosing 'public personal information' on the Internet means that individuals' information is easily accessible and be combined from various sources for identification.

2.11.5 Evaluation of websites

Information quality in government websites can affect a user's decision to use a government website (Kaisara & Pather, 2011) and then continue to use it (Teo et al., 2009; Wang, 2008). According to Wathen and Burkell (2002) the usability and credibility of websites are important elements in encouraging information use and services offered by governments. Usability refers to the extent in which the user is capable of achieving specific aims in the specified context (ISO, 1998). Website usability can be simply understood as the subjective user-friendliness of a website in assisting users achieve specific goals (Lee & Kozar, 2012). A high level of usability of government websites benefits users' impression of the government, the services offered and improves the users' performance and experience (Baker, 2009). Credibility can be interpreted as trustworthiness and believability (Fogg & Tseng, 1999). Thirteen credibility evaluation criteria were proposed as a guideline for e-Government websites (Fogg, 2002; Huang & Benyoucef, 2014). For a government, its 'source labels' (e.g. logo or entity) themselves may increase its website's credibility (Tseng & Fogg, 1999).

Website evaluation is based on a number of characteristics and features that the website offers. Various methods and tools have been proposed for website assessment (Bauer & Scharl, 2000; Pinto et al., 2007; Panopoulou et al., 2008). Bauer and Scharl (2000) put forward the technique of evaluation using a software tool for website, Pinto et al. (2007) evaluate universities' websites for their quality of information dissemination, and Panopoulou et al. (2008) proposed a framework for evaluating government websites.

Panopoulou et al. (2008) identified seven broad criteria for evaluating the websites of public authorities. As pointed out by Panopoulou et al. (2008), the criteria are: content; navigation; public outreach and communication; accessibility; privacy and security; online services and citizen participation. Based on this criteria, four dimensions of evaluation were proposed for public authority websites. The first dimension is the *general characteristics* dimension that includes *accessibility, navigation, multilingualism, privacy* and *public outreach.* This dimension seeks to assess the availability and functionality of websites (Smith, 2001).

Accessibility generally refers to a website that facilitates information available to all citizens. Kopackova et al. (2010) define it as the feature of websites that produces no or minimal obstacles for any users trying to access its contents. Access to everyone, specifically by disabled users, are an essential aspect in this factor (Paris, 2006). When evaluating a quality of a particular piece of information, its *visibility* from the homepage is an important criteria prior to the accessibility of information (Pinto et al., 2007; Pinto et al., 2014). Information that is clearly visible from the homepage will enable users to locate it without any difficulty. This will allow users to access specific information direct from the home page.

Navigation is interested in website's functionality and user-friendliness (Pinto et al., 2007). Search functionality has been identified as assisting web users in finding information in a quick and easy way (Tate, 2010). An internal search engine is a useful navigational feature that should be incorporated into government websites (Panopoulou et al., 2008). Thus, *findability* of information is an important requirement for e-Government websites (Kopackova et al., 2010; White, 2003). It is not only related to how easy it is to discover or locate objects, but also how the website provides users with assistance in finding their needed information (Shieh, 2012). Another feature is having a site map or an index which could provide a quick overview of webpages within the entire site. This is a helpful navigational aid in determining the coverage of a site and to let users know the 'positions' around the website (Pinto et al., 2007). In order to improve the user's experience, Basu (2002) suggests that users should find what they are looking for in three clicks or less.

Multilingualism refers to the ability to provide more than one language on the websites. This will facilitate information to a larger audience by not restricting to national language(s) (Bauer & Scharl, 2000).

The *privacy* factor focused on public concerns when engaging in online transactions and services on government websites (Bélanger & Carter, 2008). The public should be informed of strategies that ensure secure and private data transmissions are taking place. Studies suggested that encryption of data and a privacy and security policy that explicitly informed users about the handling of their personal information (Tate, 2010; Smith, 2001) can improve users' adoption of e-Government (Beldad et al., 2012). In fact, website policies are considered as an important factor for *quality assessment* of specific features of information (Pinto et al., 2007).

The final factor in this dimension is *public outreach*. Improving service delivery is one of the major aims of e-Government. To strengthen service delivery and improving two-way communication, adequate contact information including relevant personnel information should be provided and encouraged (Panopoulou et al., 2008; Smith, 2001; Holzer & Kim, 2005). This will expedite responses towards citizens' requests and feedback.

The second dimension is the *website's content (e-content)*. The *content* refers to the information that was provided and its characteristics. Among them are the accuracy, relevancy, reliability, frequent updating and consistency of information (Garcia et al., 2005; Smith, 2001; Holzer & Kim, 2005). The three factors encompassed in this dimension are *general content*, *specific content* and *news and updating*.

The *general content* is information about the organisations themselves, such as the mission and vision, a message from the organisation's representative, internal organisational details, services provided and other relevant information. Information about an organisation is normally considered as criteria for *authority*. *Authority* refers to information about the owner or responsible entity of the website, and this information assists in improving quality and credibility of a particular website (Pinto et al., 2007). This criteria is normally measured by the presence of an organisation's logo, name and webmaster data.

Specific content focuses on more specialised content, such as e-procurement services, financial information and vacancies availability (Panopoulou et al., 2008; Garcia et al., 2005). Finally, *news and updating* assesses whether the website is regularly maintained and updated. The availability of an online calendar and local news enhance the visibility of updating (Panopoulou et al., 2008). In addition, Pinto et al. (2014) used the term *updatedness* when measuring whether users are aware of the date of last update.

The third dimension and fourth dimension are *e-services* and *e-participation*. In contrast to the earlier dimensions, which focus on the information, both of these dimensions address online service. Therefore, this research will not delve into the details of both dimensions but will present the main idea for each dimension. *E-services* refers to the online service provided by an e-Government website. Delivering online services increases the accessibility of services and information to citizens and at the same time results in great savings for both government and citizens (Carter & Bélanger, 2005). This dimension contains two criteria, namely *services number and level* and *general information*. *Services number and level* assesses the number of services that are offered while *general information* examines the interaction possibilities with the government.

Meanwhile, *e-participation* refers to e-participation and access to information by the citizens. Three factors were proposed for this criteria: *information*, *consultation* and *active participation* (Panopoulou et al., 2008).

Although different metrics and characteristics were introduced, in general the assessment concentrated on five criteria namely: content; navigation; public outreach and communication; accessibility; and privacy and security (Panopoulou et al., 2008). Since one of the aims of this research is to evaluate personal information disclosure on government websites, this study focused on evaluating the quality of personal information dissemination that was disclosed via government websites (Pinto et al., 2007; Kopackova et al., 2010). Thus, for a greater coverage of information dissemination, these five main criteria and quality of information dissemination criteria were both considered in the light of investigating personal information disclosure in government websites. By considering this, both issues on personal information diffusion and websites' best practices were addressed.

2.11.6 Benchmarking

In the evaluation of e-Government websites, several international benchmarking assessments were conducted by different parties and organisations. E-Government benchmarking is expected to provide guidelines for organisations, in order to improve their e-Government website's quality (Fath-Allah et al., 2015). In fact, the results of e-Government benchmarking assessments were seriously considered by most public administrators (Salem, 2007). This section presents a few established benchmarking assessments, which were used by academics and the government as a reference while developing and improving e-Government initiatives.

The United Nations (UN) has conducted an e-Government assessment since 2001. The assessment is conducted every two years under the division known as the United Nations Department of Economic and Social Affairs (UNDESA), covering each of the 193 member states. The objective of the assessment is to report a country's e-Government initiatives in supporting sustainable development (United Nations Department of Economic and Social Affairs, 2002). The UN employs an e-Government development index (EGDI) which is a composite indicator that will present the willingness and capacity of a country in implementing e-Government initiatives. An e-Government index is used as a benchmark that will rank member states according to e-Government development. The EGDI were calculated based on three conceptual frameworks of e-Government namely: scope and quality of online services (Online Service Index, OSI), development status of telecommunication infrastructure (Telecommunication Infrastructure Index, TII), and inherent human capital (Human Capital Index, HCI) (United Nations Department of Economic and Social Affairs, 2014).

Another worldwide international e-Government assessment was conducted by Waseda University, Japan. The annual international rankings started in 2004, and ten years later it cooperates with the International Academy of CIOs (IAC) in conducting the assessment. In 2015, 63 countries participated in this assessment. This exercise is expected to inform countries of the common advantages, present the progress of e-Government development, describe the trend of e-Government, and act as a reference for scholars and researchers (Waseda University & International Academy of CIO, 2015). There are nine indicators that are averagely weighted for a final score. The indicators are: network preparedness, management optimisation, online service, national portal, Government CIO, e-Government promotion, e-participation, open Government and cyber security.

Brown University, through its Centre for Public Policy, analysed 198 countries to gauge the available content on e-Government websites (West, 2007). In general, the websites are evaluated based on the availability of information, service delivery and public access. There are seven categories selected in this evaluation, namely: online information, electronic services, privacy and security, disability access, foreign language access, financial reliance, and public outreach.

In 2015, the European Commission published its *12th e-Government Benchmark* report (European Commission, 2015). The report surveyed 33 European countries according to the *e-Government Benchmark Framework 2012-2015*. Five areas of interest were measured based on the action plan, namely: 1) *user centricity,* which measures the availability and usability of services provided; 2) *transparency,* which evaluates how transparent the government is in relaying information about its operations, service delivery procedures and accessibility to users of personal data; 3) *Cross-border mobility,* which measures the extent of providing seamless services across European countries; 4) *Key enablers,* which measures the presence of five technical elements e.g. Electronic Identification (eID); Electronic documents (eDocuments); Authentic Sources, Electronic Safe (eSafe), Single Sign On (SSO); and 5) *effective Government* ,which indicates users' satisfaction in using government services.

In benchmarking reports, all of the assessments employed the ranking approach in order to present the result of their benchmarking. A country with a high ranking score is considered to possess e-Government websites of high quality (Fath-Allah et al., 2015; Veljkovic et al., 2014) and is an indication of their success (Salem, 2007).

In this research context, the focus is towards Malaysian public sector websites. In Malaysia, the Malaysian Government - through the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) and the Multimedia Development Corporation (MDeC) - conducted an annual assessment of Malaysian Government websites. The assessment is known as the Malaysian Government Portals and Websites Assessment (MGPWA) and began in 2005. The aim of the assessment is to provide insights into the state of information and services available for the citizens on government websites. The websites are ranked accordingly from 1 star to 5 stars. High ranked websites with 5 stars are considered to have achieved a high standard for e-Government websites. When the present study was conducted, five criteria (or pillars) were used for the assessment which are: content; usability; security; participation; and services. Generally, the evaluation criteria were based on international standards, in ensuring that the websites were adopting the global best practices in e-Government (Haidar & Abu Bakar, 2012). In 2012, the MGPWA were benchmarked against the United Nations E-Government Survey and the Waseda University ranking (Multimedia Development Corporation, 2012).

2.11.7 e-Government and privacy

A government often has access and the capability to process personal information about individuals (e.g. collecting, aggregating, inferring, and transferring). The collection of personal information by the government understandably raises privacy concerns (Belanger & Hiller, 2006). In the United States, citizens were concerned by the government’s data collection procedure, resulting in perceptions that their privacy is not well protected (BeVier, 1995).

Belanger and Hiller (2006) discuss privacy issues with respect to e-Government. With more governments exploiting the online environment and the technological advancement of the Internet, has led to faster and easier collection of personal information. Personal information is easily entered on websites and stored directly in a database. The information can easily be shared across agencies for various reasons. Further, personal information that was collected without users’ knowledge and consent - when browsing government websites - had triggers for privacy concern.

A government’s decision to publish public records on the Internet has paved the way for a new channel for individuals, companies and any other parties to access and collect personal information about an individual. The growing popularity of conducting transactions and services through an e-Government platform on the Internet has attracted cyber attackers (Zhao & Zhao, 2010). Due to citizens’ protests, some US state governments limit the disclosure of personal information on a government website (Belanger & Hiller, 2006).

Scassa (2014) cautioned on the desire to have more government information publicly available on the Internet, saying this will have privacy consequences in relation to an evolving technological context. The author argued that there is a need for a balance between privacy and transparency when disclosing ‘public personal information’, particularly where it might cause potential harm to an individual. Tzermias et al. (2014) examined Greek Government websites and discovered that a citizen’s personal information can be collected from public data sources.

Another area that was of government interest is the confidentiality of content. Privacy and security guidelines were developed to assess the privacy impact in delivering services, for example from the UK (Information Commisioner’s Office, 2014), US (McCallister & Scarfone, 2010), Canada (Treasury Board of Canada Secretariat, 2012), Australia (Office of the Australian Information Commissioner, 2010) and the Asia Pacific Economic Cooperation (APEC) countries (Asia Pacific Economic Cooperation Secretariat, 2005). It appears that governments across the world are conducting measures to improve the handling of personal information. A security assessment conducted by Zhao and Zhao (2010) towards US state government sites concluded that state organisation websites are secure for protecting employees' and residents' privacy. However, the conclusion was made based on the presence of privacy and security policies and SSL encryption. In addition, the availability of residents' and employees' personal information was tested via the internal search function for six types of information. While this research will focus towards employees' information, a different approach examining personal information is conducted without pre-restricting to any personal information when examining the websites.

2.11.8 Employees' perspectives

Bannister and Connolly (2011) contend that employees have the right to personal privacy in the workplace. In the e-Government environment, Bannister and Connolly cautioned on the potential challenges when citizens can 'mine' information, including of that of government employees. Among issues relating to public employees are the infringement of employee (privacy) rights, defensive thinking (where this action resulted on the perception of being watched, and actions are able to be tracked), decisions and policy justifications, non-recording culture and discouragement of critical thinking.

Simpson (2011) highlights how personal information of senior government employees was discovered from government websites. He listed names, posts and salaries of staff from the Ministry of Defence (MoD) and further stresses the capabilities of gathering additional information about these individuals from other sites. Disclosure of personal information on government websites could be a double-edged sword. On one hand, revealing employees' information enables transparency and improves service delivery to the citizen. On the other hand, employees' information often contains personal information about them which made them identifiable.

The framework proposed by Belanger and Hiller (2006) to identify privacy issues in e-Government recognised employees' privacy implications. They even emphasised the importance of this relationship (Government with Employees) so as not to be confused with other categories that involved individuals' relationship with the government.

Although privacy is considered an important criterion in government websites, the focus is primarily towards users i.e. citizens/public. A privacy statement or policy was often mentioned as a feature that could increase trust and users adoption of websites (Beldad et al., 2012). Nevertheless, a statement or policies concerning published information (including employees' information) on government websites were under studied.

It is worth noting that on OSNs individuals have some element of control over their personal information, as they are offered options to either reveal or conceal information. While OSN users are able to decide what information they allow others to know about them (Abel et al., 2010), it is possible that employees don't have this advantage when obligatory disclosure happens. Further, in e-commerce websites, the disclosure is stored for internal use and not publicly available. No personal information is intentionally published for public viewing; however, it may not be the same case with disclosure by organisation. Furthermore, the accuracy of information in the organisational websites is commonly been assumed as being high, especially in e-Government, as shown in the literature.

2.12 Theoretical considerations

This section discusses the theoretical basis that informs and constructs the research framework for this study. This study integrates several relevant theories as an initial theoretical basis to guide this study through the early phase of research (Walsham, 1995). In addition, these theories serve as a framework to explain and contextualise later findings. However, the usage of theories in qualitative studies should be carefully employed in order not to be blinded into strictly following it and avoiding potential new explorations (Walsham, 1995). Walsham (1995) further suggested the researcher should have some degree of openness and flexibility on modifying initial assumptions and theories.

Protection motivation theory

This theory was developed to understand how an individual's fear appears and how it influences attitude and behaviour. It posits that individuals protect themselves based on four factors: (1) the perceived magnitude of a threat; (2) the perceived probability of the threat; (3) the efficacy of the recommended preventive behaviour that an individual undertakes; and (4) the individual's perceived self-efficacy (i.e. individual's ability) to carry out the preventive behaviour (Floyd et al., 2000; Rogers, 1975). In general, the individual's intention to protect themselves will depend on perceived threats and their ability to prevent the threats. When the threat is severe and has a high probability of occurrence, the protective intention is high when the person is incapable of addressing the risk. On the other hand, when the threat is rare or doubtful, and the coping mechanisms are effective, the protective intention is low.

Communication privacy management (CPM) theory

This theory, also known as information boundary theory (Li, 2012), suggests that individuals will develop cognitive rules for disclosure or withhold valued information with clearly defined boundaries around themselves (Petronio, 1991). Petronio suggested that these information boundaries are dynamic and judged according to selected criteria, depending on the degree of risk associated with information privacy. This theory predicts that individuals' will decide on their privacy boundaries based on the perceived benefit and cost of information disclosure. The negotiation of boundaries (i.e. strict or loose) is dynamic depending on the situational context, e.g. level of risk related to information privacy (Petronio, 2002). Stanton & Stam (2003) applied CPM theory to the workplace. This theory can assist in explaining the role of information sensitivity in affecting an individual's privacy concern (Rohm & Milne, 2004), and help to further understand how individuals regulate disclosure of personal information.

Privacy calculus theory

This theory posits that an individual's intention to disclose personal information is based on risk-benefit analysis (Laufer & Wolfe, 1977). The decision to reveal personal information depends on the return of certain benefits, and it is based on overall consequences (Xu et al., 2009). This theory builds from the idea of a "privacy paradox" (Barnes, 2006; Jensen et al., 2005), that suggests that individuals are concerned about their privacy but at the same time their behaviour does not behave correspondingly. Previous researchers have reported both competing factors that influence the privacy calculus. Examples of factors that increase privacy concerns are perceived risk and vulnerability (Dinev & Hart, 2006), computer anxiety (Stewart & Segars, 2002), privacy invasion experience (Bansal et al., 2010), and social awareness (Dinev & Hart, 2005), while factors that alleviate privacy concerns and encourage information disclosure are website reputation (Andrade et al., 2002), website informativeness (Pavlou et al., 2007), privacy policies (Faja & Trimi, 2006), information sensitivity (Bansal et al., 2010), social presence (Pavlou et al., 2007), self-efficacy (Yao et al., 2007) and control (Chen et al., 2009). Considering that privacy calculus is a complex process, it is common to incorporate other theories with this one to gain a deeper understanding of these factors (Li, 2012).

Procedural fairness theory

This theory suggests that when there are fair information practices established to protect a customer's privacy, customers are willing to disclose personal information and continue a relationship with the firm (Culnan & Armstrong, 1999). It refers to an individual's perception that the particular activity in which they are involved is conducted fairly. Companies employ procedural fairness to mitigate privacy concerns by publishing privacy policies to inform their customers (Faja & Trimi, 2006). Therefore institutional factors have a high influence on an individual's privacy perceptions (Xu et al., 2011) and this study will include those factors by considering this theory.

Agency theory

Another theory that was initially reviewed is the agency theory. The basis of agency theory is the relationship between a principal and an agent, who are both self-interested parties. It is concerned with resolving problems in agency relationships. It suggests that when the goals of the principal and agent are in conflict and they tend to act in their own self-interest, and the principal has difficulties in monitoring the agent's behaviour. The theory proposes an economic and social mechanism to reduce agency costs, such as creating a documented agreement (Eisenhardt, 1989). Ness and Mirza, (1991) reviewed 150 oil companies in Britain and proposed that agency theory can be used explain organisational disclosure.

Since government employees (principal) provide their information and it is later published on government websites (agent) to pursue each of their interests, it is assumed there is principal-agent problem. For the principal, there appears to be uncertainties with their personal information that was disclosed - such as privacy risk - while the agent used that information for the improvement of service delivery to the citizen. This theory was also employed to discuss privacy issues related to the electronic world (Peslak, 2005).

Contextual integrity

Contextual integrity suggest that the flow of information is defined by norms, which regulates the gathering and distribution of personal information. It refers to the context of information release that matches the individual's preferences in line with the contextual norms of information flow (Nissenbaum, 2004). The basis of Nissenbaum's (2004) argument is that the flow of information is always governed by context-specific norms and people's daily lives revolve within a distinct context. There are two fundamental types of norms, which are: 1) norms of appropriateness; and 2) norms of distribution. Norms of appropriateness deal with: "the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed," (2004, p. 120). For example, sharing a telephone number with strangers may not usually be appropriate, but it may be appropriate when requesting assistance during an emergency situation. The second norms are norms of distribution that refers to the: "movement, or transfer of information from one party to another or others" (p. 122).

Four key parameters of the context-relative informational norms are: contexts (situations where information flows occur); the actors (senders, recipients and subject of information); the attributes (types of information); and transmission principles (constraints on the flow of information between actors in a specific context).

Based on both norms above, individuals, organisations, and society have their own expectations about the appropriateness and distribution of information. When the established expectations are breached, contextual integrity is violated. Violation of privacy happens when the context-relative informational norms are breached (Nissenbaum, 2010).

All six theories stated above will serve as a guide in this study. Generally, this study is focusing on explore individuals' privacy issues when their personal information is disclosed online by a third party. Two theories will be focusing on an individual's internal response to external factors (i.e. *protection motivation theory* and *communication privacy management theory*), while another two focus on organisational factors that influence an individual's privacy (i.e. *procedural fairness theory* and *agency theory*), one theory focuses on an individual's joint effect of opposing factors on privacy perception and behaviour (*privacy calculus theory*), and another theory (*contextual integrity*) will guide on the situation-specific condition.

2.13 Conclusion

The aim of this chapter is to provide a literature review on online disclosure as the phenomenon of interest in this research, as well as information privacy as the focus of the investigation from the perspective of government employees. Definition of personal information was presented and its concepts were discussed. Personal information attributes from the literature were presented alongside its availability in the online world.

Different types of online disclosure were presented including its definition. The relationship between motivation and disclosure were discussed to understand users' perceptions and behaviour towards disclosure. In addition, approaches of online disclosure were explored and the risk of personal information disclosure was shown. A new category of disclosure was proposed, not only for the purpose of this research but because it was necessary to highlight this disclosure as a future focus for research.

Privacy definitions and concepts were discussed. Prior digital era and current Internet landscape definitions of privacy were presented. Factors influencing an individual's privacy, its antecedents and consequences were discussed. The literature review also covers privacy from organisational context with accompanying threats.

E-Government concepts were discussed, focusing on virtual presence. Strategies of providing information and delivering services to the public using official website were presented. The concepts of transparency that promote disclosure of employees' information were reviewed. The literature review found a lack of study focusing on government employees' perspectives, although government employees are stated as one of the important stakeholders in e-Government implementation.

Given that most research on privacy has focused on individuals' intentions to disclose information, this research will explore privacy issues caused by disclosure, not by the individuals themselves. Government employees also have their rights to personal privacy when engaging their work (Bannister & Connolly, 2011). However, it is not clear on the scale of disclosure that does not infringe into employees' personal privacy. As suggested by Belanger and Hu (2015), this research provides an opportunity to explore disclosure issues from the perspective of information disclosure by others, specifically by the practice of organisations.

Therefore, a study to investigate the meaning of 'obligatory disclosure' and how it affects government employees' privacy is indeed important with current developments in online technology.

CHAPTER 3

Methodology

3.1 Introduction

This chapter presents an overview of the research approach that was used to investigate obligatory disclosure, with its impact on employees' privacy. According to Creswell (2013b), three components should be considered in selecting a suitable research approach, namely philosophical paradigm, research design, and research methods. Careful consideration of these components is required because different approaches are suitable for answering different types of research questions and investigating certain phenomena as well as supporting relevant philosophical paradigms. Thus, understanding them will enable researchers to adopt an appropriate research approach and assist in reducing the biases of choosing a particular approach (Orlikowski & Baroudi, 1991).

Research methodology refers to the procedural framework of a study being embarked upon. The chapter begins with a discussion of research paradigms and the selected research paradigm underpinning this research. The chapter then describes the research design for this study and a few available approaches in qualitative research. The rationale for choosing the case study approach is also presented. Next, the chapter discusses the methodology of this research along with the data collection techniques. It ends with a discussion on ethical issues, the researcher's role and strategies for trustworthiness in this study. This chapter concludes with a detailed description of how this study was conducted in order to explore and understand obligatory disclosure from the perspective of public employees.

3.2 Research paradigm

Several decisions need to be taken in order to justify the research approach employed in a particular study. One of the important decisions is the consideration of various philosophical assumptions underlying the researcher's perception of the reality (Denzin & Lincoln, 2005; Creswell, 2013b). The term *'paradigm'* was introduced in 1962 by Thomas Kuhn to represent philosophical assumption (Guba & Lincoln, 1994). While some researchers opt for Kuhn's *'paradigm'* (Lincoln et.al., 2011; Patton, 2002), others are more inclined to use *'worldview'* (Creswell, 2013b), *'epistemologies and ontologies'* (Crotty, 1998) or *'broadly conceived researched methodologies'* (Neuman, 2009). From the research point of view, a research paradigm can be defined as "a basic set of beliefs that guide action" (Guba, 1990; p. 17). This has three underlying assumptions, namely *ontological* (relates to the nature of reality), *epistemological* (what counts as valid knowledge) and *methodological* (refers to the process of research) (Guba & Lincoln, 1994), whereas Creswell (2013a) also considers *axiology* (what is the role of values) as an important dimension in any research approach.

Selecting a research paradigm to fit with the objective of the research should be carefully considered. The chosen paradigm will influence how the researcher approaches the research either implicitly or explicitly because the perception of these paradigms will reflect how the researcher conducts a study. Indeed, researchers often fall into paradigm debate across various paradigm communities (Denzin, 2008). This study will not attempt to discuss this debate but instead focus on a few paradigms that are commonly used by researchers.

In general, there are four most common research paradigms, namely positivism, critical theory, post-positivism and constructivism or interpretivism (Lincoln & Guba, 2000). Meanwhile, Creswell (2013b) prefers to use the term 'transformative' over 'critical theory'. He also adds another paradigm - pragmatism paradigm - in his argument of the widely discussed paradigms. Brief descriptions of each paradigm are presented below.

3.2.1 Positivist paradigm

The positivist paradigm is concerned with the need to find causes that influence effects or outcomes of social phenomena. Positivists believe that knowledge must be based on careful observation and can be measured objectively by employing traditional scientific methods through an appropriate rigorous enquiry (Bryman, 2012). Positivists assume that reality consists of facts and exists independently of the researcher's cognition and experience. Normally, the approach begins with a theory, collects data, evaluates the findings which either support or disapprove the theory, revises and conducts additional tests (Creswell, 2013b). Positivists believe that knowledge can be acquired through observation and personal experience, and facts should be separated from values. This paradigm is normally associated with a quantitative approach and statistical analysis.

Positivism is often criticised because of its assumptions for objectivity measurement. Hence, it is concerned with the researcher's separation from what is being researched, and therefore fails to take into account human interaction and co-constructive nature of data collection with human beings (Hennick et.al., 2011). Another criticism debates on the possibility of a researcher avoiding the interference of personal values or interests during observation (Goldbart & Hustler, 2005). In information systems specifically, experimental studies (e.g. lab experiments) fail to distinguish behaviours between the real world and the experiment because of a subject's knowledge that they are participating in an experiment (Introna & Whitley, 2000). Thus, the argument lies in the questionable internal and external validity of studies using laboratory experiments. Despite these criticisms, studies in information system (IS) were largely dominated by the positivists during the 80s (Orlikowski & Baroudi, 1991). Although lately IS researchers have progressed towards a more diverse inquiry, the dominance of positivist researchers has raised some concerns. Davison and Martinsons (2011) cautioned against 'methodological exclusiveness' and the possibility of IS research becomes irrelevant to situations which are often complex in nature. Hence, it has been suggested that researchers should adopt a plurality of research perspectives (Davison & Martinsons, 2011; Orlikowski & Baroudi, 1991).

3.2.2 Post-positivist paradigm

Post-positivism emerged from the criticism of the positivist paradigm for applying scientific method to research on human behaviour and actions (Creswell, 2013b). This paradigm is also normally associated with quantitative research. The idea that there is an absolute truth of knowledge when researching human affairs was adjusted. Post-positivists acknowledge that the researcher's influence on research and knowledge about reality is bounded by the researcher's limitation. While still believing in objectivity, post-positivists recognise that their findings are fallible and contain errors. Creswell (2013b) listed that post-positivists hold assumptions that scientific theories can only be falsified but not confirmed, that absolute truth can never be obtained but a certain level of approximation is accepted, and that knowledge is shaped by data, evidence, and rational considerations.

3.2.3 Interpretivist paradigm

The interpretivist paradigm assumes that knowledge of reality is socially construed rather than objectively determined (Denzin & Lincoln, 2005). This paradigm is also known as the constructivist paradigm by some scholars (Creswell, 2013b; Denzin & Lincoln, 2005) as it emphasises on constructing meaning by the individual. Interpretivists believe that there is no objective reality and assume that "people create and associate their own subjective and intersubjective meanings as they interact with the world around them" (Orlikowski & Baroudi, 1991, p. 5).

This philosophical assumption is used to understand the phenomena in which people live and work (Creswell, 2013a). It believes that individuals develop subjective meanings of their experiences, and the aim is to utilise participants' complex views of the situation being studied and to make sense of their meanings (Creswell, 2013b). The focus may be on the processes of interaction between individuals or on the specific contexts of situations in order to understand the historical and cultural aspects of the participants (Creswell, 2013a). Thus, it allows for the researcher to construct multiple interpretations of a phenomenon in attempt to make sense of the situations as they emerge. Within this paradigm, researchers' values and beliefs are inherent in all phases of the research process.

Interpretive approaches rely heavily on qualitative methods. Since interpretive research looks for verbal accounts, observations or descriptions which are subjective, it is normally associated with qualitative inquiry methods and analysis (Creswell, 2013b). The most common approaches are qualitative interviews, focus groups and qualitative observational methods. Unlike positivist, interpretive research does not conclude by proving or disproving a theory, testing hypotheses or predefining a dependent or independent variable. Instead, the research aims to achieve deeper understanding of the phenomenon and its characteristics (Walsham, 1995).

One of the criticisms of interpretive studies is the small sample of the study, which limits the generalisability of findings. However, the aim of the interpretivist is not to generalise but to understand a phenomena and the findings can then be used to inform other settings (Orlikowski & Baroudi, 1991). Even so, Walsham (1995) explains that generalisability from interpretive research can be sought according to four types of generalisation: 1) development of concepts, 2) generation of theory, 3) drawing on specific implication, and 4) contribution of rich insight. Thus findings from interpretive studies are generalisable from empirical statements (observations in a case study) to theoretical statements (concepts, theory, specific implications, and rich insight).

3.2.4 Critical paradigm

The critical paradigm, also known as the transformative paradigm, focuses on eliminating injustices such as inequalities, oppositions, conflicts and contradictions in contemporary society in order to gain knowledge (Creswell, 2013b). It challenges the status quo and brings to light the issue of power relations within society and social institutions (Denzin & Lincoln, 2005). In addressing the marginalised people, critical researchers uphold the fact that politics and research inquiry are intertwined for an agenda of reform in confronting social oppression (Mertens, 2010), and have transformed participants' lives including the researcher's as well (Creswell, 2013b).

Since emphasis is placed on political consequences, critical studies were criticised as having lack of validity. Furthermore, prior assumptions about the phenomena may produce biases, which will skew toward the preferred interpretation of data and miss other distinctive findings (Hammersley, 2007). They believed that "knowledge consists of a series of structural/historical insights that will be transformed as time passes" (Guba & Lincoln, 1994, p. 113).

Critical theory can employ various methods to empower the target group. Based on observations, critical research may adopt qualitative, quantitative or mixed methods research design, although it has been noticeably leaning more towards a qualitative study (Hussain et.al., 2013). Its method tends to emphasise the researcher/participant interaction, for the purposes of uncovering suppressed knowledge and associating it with social critique.

3.2.5 Pragmatism paradigm

Pragmatism is derived from concerns with consequences rather than the causes (Creswell, 2013b). As the name implies, it adopts a practical approach to a problem. The core of pragmatism is action and change, including a solution to the problem (Patton, 2002). This means that for pragmatists actions are significant and fundamental to a research study, while at the same time they are not discounting other issues that are centralised around the actions (Goldkuhl, 2004). The pragmatist notion - with regards to knowledge, concepts and values - is shaped by human action and social practice and is meaningful if the actions are useful and work at the time (Goldkuhl, 2004; Creswell, 2013b). Researchers focused on solving the research problem and use all available techniques to investigate it. Thus, practical consequences of the idea or concept are vital in this paradigm (Goldkuhl, 2012).

Pragmatism is normally regarded as the philosophical partner for the mixed methods design (Creswell, 2013b). Since it is not attached to any system of philosophical assumptions, it accepts many different viewpoints and thus pragmatists are free to use both qualitative and quantitative assumptions in their research. Pragmatists are open to many approaches in understanding a research problem, which enables researchers the flexibility and adaptability in their methodological choice (Patton, 2002). The openness from a broad and diverse range of approaches leads to criticism of pragmatism. However, the pragmatist advocates argue that by choosing to limit available approaches, it will lead to research that is "insufficiently reflective and their practice is insufficiently unproblematized" (Greene & Caracelli, 2003, p. 107).

3.2.6 Selected paradigm

This research employed the interpretive paradigm as the philosophical assumption in understanding obligatory disclosure and privacy issues, from the perspectives of participants who were directly involved with this phenomenon. The essence of this study lies in the subjective meanings of obligatory disclosure and how the participants (i.e. employees) see their privacy implications relating to the phenomenon. By selecting the interpretive paradigm, this research is able to understand the participants' experience and meanings by identifying the distinctive nature of their perceptions, beliefs and attitudes through language, consciousness, shared meanings, documents, tools and other artefacts (Orlikowski & Baroudi, 1991).

In order to understand the bigger picture of the phenomenon, this research therefore explored why and how meanings have surfaced from the participants, instead of limiting the scope to identifying privacy implications. The interpretive paradigm allows the researcher to explore a diverse range of experiences in order to gain a holistic understanding of the participants (Creswell, 2013b).

Online privacy issues are gaining increased attention (Hong & Thong, 2013) and research in third party disclosure is limited (Bélanger & Xu, 2015). In addition, little is known about how individuals perceive this phenomenon specifically towards their privacy. Hence, this study focuses on the deeper understanding of the phenomenon and characteristics rather than generating hypotheses and predefining variables as done by the positivist approach (Walsham, 1995). Thus, interpretive assumptions were seen as relevant for this research.

Since privacy is a complex social phenomenon and highly contextual (Altman, 1975; van de Garde-Perik et. al., 2008), while researching privacy, the phenomenon should be context-specific in order to gain the actual understanding of the participants according to the context (Nissenbaum, 2004). Relevant contexts are brought into focus to ensure that the required knowledge is produced. As Orlikowski and Baroudi (1991) claim "... social process can be usefully studied with an interpretive perspective, which is explicitly designed to capture complex, dynamic, social phenomena that are both context and time dependent” (p. 20). Hence, the interpretive paradigm is appropriate for investigating the complex, context and time specific nature of research.

Finally, in response to Davison and Martinsons's (2011) concern that the positivist paradigm is still dominating junior researchers and Ph.D. students’ work, this research adds to the diversity of methods and perspectives in information system research by applying the interpretive paradigm.

3.3 Research design

Creswell (2013b) states that there are three types of research approach in designing a research: qualitative, quantitative, and mixed methods research. Quantitative research is a scientific, empirical and traditional approach that is used to explain a phenomenon by examining the relationship between variables. It is normally associated with the positivist paradigm. Qualitative research is used to explore and understand a phenomenon, and is also known as the naturalistic approach (Lincoln & Guba, 1985). Qualitative research aims to study things in their natural settings as well as attempting to make sense of or interpret phenomena in terms of how people make sense of the world (Willig, 2001). Meanwhile, the third approach, i.e. mixed methods research, involves “collecting both quantitative and qualitative data” (Creswell, 2013b, p. 4). Having considered the three research designs, the decision was made to adopt qualitative research design as the mode of inquiry. The qualitative approach provides the researcher with a greater understanding of the particular experiences of the phenomenon. It involves studying things in their natural settings, attempting to derive or interpret meanings of subject matter to the participants and making sense of it (Denzin & Lincoln, 2013). This approach is also popular within the interpretivist paradigm (Lincoln & Guba, 2005). Moreover, a qualitative approach based on an interpretivist methodological stance is less common in privacy research (Bogdanovic et.al., 2012).

Qualitative research is a broad approach to the study of social phenomena. It is chosen as an approach to explore the complexity of social interactions in daily life and the meanings that the participants themselves attribute to this (Marshall & Rossman, 2011). A qualitative approach is deemed suitable when the issue needs in-depth understanding of hidden beliefs, to hear ‘silenced voices’ and the lived experiences of the participants (Creswell, 2007).

In this research, the main objective is to explore and understand what obligatory disclosure means to government employees concerning their privacy issues. Their concerns revolve around personal information published on an official website, and specifically when the website belongs to their employer. In line with the interpretivist paradigm that implies reality as subjective and socially constructed through language and shared meanings, qualitative research believes that individuals have different perceptions of reality (Savin-Baden & Major, 2013). Another purpose of qualitative research is to understand people and their circumstances (often complex) including individuals, cultures and other phenomena rather than merely testing hypothesis or cause-effect relationship (Savin-Baden & Major, 2013).

Understanding issues in context is particularly important in qualitative research. Qualitative researchers tend to examine the issues in their participants’ natural settings, in which the time and location are two critical considerations of the research. In addition, interpretation of meanings and making sense of the data are normally made according to the context (Savin-Baden & Major, 2013). As this investigation is from the perspective of public employees, qualitative research is considered suitable as it supports the participant’s views from a specific context. In fact, the contextual nature of privacy suggests that qualitative research is appropriate (Nissenbaum, 2004; Ackerman & Mainwaring, 2005).

The analysis of qualitative research uses an inductive approach in which codes, categories, and themes are generated or emerge from the data. It is also concerned with generating a new theory emerging from the data. This demonstrates the primacy of the data i.e. central to meaning where the essence and meanings are derived from the data itself. As opposed to the inductive approach, the deductive approach explores existing theory and tests the theory against observations (Babbie, 2010). Simply put, the deductive approach can be defined as “reasoning from the general to the particular” (Pellissier, 2008, p. 16). The research starts from the general and ends with the specific. For example, from a theory to hypotheses, and testing them either to add to or contradict the theory

(Creswell & Clark, 2007). While it seems there might be some disagreement among researchers as to which method is the most suitable for conducting research, they are not mutually exclusive and can rather be complementary. Some researchers may adopt both inductive and deductive approaches in their research while in other cases a complementing approach may be discovered along the research process.

Since previous research has suggested that disclosure of personal information online has a link with privacy issues (Joinson et.al., 2010), another objective is to understand how obligatory disclosure affects government employees' privacy. Currently there is a limited understanding on issues surrounding 'obligatory disclosure', in relation to an individual's information privacy. As such, qualitative research design is relevant to gather subjective views and opinions of the phenomenon which had been investigated, but little was known (Marshall & Rossman, 2011).

Qualitative research benefits from the data that is directly collected by the researcher. The researcher does not rely on other instruments that were developed by other researchers (e.g. questionnaires). Instead, the researcher may use a protocol (as guidelines) but the information and data are collected by the individual researcher. The values are believed to be evident in the way that they are based on the interaction between the researcher and the people under study (Savin-Baden & Major, 2013). Thus, in qualitative research, the researcher is the primary instrument of data collection.

Qualitative inquiry will provide an in-depth understanding of the social and organisational context, study holistically, elicit tacit knowledge and subjective understandings as well as interpretations (Marshall & Rossman, 2011). Furthermore, Corbin and Strauss (2008) emphasise that among the convenience of qualitative research is the abundance of data sources to be explored.

Creswell (2013a) presents the five most popular qualitative inquiry approaches in the social sciences and health sciences, which are *narrative research, phenomenological research, grounded theory research, ethnographic research,* and *case study research*. Several qualitative approaches were considered in choosing the best approach for this study, namely grounded theory, virtual ethnography, phenomenology, and case study.

This study will discuss four qualitative approaches that were initially considered for this research.

3.3.1 Grounded theory research approach

The ultimate goal of this approach is to generate or discover a theory that is grounded in the data that is systematically gathered (Strauss & Corbin, 1994). Discovery of a theory can appear during actual research, either initially from the data or adapted accordingly based on a relevant existing theory (Strauss, 1987). It places emphasis on the participants' experiences of social and psychological phenomena and allows theories generated from or "grounded" through a process of induction from the participants who have experienced the process or an action (Strauss & Corbin, 1998). Besides discovering theory, this approach also looks at finding an explanation for a process.

However, since the aim of this research is not to generate theories, this approach was not considered for this study. Moreover, grounded theory is a time-consuming process (Hussein et.al., 2014) where in this study, the researcher has a limited timeframe to conduct the research. Willig (2001) suggests that when grounded theory is applied to the nature of experience, it becomes a technique for systematic categorisation rather than unfolding social processes. Therefore, it was felt that a different approach would be more appropriate.

3.3.2 Ethnographic research approach

Ethnography studies the meanings of social interactions, values, behaviours, the language and perceptions which occur among members of an entire culture-sharing group. It involves long-term engagement in the field or setting in which the researcher "blends in" with the participants and further collects data by observing and conducting interviews (Creswell, 2013a). While there are many forms of ethnography, two forms will be discussed here: realist ethnography and virtual ethnography.

Realist ethnography is when the researcher reports the data impartially based on findings learned from the participants, which are free from personal biases, political goals or judgments (Creswell, 2013a). Another feature of this approach is its close attention to detail, regular sharing of experiences to demonstrate the researcher's experiences and its claim to authority (Marcus & Cushman, 1982). It is typically narrated in the third-person voice reporting based on observation.

Another type of ethnography is *virtual ethnography*. Virtual ethnography derives from the foundation of classical ethnography. As a newer development, it is also known as Internet ethnography from the development of the Internet as a medium for communication, interaction, and a socially-constructed space where people live more online (Markham, 2004). The researcher may analyse from web pages, chat rooms, daily lifestyles to emoticon symbols.

Although employing the virtual ethnography approach alone is not fit to answer the research problem, combining it with the realist ethnography approach extends its capabilities. Nonetheless, while this study seeks understanding of meanings from the online environment and their experiences, it does not intend to observe a participant's day-to-day activities.

3.3.3 Phenomenological research approach

Creswell (2009) defines phenomenology as "a research strategy of inquiry in which the researcher identifies the essence of human experiences about a phenomenon, as described by participants" (p. 13). Phenomenological research illuminates the lived experiences of several individuals as described by participants. It seeks to explore, describe, and analyse the essence of the experience for the specific phenomenon of interest from several participants who have had similar experiences (Creswell, 2013b). The purpose is to reduce the experiences to a description of the universal essence (van Manen, 1990). Moustakas (1994) stated "Phenomenology seeks meanings from appearances and arrives at essences through intuition and reflection on conscious acts of experience, leading to ideas, concepts judgments, and understandings" (p. 58). This approach has been recognised to be effective in identifying the deeper understanding of direct experiences and perceptions from an individual's perspective (Stan, 1999). Moreover, Lester (1999) claims that by combining it with interpretive dimensions, it can be used as a basis to assess or challenge a policy or an action.

However, phenomenology does not seek to understand why the phenomenon happens as its emphasis is on the experiences of participants (textural description) and how they experience it (structural description) (Creswell, 2013a). By focusing on the description of an experience, phenomenology may overlook what forms that experience and other factors associated with it. Similarly, this approach is not appropriate for understanding how the phenomenon leads to employees' personal information disclosure without actually observing the point of disclosure.

3.3.4 Case study research approach

Yin (2014) defined a case study as an empirical enquiry that examines a real-life contemporary phenomenon within its context and settings, particularly when there are no clear contextual boundaries. Thus with this definition, a case study fits well within the interpretivist paradigm in line with this research philosophical assumptions. Yin's definition puts forward the difference between a case study and other research methods such as experimental research, which separates the phenomenon from its context; historical research, which usually focuses on non-contemporary phenomenon; and survey research, which has limitations on contextual research (Yin, 2014). According to Creswell (2013a), case study research is a "qualitative approach where the investigator explores a real-life, contemporary bounded system (a case) or multiple bounded systems (cases) over time, through detailed, in-depth data collection involving multiple source of information" (p. 97). The strength of a case study is by employing multiple methods to obtain a stronger understanding of the problem and minimise the limitations of any single method being used by complementing the strength of the others. In particular, Baxter and Jack (2008) argue that a qualitative case study approach can employ quantitative data as a means to produce holistic understanding. Multiple sources of information are combined and integrated during the analysis process to answer certain aspects of the phenomenon, and eventually combine all sources of data which add to greater understanding. Nevertheless, they singled this as a unique characteristic of case study research.

In case study research, Yin (2014) reasoned that there are three main motives for choosing this approach: research questions with 'how' or 'why' questions; the researcher's inability to manipulate relevant behaviours; and contemporary as opposed to historical phenomenon as the subject of study.

This strategy is applicable for an in-depth understanding of complex phenomena using various data collection methods such as interviews, observation, documentations, surveys and focus groups. Thus, a case study can have diverse epistemological perspectives, which in turn incorporate different philosophical assumptions about the nature of knowledge, and require different approaches of inquiry (Yin, 2014). Hence, this research is drawn from Creswell's (2013a) views of case studies as one of the approaches in qualitative inquiry, and thus aligned with the underlying interpretivist paradigm as presented before this.

Different types of case study can exist. Yin (2014) describes it as exploratory, explanatory and descriptive, while others (Stake, 1995; Creswell, 2013a) categorise it as an instrumental case study, collective case study and intrinsic case study. Exploratory cases refer to investigating phenomenon that have no clear single set of outcomes, whereas an explanatory case study is when the researcher investigates a causal relationship. A descriptive case study is used to describe the phenomenon and its real-life context (Yin, 2014). In the same way, Stake (1995) categorises a case study according to reasons for conducting it. An instrumental case study is when the researcher explores a case in order to provide understanding and insights about an issue of interest. The 'case' facilitates understanding on other issues or concerns and may not be the primary interest as in an intrinsic case study. An intrinsic case study is when an issue or concern is of particular interest and the researcher has a genuine interest in the case. The purpose is to acquire a better understanding of the case in reference to all its uniqueness and commonality (Baxter & Jack, 2008) and not used for theory building. Finally, a collective case study selects multiple instrumental case studies to investigate an issue (Creswell, 2013a). Conversely, Stake (1995) also cautioned the researcher that studies seldom follow the categories neatly, because it depends on the researcher's capacity to decide on the research aims and the scope of the study.

Case studies are not without criticism. Case studies have often been criticised as lacking scientific rigour. Yin (2014) acknowledged this concern and assumed that it is due to the lack of existing methodological texts to guide researchers in case studies. There are several strategies that can be employed to address this concern, namely by implementing triangulation, respondent validation, scrutinising use of theoretical sampling and producing transparency of the research process (Crowe et.al., 2011). Another concern regarding a case study is that it provides little basis for scientific generalisation. This concern arises from the small number of case studies that were conducted on the basis of an individual case. Despite the commonly raised question "How can you generalise from a single case?", Yin (2014) explains that case studies can be generalised: "to theoretical populations" and not to general populations. In addition, case study research is able to facilitate expanding and generalising theories rather than extrapolating probabilities (Yin, 2014). Another strategy for generalisation is by employing multiple cases for case study research. Multiple cases should be selected according to replicate design and not as sampling logic. Thus, each case must be carefully chosen as to how the researcher predicts the results (either literal or theoretical replication). In this sense, when similar results replicate among the cases, the overall findings can be considered as achieving better generalisability (Yin, 2014).

For this research, it was decided to employ a case study research approach as the data collection method in order to understand the experience of public employees in a real world phenomenon i.e. obligatory disclosure and its relation to privacy. The inspiration is derived from the nature of the phenomenon under study (i.e. obligatory disclosure and privacy) which is considered a complex phenomenon and contextually influenced. As Yin (2014) argues, case study research offers a holistic and in-depth understanding of a contemporary phenomenon within its context.

Secondly, the research questions in this research were mostly composed of 'how' questions, with the aims being to not only identify types of personal information that were disclosed online but also uncover why and how employees perceived them in relations to their privacy. Hence, research that requires answers from 'how' and 'why' questions is appropriate with case study research (Yin, 2014; Benbasat et.al., 1987).

Thirdly, the flexibility of using multiple sources of data allows the investigation to employ more techniques in gathering diverse information and for providing richer information. This will allow analysing the perceptions and feelings of employees and at the same time observing the natural settings of the phenomenon (Yin, 2014).

Additionally, the phenomenon of obligatory disclosure is under studied and little is known about how it is perceived towards an individual’s privacy. Moreover, privacy has been agreed by many authors as a complex and complicated topic (Reips, 2010; Finn et.al., 2013). Thus, a phenomenon that has a limited theoretical base for research - such as privacy - seems to favour case study research to provide insights into an issue or for theory building (Benbasat et.al., 1987). However, this research was not focused on theory building but providing rich sources of data that can be used to refine or build new theories.

3.4 Case study

Whilst several qualitative approaches were considered, case study was selected for this research. Qualitative studies often encapsulate the philosophical assumptions which shape the research problem, research questions and answer to them within the chosen interpretive frameworks. A qualitative case study is appropriate for this research as it involves an interpretive and naturalist approach for investigating the phenomenon in natural settings and attempts to give meanings to it by the participants (Denzin & Lincoln, 2000). Since a case study seeks to understand the phenomenon within its context, it is pertinent to define the context of this study. Henceforth, the context of this study is the obligatory disclosure in public organisations website.

With a complex phenomenon, multiple methods for data collection - including qualitative and quantitative data - will be utilised. Nevertheless, this research was grounded within the interpretivist paradigm and influenced by naturalistic inquiry, although quantitative data was used. The purpose for quantitative data was only at the initial stage and served as a triangulation technique as shown in section 3.4.1.

In order to proceed with the selected approach, the unit of analysis (case) must be determined. Defining a case for the case study is not an easy task (Baxter & Jack, 2008). It is important too to identify the main case before proceeding with the data collection. Moreover, different researchers view the *case* differently. A case can be an event, a process, an individual, a group or an organisation (Yin, 2014). A clearer definition of a case is defined by Miles et.al. (2014) as: “a phenomenon of some sort occurring in a bounded context" (p. 21) which is the unit of analysis. It can range from the role of individuals, episodes or encounters, a culture, and to space and an environment. In order to determine what the case was for the study, the researcher revisited the research questions as suggested by Yin (2014). Based on that, this research selected two cases as the unit of analysis.

The first case is defined as *public employees' experiences over obligatory disclosure and its relation to their privacy*. Public employees in Malaysia who were in-service and their personal information was published on their organisation's website were of interest. However, to cover all public employees in Malaysia was time consuming and too large a scale. Therefore, only public employees within the administrative capital of Malaysia, i.e. Putrajaya, that consists of different working categories and from federal agencies, departments and ministries were studied. This case was the main case of this research.

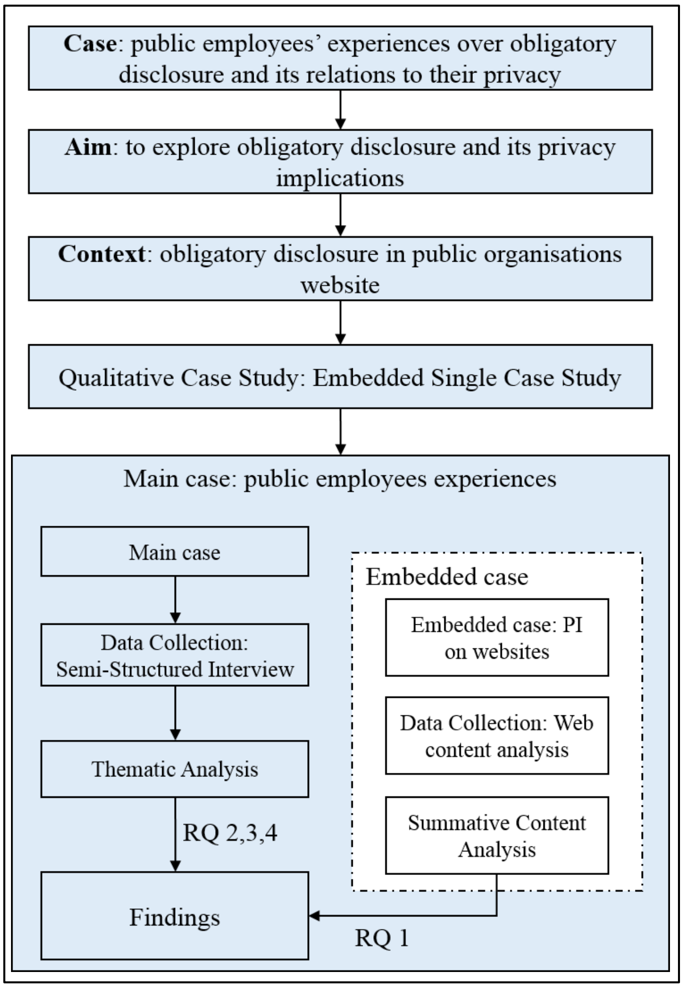

Case: public employees' experiences over obligatory disclosure and its relations to their privacy
Aim: to explore obligatory disclosure and its privacy implications
Context: obligatory disclosure in public organisations website
Qualitative Case Study: Embedded Single Case Study
Main case: public employees experiences
Main case
Data Collection: Semi-Structured Interview
Thematic Analysis
RQ 2,3,4
Findings
Embedded case
Embedded case: PI on websites
Data Collection: Web content analysis
Summative Content Analysis
RQ 1

Figure 3-1: Illustration of operational framework

The second case of interest is *personal information of public employees that is publicly available on public organisation's website*. Since the individuals were Malaysian public service employees, this case was bounded within the Malaysian official government's websites. Any types of personal information that belonged to an employee were selected as the unit of analysis. Figure 3-1 illustrates the operational framework of this study. This case was the embedded case in this study.

Case study research can either be conducted for a single case or multiple case study. Single case studies are appropriate to be selected when they fall within five circumstances (Yin, 2014). Firstly, when the case is a critical case i.e. critical to theory; therefore, a single case can be used to test the propositions. Secondly, an unusual case where a specific or unique case occurred and is worth investigating. Thirdly, a common case when the objective of the study is to examine the circumstances and situations of everyday phenomenon. Fourthly, a revelatory case is when a usually inaccessible phenomenon is available. Fifthly, a longitudinal case that studies the same case over a period of time. Accordingly, the decision to conduct a single case study should consider these five circumstances. Criticism of a single case study includes the issue of generalisability which mainly stems from the sampling process (Simons, 1996).

A multiple case study, on the other hand, is used to understand similarities and differences between cases with the potential for generalisability of findings (Patton, 2002). It is especially useful when the phenomenon is too complex or too many parties are involved. It provides a stronger analytic conclusions and a better foundation for theory building compared to a single case study (Yin, 2014).

On the contrary, Dyer and Wilkins (1991) contend the use of more cases as the researcher may lose the contextual insights of the case, which offer surface description instead of rich and thick description. In fact, multiple case studies require higher financial capabilities and a longer duration of study (Yin, 2014) which this doctoral study could not afford.

The decision to select single or multiple case studies must be related to how much information of the phenomenon is known, the nature of research questions, accessibility to the case, availability of resources and the research timeframe (Darke et.al., 1998; Yin, 2014; Walsham, 2006).

This research decided to conduct a single case study as it represents the 'common' case properties. This 'common' rationale fits well with the objective of this research which is to investigate obligatory disclosure. This phenomenon was found to be evident in many organisations' websites, as highlighted in the findings of the literature review. Furthermore, individuals who participated in this research experienced obligatory disclosure most of the time as the websites were publicly available online, i.e. 24 hours a day. In addition, a single case study places the importance of a rich description of data over the ability to compare cases (Dyer & Wilkins, 1991).

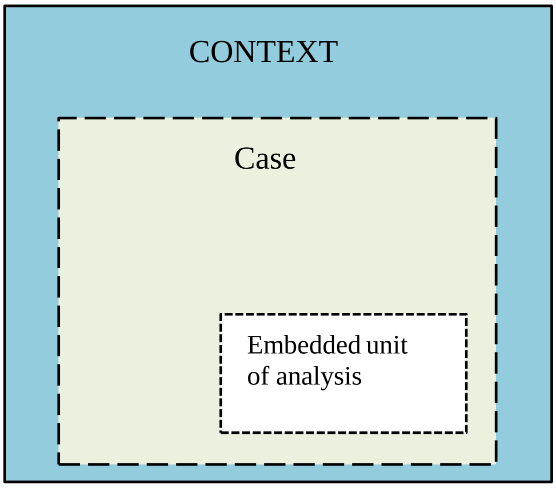


Figure 3-2: Single-case embedded design
Source: Adapted from Yin (2014)

This research also adopted the embedded single-case study design as shown in Figure 3-2. The decision was made to not use a holistic single case design because two units of analysis were used as explained above. Similarly, it was not suitable for multiple-case design as well because the embedded unit of analysis needed to be scrutinised within the larger case of interest. The embedded unit of analysis was the government employees' personal information publicly available on public organisation's website. The main case of interest was those employees' experiences of obligatory disclosure and its relation to their privacy. The opportunity to have an embedded unit within a larger case allows for determining the influence of it within the main case. In respect to this research, analysing the availability of personal information on an organisation's website enabled the researcher to gain insights of the real situation, and envision on the consequences that may arise (Yin, 2014). Also, information collected from this source can then be used for triangulation purposes. Moreover, the sub unit of analysis will assist in directing the research within its scope by minimising diversion from the intended investigation (Yin, 2014).

As mentioned earlier, the interpretivist believes that multiple realities are constructed through lived experiences and the meanings differ as well as being numerous. Thus, this type of research positions the importance of the participants' information on the researched phenomenon. Therefore, engaging in a discussion with participants will generate ideas and meanings of an investigated phenomenon. Realities are shaped by individual experiences and knowledge is gained through social constructions. Inductive methods are used to identify themes or patterns of ideas from the participants, such as interviewing or analysing texts (Lincoln et.al., 2011). Furthermore, the researchers position themselves to make their values known to the readers, so that they are aware of the researchers' own experiences and backgrounds when interpreting.

The primary data collection technique adopted in this study was an in-depth semi-structured interview, as a qualitative approach was best suited to explore this issue. This technique was complemented with web content analysis, to examine publicly available personal information of employees from government websites as they naturally and normally occur (Neuendorf, 2002). It, too, included published reports/documentary sources as a method to cross-validate information from participants. A semi-structured interview was deemed suitable since it enables flexibility and openness to participants' answers. Besides, the data collection for the embedded case utilised web content analysis to systematically analyse types of personal information (Krippendorff, 2013). The web content analysis method allows for unobtrusive investigation (Stemler, 2001), into manifest and lateral content on organisation websites (Hsieh & Shannon, 2005).

It was important to gain understanding of obligatory disclosure in real-life situations before proceeding with the government employees' experiences, in order to grasp the scope of the disclosure and get the entire picture of the phenomenon, (i.e. on the website), which would assist the researcher during the interview session. Moreover, as a requisite to address the experience of obligatory disclosure among government employees in light of how they felt about it and privacy implications towards them, semi-structured interviews were consequently conducted.

3.4.1 Web content analysis

This section describes the method employed to answer research question 1, which is concerned with the personal information of employees' that is publicly available on their organisation websites. The aim of this method was to be exploratory rather than hypothesis testing, which was to discover how and what types of employees' personal information were revealed on official government websites. By applying qualitative design in this study, the qualitative content analysis includes searching for underlying themes, (Bryman, 2012), for obligatory disclosure, besides identifying occurrences of personal information within public organisation websites. Content analysis, although being seen as a simplistic survey method, was in fact a systematic tool and widely used in various disciplines.

According to Holsti (1969), content analysis is "any technique for making inferences by objectively and systematically identifying specified characteristics of messages" (p. 14). Meanwhile, Krippendorff (2013) defines it as "a research technique for making replicable and valid inferences from texts (or other meaningful matter) to the context of their use" (p. 24). Henceforth, any types of information, whether texts, images, maps, audios, symbols or signs, can be included as data. Krippendorff (2013) further adds that content analysis consists of four distinctive features: a) it is unobtrusive, b) it has the ability to manage unstructured matter as data, c) it is context sensitive, and d) it has the ability to cope with large volumes of data. Its unobtrusive feature is very helpful in this research situation, by which the data of interest (i.e. personal information) on the websites is in its natural settings as seen by the public. There is no external intervention and as a result, data is not distorted or manipulated. Another characteristic of content analysis is the capability to manage unstructured data or content which is difficult to be tabulated or coded. It is also capable of analysing a large amount of data where thousands of data sources can be included in a single content analysis study.

This method was the primary tool used to review the content of web pages for the intended organisation websites. The technique of applying content analysis to the web began in 1995 (McMillan, 2000), where the majority of the studies were in the context of researching websites. This technique has also been widely applied in organisational website disclosure research to identify content available on organisations' websites (Ettredge et.al., 2001; Jose & Lee, 2007; Dutta & Bose, 2007). To illustrate, Ettredge et.al. (2001) highlighted financial information on 402 corporate websites, Jose and Lee (2007) examined environmental policies on 200 multinational companies' websites, whereas Dutta and Bose (2007) investigated corporate reporting on listed companies' websites in Bangladesh. Likewise in the tourism industry, content analysis was widely adopted to analyse hotel and tourism related websites (Hsieh, 2012; Baloglu & Pekcan, 2006; Wan, 2002).

It is worth noting that most research on government websites focused on assessment and functions (Huang, 2006; Zhou, 2004; Latif & Masrek, 2010) or website implementation (Kaaya, 2004; Parajuli, 2007). A recent study on United States Government websites discovered topics - transparency, security threats, public participation, crisis support and comparisons of how federal and business carried out their e-Government initiatives (Snead & Wright, 2014) - which were among the research focus. Despite interest in privacy and e-Government, no studies were found that systematically extract and categorise personal information specifically from public organisation websites.

To identify and assess the amount of personal information published on official websites including its types and depth of disclosure, this research employed web content analysis method to examine public organisation websites. This method's content of interest involved any publicly available information that could be used to distinguish or trace an individual's identity found on the websites.

Two types of data that are normally referred to in content analysis are manifest content and latent content. Manifest content is data that are "physically present and countable" (Gray & Densten, 1998). As an example, counting the number of occurrences of a specific word or content in a document. In contrast, latent content is the underlying meanings conveyed by the message that can be measured indirectly by one or more indicators (Neuendorf, 2002).

For the purpose of this study, content analysis focused on both manifest and latent content which were the occurrence of types of employees' personal information and the strategies of their disclosure.

Conducting content analysis on websites provides additional challenges due to its complexity (Neuendorf, 2002). Neuendorf (2002) cautioned that websites may have many forms of content, diversity in website designs, commercial activities performed on websites and sampling difficulties. Due to the complexity of web content analysis, a pilot study was considered for this research.

3.4.1.1 Pilot phase

A preliminary investigation was conducted on 17 public organisations' websites from seven countries -. England, Malaysia, Scotland, Singapore, South Korea, Australia and New Zealand - to gauge the disclosure of identifiable information with samples from ministerial and local level of administrations (Badrul et al., 2014). The aim of this preliminary study was to achieve the following:

a. Identify types of personal information that are accessible publicly.

b. Identify the source of disclosure.

c. Observe the pattern of disclosure across different countries.

d. Evaluate the coding process and technique.

e. Experience manual coding technique as a preparation for the main data collection phase.

f. Provide a basis for the main web content analysis sampling consideration.

The pilot study discovered that personal information of employees could easily be found on all public organisation websites, with full name and employment information being the most visible attributes (Badrul et al., 2014). Sections on the websites, where most of the personal information was discovered, were identified. This information could assist the researcher during the main content analysis, in which the coding process could therefore be intensified when coding these sections.

The pilot study allowed the researcher to familiarise with the procedure of web content analysis. It was also useful in testing the preliminary codebook and exploring the practice of obligatory disclosure internationally. Based on that, the codebook was revised and improved. For example, *'biography'* that was identified as one type of personal information, was reviewed since it could be recoded and divided into several different types of personal information (e.g. age and gender).

Based on the findings, this research decided to focus on Malaysian Government websites as the basis for sampling decisions. This is because the disclosure of employees' personal information from Malaysian websites was noticeably higher than other countries. It could be due to the availability of staff directory features on all Malaysian websites, and an internal search engine functionality that is specifically for searching an employee. With the availability of a staff directory, exposure of staff was considerably higher compared to other countries. Thus, the possibility of finding participants who had experienced obligatory disclosure would be much higher when the websites included staff directory feature. Moreover, with the higher disclosure of personal information, a rich description of obligatory disclosure and privacy was anticipated.

3.4.1.2 Unit of analysis

According to Neuendorf (2002), a unit of analysis is the element of which data is analysed and reported. The unit of analysis in this study was the web pages that contained employees' personal information in written text and images on their organisation's websites. Files that were embedded or hosted on their website, such as annual reports and newsletters, were included in the study. Most of the websites had a dual language option with either a Malay language version (which is the official language of Malaysia) or an English version. In addition, some websites embedded a translating function to assist users with other language capabilities. To maintain consistency, only web pages in the Malay language were selected for this study since it is the official language of Malaysia. Personal information of employees from political appointments and any links to third party websites were excluded since it is outside the scope of this study.

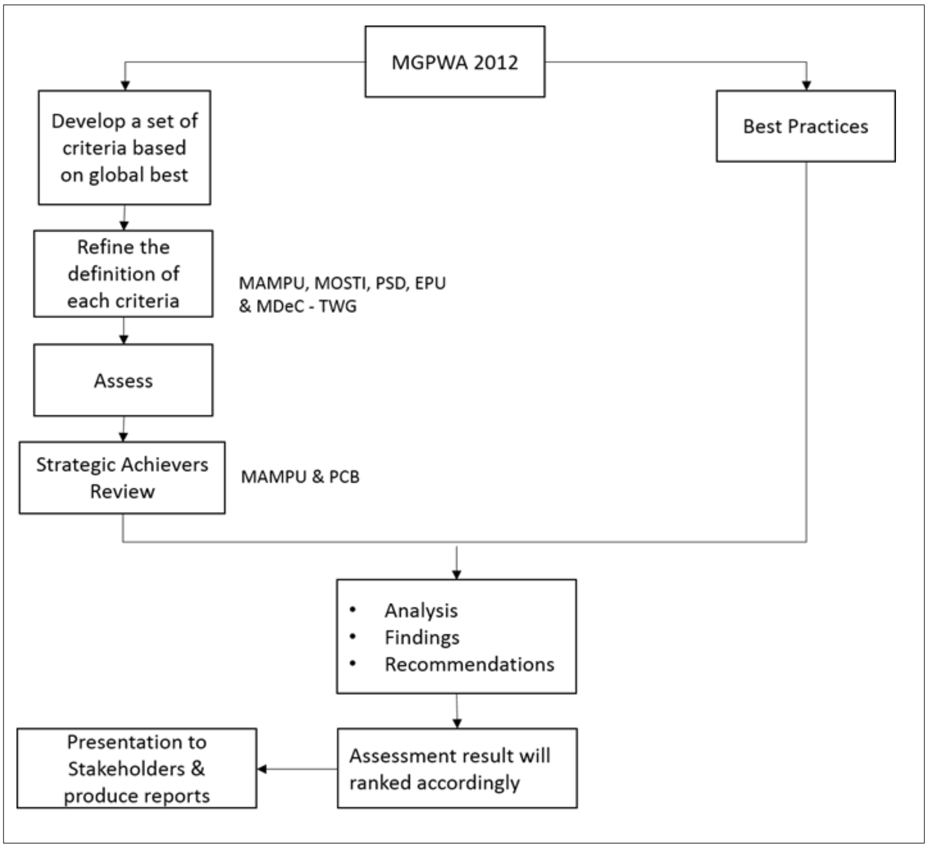
Neuendorf (2002) argues that the nature of the medium, and particular variables that are relevant to the study, should be considered when identifying this type of variables. Furthermore, when a characteristic is specific to a given medium then it should definitely be included in the study as long as its unique characteristics are significant within the research context. The prospect of specific websites' characteristics that facilitate the disclosure of employee's personal information should not be ignored and are included in the analysis.

3.4.1.3 Website selection

For the web content analysis, six federal agencies and ministerial websites, six state Government websites and six local authority websites were selected as samples to represent the Malaysian Government agencies. The top six websites which were selected from each category were assessed by the annual MGPWA for the year 2012 (Multimedia Development Corporation, 2012) and achieved five stars. MGPWA assessment was carried out to evaluate the websites of government agencies in providing better service and information delivery through the Internet (Figure 3-3). It is the only assessment that is currently implemented to evaluate public organisations' websites in Malaysia. In 2012, a total of 1,349 portals and websites were assessed, and the results were tabulated and ranked accordingly. Out of this, 182 websites were from the ministry and federal agencies, state Government and local Government websites. The websites selected as samples formed 9.9% of the total population.

MGPWA criteria were developed and agreed upon by a Technical Working Group (TWG), composed of five different key agencies which are: Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) as the lead agency, Ministry of Science, Technology and Innovation (MOSTI), Economic Planning Unit (EPU), and Public Service Department (PSD) and Multimedia Development Corporation (MDeC), who also act as the secretariat. The criteria largely adopts a few international approaches of assessment, with some adaptation to the local environment and capabilities (Haidar & Abu Bakar, 2012). In ensuring the standards and criteria meet global requirements, two international standards were employed as a benchmark, i.e. *United Nations E-Government Survey 2012: E-Government for the People* (Department of Economic and

Social Affairs, 2012) and *The 2012 Waseda University International e-Government ranking* (Waseda University, 2012).



MGPWA 2012
Develop a set of criteria based on global best
Best Practices
Refine the definition of each criteria
MAMPU, MOSTI, PSD, EPU & MDeC - TWG
Assess
Strategic Achievers Review
MAMPU & PCB
• Analysis
• Findings
• Recommendations
Assessment result will ranked accordingly
Presentation to Stakeholders & produce reports

Figure 3-3: MGPWA assessment structure
Source: Adapted from (Multimedia Development Corporation, 2012)

The portals and websites were evaluated based on usability, content, services, participation and security. *Usability*, which had the largest allocation of marks, focused on users' experience, followed by *content* that examined the information offered to the users. *Services*, which consisted of online services, online responses and online searchable database carried 15 marks, and was the third main factor. *Participation* focused on feedbacks/comments and Web 2.0 functions and finally, *security*, with five marks, considered security, privacy policy and single sign-on functionality. In addition, portals were allocated additional 10 marks for offering an e-payment service and displaying digital accreditation marks. The distribution of marks is presented in Table 3-1.

Table 3-1: MGPWA Portal and Website Score Allocation for 2012
Source: Adapted from Multimedia Development Corporation (2012)

Pillar	Score	
	Website	Portal
Content	25	25
Usability	45	45
Security	5	5
Participation	10	10
Services	15	15
Bonus	-	10
TOTAL	**100**	**110**

By selecting the websites and portals from the MGPWA report, it is almost certain that the websites are genuine, fully-functional, accessible, and demonstrated the high quality expected of government websites. Thus, the authenticity and credibility of the selected websites were addressed. In order to evaluate websites that meet the quality standards of the Government, only top six websites from three categories were selected. The categories that were selected were from ministry/central agencies, state and local Government. Websites from universities were excluded to focus on categories that constituted the general component of a government. Thus, these websites may represent the highest standards among all the websites of Malaysian Government agencies, which could also reflect the expectations of Malaysian Government agencies towards their websites.

The number of websites was limited in order for it to be scrutinised in great detail, since this research coded each page of the websites. Furthermore, the content analysis was conducted manually with limited resources by coding websites, which was a time-consuming process (Ha & James, 1998). For the purpose of this study, the website terminology was chosen to represent both websites and portals, and both were included as samples.

3.4.1.4 Data analysis procedure

In general, there are seven phases of content analysis procedure (Williams van Rooij & Lemp, 2010; Zhang & Wildemuth, 2009). The phases are presented in Figure 3-4. The first step in content analysis is to define the unit of analysis. Unit of analysis can be a unit of text or individual themes. Next, the categories and coding scheme were developed based on the data, literature reviews, and theories. A coding manual or codebook is recommended to ensure consistency. The coding scheme need to be tested on a sample of text for consistency and validity. After sufficient coding consistency is achieved, the entire set of data is coded. The coded data is checked for coding consistency. This is to assess the consistency of the coders, moreover when using multiple coders. Having satisfied with the consistency, the data is analysed and interpreted. Finally, the findings are reported including the decisions and practices during the coding process.

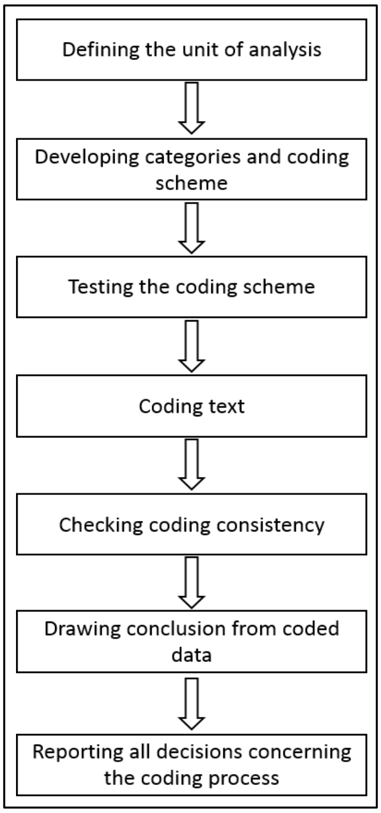

Defining the unit of analysis
Developing categories and coding scheme
Testing the coding scheme
Coding text
Checking coding consistency
Drawing conclusion from coded data
Reporting all decisions concerning the coding process

Figure 3-4: General phase of content analysis
Source: Adapted from Williams van Rooij and Lemp (2010); Zhang and Wildemuth (2009)

This research adopts a summative approach to qualitative content analysis (Hsieh & Shannon, 2005) for analysing employees' personal information disclosure on government websites. A summative content analysis approach starts with manifesting content analysis which employs Neuendorf's (2002) approach and further includes latent content analysis for interpretation of the content (Holsti, 1969). It offers an unobtrusive technique to study the phenomenon in its natural setting, and understands the underlying contexts of its content (Hsieh & Shannon, 2005; Babbie, 2010). Thus, this approach is appropriate for discovering the underlying meanings of the content, based on research question 1 from section 1.4 which is:

How does obligatory disclosure result in employees' personal information disclosure?

To answer this research question, identifying and enumerating the occurrences of personal information only is not sufficient, because it will only address the manifested content of data. In order to address the possible explanation of obligatory disclosure on government websites, the content analysis must move beyond the counting of occurrences. The summative approach strategy is not only involved in quantifying occurrences of personal information, but also attempts to interpret the meaning by examining the disclosure associated with certain features of websites. Analysing the manifested content allows this study to determine the presence of information and the extent of disclosure, while the latent content will attempt to interpret the disclosure.

Thus, the analysis of the manifested content is guided by Neuendorf's (2002) approach. According to Neuendorf (2002), there are four approaches to quantitative content analysis: a) descriptive content analysis, b) inferential content analysis, c) psychometric content analysis and d) predictive content analysis. This research applies descriptive content analysis with frequency analysis technique in gathering the amount of personal information that appeared on the websites. In other words, this is also known as calculating the occurrence of certain categories based on the coding rules. This technique usually leads to a disclosure index (Beattie et al., 2004), which is a numerical indicator that quantifies the information disclosed with the aim of displaying the level of disclosure of a specific piece of information. In other words, disclosure index assumes that the quality of disclosure is commensurate with the disclosure quality (Beattie et al., 2004).

In disclosure index studies, there are three characteristics of indices that are normally applied in the content analysis method. The first is a binary or ordinal measurement of items, the second is by using the weighted or unweighted index and thirdly is whether it is a nested or unnested items (i.e. grouping of items into hierarchical categories) (Beattie et al., 2004).

This study will assess the disclosure of personal information by using three ordinal schemes, also known as serials schemes, as this approach was adopted by researchers to assess the quality of disclosure (Botosan, 1997; Beattie et al., 2004; Gallego-Álvarez et al., 2011). A disclosure index with the value of '1' is coded if the information is partially disclosed by the organisation and '0' when no information is found. A further value of '2' is assigned if the information is disclosed completely (Gallego-Álvarez et al., 2011). Table 3-2 presents the grading index adopted in this study.

Table 3-2: Grading index for the disclosure of personal information

Grading scale value	Types of disclosure
0	Non-disclosure
1	Partial disclosure
2	Full disclosure

When assigning this type of value, it should be interpreted with caution. This is because the distances between values can only be assumed. Intermediate distances are not known and as a reason it is not exact (Gatfield et al., 1999). Thus in this study, the higher scores will suggest a higher amount of disclosure and lower score means less disclosure. While this index could be seen as employing some subjective assessment, coders were given precise coding guidelines in order to minimise subjectivity (Evans & King, 1999). Thus, the coding guidelines are very important in ensuring that the coding process is conducted according to what has transpired from the website.

To evaluate the specific website characteristics, a binary measurement scheme was employed instead of ordinal schema. A value of '1' is recorded when the information was found and '0' when there was no information available. When a value of '1' was recorded, if required, coders identified the relevant phrases or words that address the researched issue. After exploring the occurrence of the specific website characteristics, it is followed by searching for the underlying meanings in the materials based on the availability of the features (Hsieh & Shannon, 2005).

Table 3-3: Grading index for specific website characteristics

Grading scale value	Disclosure
0	Not available
1	Available

Table 3-3 illustrated the grading index for analysing the specific website characteristics. Next, the process of developing codes and categories were conducted and discussed in chapter four.

3.4.2 Interview

Interviews provide in-depth information pertaining to participants' experience and viewpoints of a particular topic. The focus of the interview is to develop understanding and interpretation of participants and situations. It is employed as the central method for exploring "data on understandings, opinions, what people remember doing, attitudes, feelings, and the like, that people have in common" (Arksey & Knight, 1999; p. 2).

There are generally three categories of interviews according to Patton (2002):

a. the informal conversational interview,

b. the interview guide or topical approach, and

c. the standardised open-ended interview.

Meanwhile, Rossman and Rallis (2011) added another category i.e.

d. the co-constructed, or the dialog interview.

While the informal conversational interview is more casual, spontaneous and impromptu, the interview guide or topical approach is more structured, with lists of topics or questions. However, it lets the participants unfold their views and express them using their own words. Standardised open interview, also called structured interview, has a strict approach in asking specific questions in a specific sequence. This type of interview is useful in a multi-site study with multiple interviewers. The co-constructed or the dialogic interview emphasises both interview and interviewee generating new meaning together.

As this topic is exploratory and rather complex in nature, it is appropriate to employ the interview guide or topical approach. This approach is also known as the semi-structured interview. In a semi-structured interview, the interviewer is not tied to following a pre-set script in asking each interviewee the same closed questions using similar words in each interview. It is more flexible, in the sense that it allows the interviewer to include additional questions in response to participants' comments and reactions. Although the interviewer relies on an interview protocol, sometimes acting freely on the basis of certain research points whenever appropriate is permissible. The questions moved gradually from general to the specific, with the interviewer probes discussions and follows ideas (Savin-Baden & Major, 2013). In contrast, interviewees have the opportunity to express their opinion openly about the investigated topics. This technique caters to the fact of diverse interpretation towards obligatory disclosure and meanings of information privacy to public employees.

The semi-structured interview was administered as a face-to-face interview rather than telephone or Internet interviews. This technique allows for direct contact between the interviewer and the interviewee, the opportunity to observe non-verbal behaviour and flexibility to meet diverse situations (Sarantakos, 2013). Moreover, since the sample of this study were government employees and they were normally occupied during office hours, this technique ought to offer a higher response rate and produce data quickly.

Turner (2010) presents general practical approaches and suggestions in conducting in-depth qualitative interviews to researchers. He stresses the importance of the preparation stage which may result in either a successful or failure of the process. He lists selecting participants and pilot testing as two important elements in the interview preparation.

However, interviews also have their limitations. Three main limitations of interviews have been disputed by critics. Firstly, on the reliability issue, where questions arise around whether interviews would yield the same result with the same respondents if they are asked repeatedly. Secondly, interview results cannot be generalised if the sample is not random and only a small number of interviews are conducted. Furthermore, the respondents can have anomalous views or experiences that are not normatively representative. Thirdly, in some cases, interviewees may be unwilling to share all the interviewer hopes to explore (Sarantakos, 2013).

Interview is a suitable method for the study of privacy because of the complexity of the topic itself. Therefore, a flexible and interactive approach facilitates in producing rich information from the participants. Privacy researchers have used interviews as the method to study privacy perceptions in specific contexts (e.g. Tu, 2002), personal information disclosure attitudes and behaviours (e.g. Olivero & Lunt, 2004; Razavi & Iverson, 2006) and privacy perceptions in organisations (e.g. Stanton, 2003; Smith, 1993; Stone et.al., 1983).

3.4.2.1 Pilot interview

Before performing the pilot study, one pre-pilot interview session was conducted to test and evaluate the draft of the interview protocol. This is the first step to familiarise the researcher with the interview process and identify room for improvements. Jacob and Furgerson (2012) suggested practicing the interview with friends before conducting the main interview, so as to assess the interview protocol. However, this study decided to conduct a pre-pilot interview since there was limited sample for the pilot study. The interview was finally conducted on the 21st of March, 2014 after three postponements. A participant who is a Malaysian lecturer currently pursuing Ph.D. at the University of Reading was selected. The participant was selected as she closely resembles the requirement of this study since she is a government employee (i.e. lecturer) in a public university. The interview session was audio recorded with the participant’s consent and lasted for 45 minutes. An interview protocol was prepared to guide the researcher during this process. It was constructed based on initial literature reviews.

During this pre-pilot interview, the researcher did a few interruptions while waiting for the interviewee to answer the question. The eagerness in waiting for an answer made the researcher provide answers to the participant. This caused the participant to use the researcher's wording for explaining and not their own words. Thus, the intended meaning from the participant might not be clear. The researcher was also observed asking new questions, without waiting for the participant to finish her answers. The researcher realised that this should be improved during the pilot interview. The participants should be allowed to express what they have to say and the researcher should improve on the listening skill to capture participants' views (Jacob & Furgerson, 2012). Besides that, several questions had to be revised as not to lead the participant when responding. Also, this session provided the opportunity to test the recording device and anticipated the duration of the interview. Based on the pre-pilot interview, the interview protocol was revised and the researcher was more aware of procedural ethics and techniques for interviewing, as suggested by Jacob and Furgerson (2012). This session not only assists the researcher greatly in gaining confidence but also acts as a practice session for the pilot interview.

The purpose of this pilot interview is to bring the issue into context, as it helps identify any practical problems in following the research procedure - since the enquiry can cover both substantive and methodological issues. It is also useful for testing the quality of an interview protocol and identifying potential researcher biases (van Teijlingen & Hundley, 2001).

Creswell (2007) stresses the importance of obtaining qualified candidates who will provide the most credible information to the study. For this pilot study, participants were selected through purposive convenience sampling, from government officials that are currently pursuing their postgraduate studies in the United Kingdom. As their characteristics were similar to the main study of this research in which they had experienced obligatory disclosure, those participants were deemed suitable for the pilot study (Turner, 2010).

Although the participants are currently under study leave, they are technically still government employees. In addition, most of them have more than five years' experience serving the government. However, the researcher managed to include one participant that is currently working with the Government. Twelve participants from Reading, London and Sheffield were initially identified and seven were recruited for the interview. Details of the participants and their interviews are shown in Table 3-4.

Each interview was conducted in the Malay language, since it is the official language of the country and widely used in public organisations in Malaysia. Furthermore, the participants and the researcher were also more comfortable in engaging in the interview session using this language. A demographic form was given to the participants before the interview started. The interview was audio recorded using a Samsung Galaxy Note 2 smartphone. The transcription process began after all of the seven interviews were completed. The interviews were transcribed by the researcher and coded using QSR Nvivo version 10 software.

Table 3-4: Pilot study of participant interviews

Participants	Date	Duration	Location
001	25 April 2014	56.41 min	Reading (Study room)
002	3 May 2014	45.47 min	London (House)
003	3 May 2014	45.50 min	London (House)
004	3 May 2014	38.49 min	London (Café)
005	3 May 2014	34.48 min	London (Café)
006	11 May 2014	39.44 min	London (House)
007	11 May 2014	31.12 min	London (Café)

Based on the pilot interviews, the researcher learnt that choosing the interview location is imperative to minimise noise and distraction. Three interviews were conducted in cafés and as a result, noises from the surroundings were clearly heard in the audio recordings. Moreover, one interview had to be relocated as the café was closing.

Although the pilot interview participants did not resemble the full characteristics of the main participants, they provided useful feedback for improving the interview questions. Some interview questions were revised based on the participants' responses, which might have some clarity issues. While questions were asked in the Malay language, some participants preferred to combine this with some English terms in order to increase their understanding of the questions. Similarly, at times participants seemed comfortable with expressing their views in English when they could not find the right Malay words.

The researcher also noted from this pilot study that the participants were willing to share more of their thoughts when the researcher listened attentively and showed interest in their views rather than taking notes. In addition, maintaining a good rapport with the participants and gaining trust were pertinent in producing more data.

The pilot study allowed the researcher to gain some insights into how participants viewed the obligatory disclosure. Participants' awareness of obligatory disclosure was generally high. Most of the participants considered the disclosure as an important strategy for public service and, therefore, were not paying too much attention towards their privacy needs. With respect to their privacy behaviours on social media, almost all participants had configured their privacy settings to private. However, these findings were not exhaustive as they were not analysed further. Nonetheless, they provided the researcher with initial observations and some "intriguing patterns" (Marshall & Rossman, 2011, p. 96).

3.4.3 Documentation

In qualitative research, a document review can be used to confirm and enhance evidence from other sources and it is relevant to case study research (Yin, 2014). In this research, documentation was adopted as a secondary source of evidence as it was not initially selected as a data collection method. However, as the research progressed, it became important to refer to published reports, such as the MGPWA report regarding their evaluation methodology and the official circulars from the Malaysian Government website management prompting for a documentation review. It must be noted that the use of documentation is only for the specific reference that is relevant to the privacy topic. The purpose of reviewing these documents was to gain insight into the commitment of the organisation and as a method of triangulation. In fact, analysing public documents is good practice in qualitative research (Creswell, 2013a).

3.4.4 Data collection

3.4.4.1 Sampling and recruitment

The units for analysis in this study were government employees in the Malaysian Federal Public Service (MFPS). The researcher, being a government employee himself, was aware of the size and geographical properties of the MFPS. Thus, the researcher decided on a reasonable size of population and at the same time worked within the limited resources that were available to identify the participants (Berg, 2007). Participants were selected via a purposive sampling strategy. This strategy is a non-probability sampling strategy based on purpose, and it was used to sample participants who had experienced obligatory disclosure. Purposefully selecting sites and participants is advantageous in gaining an understanding of the phenomenon for qualitative researchers (Creswell, 2013b).

In this study, purposive sampling strategy with maximum variation sampling technique was employed to identify and describe common themes and patterns from a small number of samples with diverse participants' characteristics (Patton, 2002). The purpose of employing maximum variation technique is to cover a diverse and wider array of interviewees' characteristics in order to provide greater generalisability of the research findings, compared to the homogenous type of sampling. Hence, the importance of including specific characteristics of the participants called for applying purposive sampling for this study (Williamson, 2002).

Before identifying potential participants, the researcher developed a characteristic matrix to assist in selecting participants with appropriate characteristics. The researcher was careful in trying to avoid recruiting two or more participants with similar characteristics in order to reach as diverse participants as possible. To maximise sample variation, each participant in the sample was selected to be as different as possible from others in criteria such as working group category, working experience, gender, working grade, age group, ethnicity, and education level. These criteria were found to influence individuals on their privacy beliefs and perceptions. Therefore, in order to ensure richness of data and that all groups were represented, purposive sampling with maximum variation strategy was applied.

The researcher had to obtain approval from the Malaysian Government and his sponsor to conduct data collection in Malaysia prior to the data collection phase. After obtaining necessary approval for data collection which was granted for two months, the data collection phase started in August 2014. Interviews were conducted from 20th of August 2014 to 19th of October 2014. The specified time frame for data collection (i.e. eight weeks), and difficulties in getting participants' agreement to participate, were among the challenges faced during this process.

There are three category of interviewees in this study, namely participants, IT stakeholders and commentators:

- Participants - Government employees from different working group categories (Top Management, Professional & Management, Support)
- Government IT stakeholders - key agencies that were involved in the policy of public organisation's website and website evaluation.
- Commentators – individuals who were identified as having insights into the subject of this study such as academics.

Participants were identified from the federal agencies located in Putrajaya, either at the Ministries or Department level. Participants must possess three main criteria, which are: must be currently in service, participants' organisations have a web presence, and participants must be working in the administrative capital of Malaysia, Putrajaya. It is vital that participants' organisations have official websites because it is one of the features of obligatory disclosure. However, being that Malaysia is a country that is actively promoting e-Government initiatives, most agencies are well represented online. Participants were identified from various different organisations, such as ministries, federal departments and central agencies. In addition, Government IT stakeholders and experts from two universities were recruited as commentators.

Initially, participants were contacted through direct approach, e-mails and telephone. A brief description of the study was specified to them. During the earlier stages, selection of participants was relatively simple in meeting the sampling criteria, but then became more difficult. Since specific characteristics were required from the participants, the researcher decided to utilise his 'special networking contacts' as a government employee.

The researcher made use of his network of colleagues and friends within the government circle to assist in finding appropriate participants. Selected characteristics of participants were described in detail to the researcher's networking contacts, and the researcher was then directed to potential participants. This saved a lot of time, by identifying potential participants who met the requirements in advance compared to searching via the normal public channels (i.e. direct to the organisations). As the interview progressed, the recruitment of participants became more targeted to meet the maximum variation technique. Thus, this strategy was found to assist the researcher in obtaining wider accessibility to the locations of potential participants. In addition, fewer participants who did not meet the criteria were turned down and the risk of cancelling appointments was minimised. Nevertheless, getting participants to agree to be interviewed was not an easy task. Even more so if the participant was a senior officer from government agencies, where an appropriate approach had to be considered.

Sample size in qualitative studies is normally less than in quantitative. If too large a sample is recruited, data will be difficult to analyse and manage. The size of the sample depends on the aims of the study, the types of data collection and available resources (Ritchie, 2003). Therefore, this study was based on the idea of saturation, introduced by Glaser and Strauss (1967), as the guiding principle during the data collection process. In grounded theory (see section 3.3.1), a comparative analysis of empirical data is conducted to identify similarities and differences that emerges from the data. The concept of saturation refers to a stage when the data does not shed any new information on the issue under investigation. In deciding for achieving saturation, this research was based on Strauss and Corbin's (1998) suggestion that 'the new' information does not merely mean new because potentiality for emerging data is always there. Instead, it refers to 'the new' data emerging which do not contribute to the overall story, model, theory or framework.

From a total of 40 identified potential participants who were government employees, 25 participants were contacted. Six people refused to participate. After interviewing 19 of them, it was felt that the information was largely repetitive and no new insights were identified. Interview data was constantly referred to during the data collection phase as participants' ideas and expressions were noted in memos/jottings. Jotting assisted in refining and keeping track of ideas that developed. It was noticed that the information gathered was largely repetitive after interviewing 17 participants, indicating that saturation is emerging. As a result, the interviews were stopped at 19 participants when no new data emerged from the participants.

Five commentators were contacted and three agreed to participate in the research. They were academicians from public universities in Malaysia. The commentators were selected to represent their area of expertise, represent views from the Malaysian context and their perspective of the investigated phenomenon. Interview sessions with them were conducted near the end of the data collection. The reason for this is that information gathered from participants would serve as the points of discussion during the session with commentators.

Similarly, the interviews with IT stakeholders were conducted after completing interviewing the participants. MDeC commentators were contacted through a researcher's friend currently working in MDeC. He assisted the researcher in identifying the correct division and officer handling MGPWA. Meanwhile, MAMPU commentators were contacted by email and the researcher was directed to the officer in-charge after a few e-mail exchanges. Two employees, each representing both MDeC and MAMPU, were interviewed. Both agencies are directly involved with the yearly assessment of Malaysian Government websites while MAMPU is the public sector IT stakeholder which oversees all IT developments in the public sector. Overall, 24 interviewees were interviewed in this research.

3.4.4.2 Interview procedures

After making initial contact with participants, an interview date and time was scheduled. The researcher had to be aware of the possibility that participants might reschedule or postpone the interview. Therefore, a dedicated appointment calendar was devised. To minimise the impact of postponing, the researcher had allocated one participant for each session (i.e. either morning or afternoon session). By doing this, each participant's time slot was allocated for four hours by taking into consideration that the interview session was one hour with three hours' buffer for any last minute changes. As such, Savin-Baden and Major (2013) cautioned of having more than two interviews scheduled per day due to tiredness, which will result in making mistakes. For participants who had a higher risk of rescheduling (e.g. top management), the researcher allocated one whole day to this category in order to minimise the risk of rescheduling to a new date.

Most of the interviews were conducted within the participants' office premises, while three participants chose to attend the interviews outside of their office compound but nearby. The choice of location for these three participants was decided based on mutual agreement. Hence, a nearby restaurant that is less crowded was chosen. The researcher was careful in selecting the interview location, based on prior experience from the pilot interview phase where background noises affected the quality of audio. This would cause distractions during the interview session and further create difficulties during the transcribing phase. Furthermore, since all participants are currently working, it was convenient for the participants if the interview was conducted in or near their offices. The accessibility and convenience factors are important when deciding on the location for data collection (Savin-Baden & Major, 2013).

Before the interviews took place, the researcher built up confidence and rapport with the participants by engaging in casual conversations such as current issues, weather and the civil service. A more relaxed participant will result in more productive and richer data during the interview (Kvale & Brinkmann, 2009). Then, the participants were informed about the details of the study and shown the research information sheet (Appendix B). Participants were asked to read it and enquired if there were any questions. If they agreed to participate, the consent form (Appendix C) and demographic form (Appendix D) were handed to them. Participants were informed that the interview was audio recorded and they may withdraw from participating at any time because the participation was voluntary. A participant decided to opt out after reading the consent form only in one instance, while others agreed to participate. The list of interviewees is presented in Table 3-5.

Once the informed consent was sought, the researcher began interviewing. All interviews were audio recorded. Recorded interviews provide rich descriptions and capture the actual words, which assists in providing actual quotes to support data analysis (Patton, 2002). Two Samsung Galaxy Note smartphones were used to record the interviews. The decision to use two different devices was made to ensure that the data was safely recorded and might serve as a backup if either one of the devices failed to record. Both devices were placed on the table between the participants and the researcher. Since the recorders were within easy reach of the participants, they were able to reach the audio recorder and stop the recording whenever they felt uncomfortable. This strategy was designed to make participants feel more comfortable because they had control over the audio recorders, and at the same time improve audio quality.

Table 3-5: List of interviewees

No	Participant	Gender	Date	Duration (min:sec)
1	001	M	20 August 2014	39:07
2	002	F	22 August 2014	37:32
3	003	M	25 August 2014	25:20
4	004	F	29 August 2014	34:07
5	005	M	5 September 2014	33:36
6	006	F	9 September 2014	34:54
7	007	M	10 September 2014	35:40
8	008	M	14 September 2014	1:01:35
9	009	M	15 September 2014	47:34
10	010	F	19 September 2014	52:35
11	011	F	24 September 2014	35:19
12	012	F	24 September 2014	26:37
13	013	M	26 September 2014	39:57
14	014	F	26 September 2014	44:38
15	015	M	26 September 2014	23:37
16	016	M	1 October 2014	58:11
17	017	M	3 October 2014	32:20
18	018	M	9 October 2014	59:28
19	019*	M	10 October 2014	42:04
20	020	F	14 October 2014	36:45
21	021*	F	15 October 2014	21:31
22	022*	F	16 October 2014	27:30
23	023*	F	16 October 2014	35:30
24	024*	F	19 October 2014	14:54

*(*inclusive of 3 commentators and 2 IT stakeholders)*

Participants were interviewed individually and face-to-face. Face-to-face interviews enabled the researcher to gather verbal and non-verbal responses from the participants. Participants' expressions, tone of voice and body language were clearly visible to the researcher, and this could have implications on the meanings conveyed by them. Notes were taken by the researcher when important points stated by the participants were identified. The points were then used as a reminder to seek further explanation from the participants. The participants' reaction and expression were also recorded in the notes.

The interviews were conducted in Malay, which is the official language of Malaysia and the Malaysian Government. Since Malay functions as the main medium of government communication, it became the language of choice for the interviews.

On average, the interviews lasted approximately 40 minutes, which was within the time frame agreed in advance (40 to 50 minutes) with the participants. However, some participants were willing to spend more time in this study and continue with the interview session.

Table 3-6: Participants agencies

No.	Agency
1.	Ministry of Finance (2 participants)
2.	Manpower Department
3.	Department of Skills Development (3 participants)
4.	Public Service Department
5.	Ministry of Human Resources (3 participants)
6.	Department of Personal Data Protection
7.	Ministry of Natural Resources and Environment (2 participants)
8.	Department of Islamic Development Malaysia
9.	Ministry of Communication and Multimedia
10.	Department of Director General of Lands and Mines
11.	Department of Safety and Health
12.	National Registration Department
13.	National Housing Department

Participants were selected from various agencies listed in Table 3-6 to enrich the diversity of the sample. However, since selecting different agencies was insufficient, henceforth, as stated earlier, the researcher also included other characteristics in the selection criteria.

Upon completion, participants were thanked once again for their participation and a small token of appreciation was handed to them in accordance with the ethical approval. The researcher jotted down some thoughts and impressions of the participants**.**

3.4.4.3 Materials

Interview questions are important because they aim to elicit responses from the participants. Therefore, the research literature guides the construction of interview questions by developing questions that focus on answering research questions (Jacob & Furgerson, 2012). Additionally, wordings of the questions have to be carefully constructed to not lead the participants. Generally, qualitative questions must at least "be open-ended, neutral, singular, and clear" (Patton, 2002, p. 353).

As mentioned previously, this study employed in-depth semi-structured interviews. This type of interview is flexibly worded and the researcher may include additional probes or questions depending on participants' responses. As a result, open-ended interview questions were constructed so as to ensure the participants answered what they thought and used whatever words they want to express.

Interview questions were prepared as a guide for the researcher during the interview session. The pilot study assisted in preparing the interview protocol, considering this was the major data collection method for this study. For data collection in Malaysia, four sets of interview questions were developed for three different categories of participants: (1) government employees; (2) commentators; (3) IT stakeholders for public sector IT development; and (4) IT stakeholders for website assessment. The list of interview questions is provided in Appendix E.

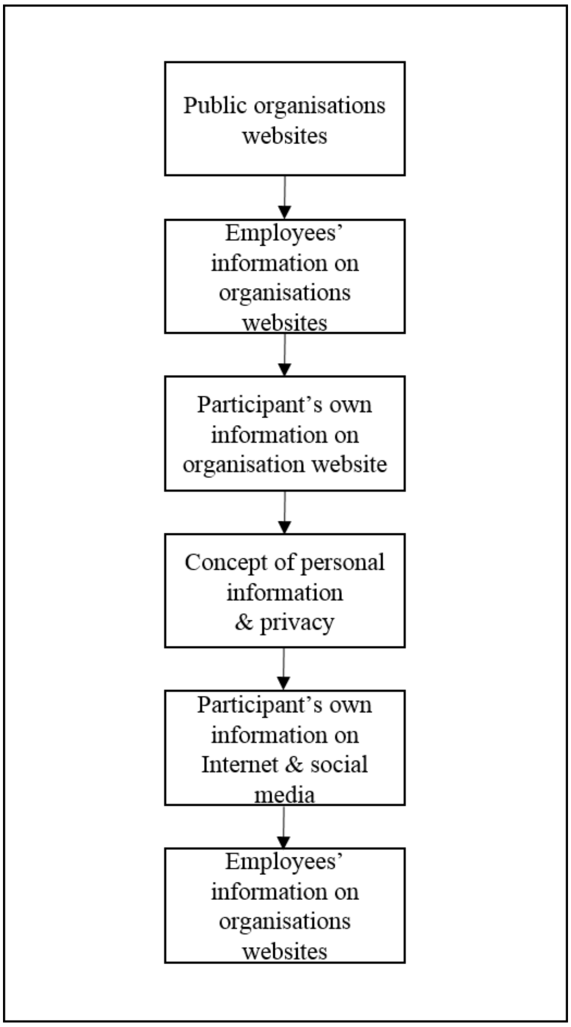

Public organisations websites
Employees' information on organisations websites
Participant's own information on organisation website
Concept of personal information & privacy
Participant's own information on Internet & social media
Employees' information on organisations websites

Figure 3-5: Interview topics

As an introduction, participants were asked about their background in government service, such as working experience, departments served, and their career roles. To start the interview with simple and basic questions is a good practice to gain trust from participants and as a way of warming up the session (Jacob & Furgerson, 2012).

This was then followed by the topics of study as presented in Figure 3-5. Participants were questioned on their familiarity with the public organisation's website in general and their own organisation's website. Later, the questions moved on to the availability of employees' personal information on the public organisation's website and their experience with it. It was crucial to ensure that questions relating to these did not lead the participants into the issue of privacy. It was one of the aims of this study to explore what obligatory disclosure in general meant to the participants. Any preconceived ideas from the participants might limit the findings of research.

Next, participants' perceptions of their own information availability on their organisation's website were gathered. Following this, issues of privacy were dealt with by seeking their conceptual understanding of personal information and privacy. Then, their perceptions and behaviours regarding their personal information on the Internet and social media were explored. Finally, participants were questioned once again regarding their views of the practice in disclosing employees' information on public organisation's websites. In general, the questions were structured in a topical format, but questions within a topic were flexible and could be tailored according to the participants' responses.

3.5 Qualitative data analysis

The qualitative analysis was used when analysing the semi-structured interviews. In qualitative analysis there are various approaches to analysis (Kawulich, 2004). For example, Savin-Baden and Major (2013) listed narrative analysis, ethnographic analysis, discourse analysis, phenomenological analysis and thematic analysis, just to name a few.

Narrative analysis involves discovering similarities through a participant's story. It focuses on the ways participants tell the stories and make sense of the events and actions in which they participated (Savin-Baden & Major, 2013). Ethnographic analysis refers to identifying categories according to a set of classification schemes, based upon concepts from culture or developed by the researcher (Savin-Baden & Major, 2013). Discourse analysis looks into the interaction of people by analysing the mechanism of human communication (Jørgensen & Phillips, 2002). It considers how language enacts social and cultural perspectives and identities. The phenomenological analysis approach attempts to discover how individuals make sense of a particular phenomenon (Savin-Baden & Major, 2013). It is generally centred on an individual's lived experiences which are then synthesised to provide a general description of the experience. Thematic analysis is a systematic approach to identify, analyse and report patterns within data and interpreting it by seeking commonalities, relationships or explanatory principles (Braun

& Clarke, 2006). It is considered one of the primary methods to uncover themes from the data (Savin-Baden & Major, 2013).

Initially the phenomenological analysis was considered to analyse the interview data. It was recognised that phenomenological analysis may also be used for exploration and understanding individual experiences. This approach, which focuses on the experience of lived individuals, aims to interpret meanings from participants according to the investigated context (Savin-Baden & Major, 2013). However, phenomenology is heavily grounded in philosophical assumptions, and some qualitative researchers believe it is too structured (Creswell, 2013a). It was felt that phenomenology may have restricted analysis where it exclusively focuses on an individual's experience without considering other sources of data. Another approach that was also considered is thematic analysis. Thematic analysis is commonly used in many fields and disciplines including case study research. The data is coded and clustered into categories according to its meaning. The strength of thematic analysis is the flexibility of the method, that allows for a wide range of analytic options (Braun & Clarke, 2006).

The difference of analysis between the phenomenological approach and thematic approach is that the latter normally uses *a priori* code at the initial stage of analysis (King, 2004). For this research, *a priori* coding was used during the early phase of research along with an open coding technique for analysing the data.

Henceforth, thematic analysis was selected as the analysis method for the qualitative data collected, because of the flexibility of its analysis approach i.e. inductively, where themes emerge from the data or deductively, which is theory driven (Boyatzis, 1998). Thematic analysis can be used as an inductive or deductive approach which makes it relatively flexible compared to other qualitative methodologies (Boyatzis, 1998). In this study, the inductive approach was used. Themes were linked directly based on the collected data, thus producing semantic themes. Semantic themes offer a descriptive account of meanings of the data. Then, broader meanings of the themes were investigated to uncover latent themes. Latent themes attempt to identify "underlying ideas, assumptions, conceptualizations, - and ideologies - that are theorized as shaping or informing the semantic content of the data" (Braun & Clarke, 2006, p. 84). This analysis requires a more in-depth interpretation. Moreover, the six phase analysis method (Figure 3-6), as suggested by Braun and Clarke (2006), is a recursive process and not systematically rigid. Thus, the process can be suited to the different types and content of the data. It should be noted that the analysis steps by Braun and Clarke are intended as guidelines and not rules.

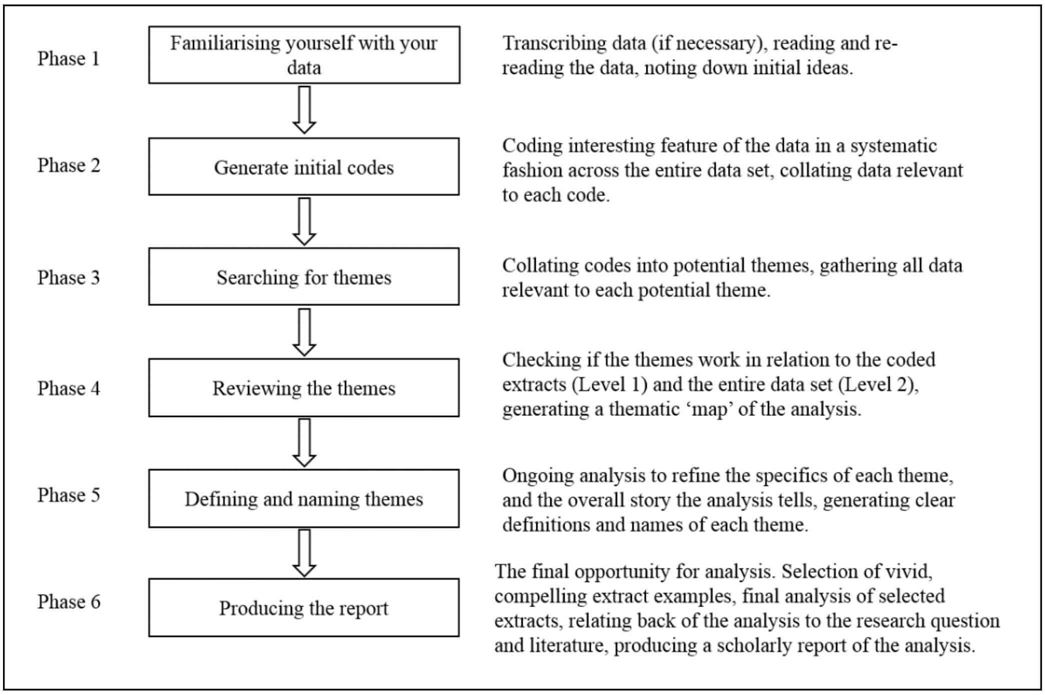

Phase 1
Familiarising yourself with your data
Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
Phase 2
Generate initial codes
Coding interesting feature of the data in a systematic fashion across the entire data set, collating data relevant to each code.
Phase 3
Searching for themes
Collating codes into potential themes, gathering all data relevant to each potential theme.
Phase 4
Reviewing the themes
Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
Phase 5
Defining and naming themes
Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names of each theme.
Phase 6
Producing the report
The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

Figure 3-6: Phases of thematic analysis
Source: Adapted from Braun and Clarke, (2006, p.87)

Few documents were subjected for review in order to gain better understanding of obligatory disclosure. Since obligatory disclosure was related to organisations, a documentation review regarding policies and reports that are relevant to the research questions were corroborated.

3.6 Trustworthiness

Trustworthiness is essential for establishing findings which are authentically collected and accurately represented (Creswell, 2013b). Establishing trustworthiness in a qualitative study is less standardised when compared to quantitative research. However, qualitative researchers have developed rigorous criteria for judging the trustworthiness of qualitative study (Savin-Baden & Major, 2013).

The trustworthiness of qualitative research can be established by its credibility, transferability, dependability and confirmability (Lincoln & Guba, 1985). This research adopted Lincoln and Guba's perspective for achieving trustworthiness as it applies further towards naturalistic inquiry. Therefore, in this research, multiple strategies were incorporated in order to seek higher trustworthiness of the study.

Lincoln and Guba (1985) suggested that credibility is one of the primary factors in establishing trustworthiness. It seeks to ensure that the study is measuring what it is intended to measure. Strategies for achieving credibility in this study included recording the participants' interviews followed by transcribing word verbatim. The participants' transcripts were transcribed faithfully by the researcher. Audio data was listened to repeatedly while the transcripts were reviewed to increase the accuracy of the transcriptions, hence avoiding obvious mistakes.

Another method that was employed was triangulation. Triangulation is an approach of using several different sources of information, either the data or participants' perspectives, to provide supporting and coherent arguments (Creswell, 2013b). This study triangulates its data sources using three data collection approaches, namely: web content analysis, commentators, and documentation.

The different types of personal information that were identified on public organisation websites and what the participants said were utilised for corroboration of information. Another source of information was using commentators. Commentators were selected from academic experts and ICT stakeholders who were involved in the development of ICT in the public sector and assessment of government websites. In addition, users who had had obligatory disclosure imposed upon them and stakeholders who were responsible for ICT development were identified. Documented data that relates to obligatory disclosure was also examined, such as government reports and circulars. By employing more than one source of information, the findings will achieve greater credibility and assist in locating major and minor themes (Shenton, 2004).

Contrasting information from the participants was included in the findings to increase the credibility of the study (Creswell, 2013b). Negative or discrepant information was included when discussing evidence for a particular theme. Those views were treated as an alternative explanation and were examined during the data analysis process. The researcher endeavoured to keep an open mind during the analysis process of this research to search for true data.

Transferability refers to presenting the findings in detail so that it enables readers to decide the applicability of the research in other contexts (Lincoln & Guba, 1985). Thus, a rich description was presented in this study in order to accomplish transferability and help the reader understand the investigated phenomenon and the contexts that surround them (Shenton, 2004). Moreover, detailed procedures were articulated, and a clear and detailed report were provided to enable the readers to "see" the setting for themselves (Lincoln & Guba, 1985).

Dependability can be achieved when the processes of the study are reported in detail. It has to be logical and traceable for other interested researchers to repeat the study with the same results. In this study, the research process and procedure were described including data collection and the effectiveness of the process were reflected (Shenton, 2004).

Confirmability is ensuring that the results of the study are shaped by the participants rather than the characteristics or motivations of the researcher (Shenton, 2004). In addressing confirmability, this study disclosed the researcher's assumptions, beliefs, and possible biases at the outset of study (i.e. chapter 1) to allow the readers to understand the researcher's position. The researcher had to ensure that his personal experiences and assumptions are put aside in order not to influence the participants' views (Patton, 2002). Research documentations, for example, consent forms, research protocols, interview transcripts, and procedures were presented in the main thesis and also in the appendices (Creswell & Miller, 2000). Direct quotations were included in this study to support the findings and increase confirmability. These trustworthiness strategies were employed during the whole course of this research in pursuit of a trustworthy study.

As usual, there are limitations of the analysis method chosen. Transcript data was coded and identified by the researcher. Similarly, developing categories and identifying emerging themes were conducted by the same researcher due to the nature of a doctoral study. Nevertheless, the results were presented to two supervisors for feedback and discussion. By doing this, it was possible to maintain consistency but by discounting the feedback from different views.

3.7 Ethical approval

As this study involved human participants, the researcher had to seek ethical committee approval before conducting the data collection. The ethical approval is meant to protect human subjects when participating in research conducted by institutions. Ethical research practice is typically guided by three principles, namely respect for persons, beneficence and justice (Marshall & Rossman, 2011). It addresses the rights of the participants to participate and protect their privacy as well as considering participants' risks, safety and fair treatment as individuals.

Approval to conduct the study was received on 23rd of April, 2014 from the University of Reading Research Ethics Committee (Appendix F). The researcher clarified to all participants that their participation was voluntary and they could withdraw from this research at any time. All participants were issued a demographic survey form, and an information sheet along with a consent form that described the research purposes, data confidentiality and voluntary participation in the study. Participants who agreed to participate must sign off the consent form indicating that they had read and agreed to willingly participate in the study. All participants were offered US$4.00 as a token of appreciation.

3.8 The researcher's role

Qualitative research acknowledges the influence and important role of the researcher as an instrument across all phases of research. Therefore, it is important for qualitative researchers to acknowledge their pre-existing thoughts and biases early in the research process. This is for the readers to gauge the researchers' position, and suspend or hold their presuppositions, assumptions or previous experiences (Creswell & Miller, 2000).

It was imperative for the researcher to activate the inquiry through fresh and unencumbered lenses in order to focus on the topic without personal judgement or biases (Moustakas, 1994). The researcher was mindful to abstain from including his perspectives on the participants' experience. Borrowing from the phenomenological approach, the researcher took precautions to set aside any pre-existing biases, assumptions and knowledge by being open to participants' descriptions and views. This process is known as 'bracketing', where it excludes the researcher's personal opinions and perceptions of the phenomenon, thus allowing the researcher to focus wholly on participants' views and ideas. Bracketing is also known as *"epoche",* where the researchers' experiences and personal biases are made known to others in order to avoid judgments and biases. The idea is to allow the researchers to distant themselves from the study so that they are not influential (Giorgi, 2009).

Hence, the researcher stated his personal motivation in section 1.2, at the initial part of the research process, to avoid biases cascading from one phase to another due to the nature of the qualitative study (Tufford & Newman, 2012). This approach stresses that the study observes the phenomenon from the person's point of view. It is also believed that the phenomenon cannot be separated from the context in which the topic of interest is investigated.

CHAPTER 4

Analysis

4.1 Introduction

This chapter describes the strategy used in analysing the data. As discussed in the previous chapter, the case study was selected as the research approach in this study. Data analysis for this study consisted of both quantitative and qualitative methods since the data collection technique employed web content analysis, semi-structured interviews and documentation.

The web content analysis adopts a summative approach for analysing personal information disclosure on government websites. This approach used both quantitative and qualitative methods in analysing websites (Hsieh & Shannon, 2005). The websites are evaluated based on the occurrence of pre-determined keywords or variables to classify and determine the existence of the material, (Neuendorf, 2002), which will offers analysis of data in terms of percentages and frequency that will increase understanding of the situation. The chapter then discusses the thematic analysis process that was selected for analysing data collected from in-depth semi-structured interviews. Next, the analysis is extended to include interpretation to the content or contextual meaning of the material (Hsieh & Shannon, 2005).

4.2 Web content analysis

In order to explore and understand how obligatory disclosure discloses employees' information, web content analysis of selected websites was conducted. Different types of personal information can be systematically identified and evaluated accordingly. Two types of variables were identified for the data analysis, which are personal information of employees and the specific website characteristics. The process of analysis underwent several steps as stated in section 3.4.1.4. After defining the unit of analysis (refer to section 3.4.1.2), the next step is to develop codes, categories and the coding scheme.

4.2.1 Developing codes and categories

Codes and categories were developed by using both inductive and deductive approaches. In this study, where studies of personal information on organisation websites were scant, an inductive approach is preferred (Neuendorf, 2002). Codes were developed by scrutinising the possible context of investigated phenomenon. Thus, the initial list of codes and categories were developed from the results of the researcher's pilot study. By doing this, variables that emerged from the process were grounded in the context (Neuendorf, 2002). However Neuendorf (2002) cautioned on being too reliant on the inductive approach as it may limit the researcher from other possible variables. Therefore *a priori* or deductive technique for selecting variables were employed together with inductive technique. In *a priori* coding, findings from literature assist in establishing initial codes.

Preliminary investigations on 17 public organisation websites (not included in the main sample) from seven countries (Badrul et al., 2014) served as a basis for the construction of a coding scheme (i.e. a set of measures in a codebook) including findings from available literature. Earlier studies which listed attributes as personal information were also considered in developing the codebook. Thus, preliminary study and literature identified eight personal information attributes.

For this main web content analysis, first, the researcher identified and listed personal information attributes as the initial code. In addition, during the coding process, the researcher discovered new attributes that did not fit within existing codes. Hence, new codes were developed to assign each type of the personal information to a category. Similarly, if an existing code can be further segregated to smaller code-able data, the codes were reassigned to new codes. For example, 'biography' was recoded into 'age' and 'gender' in order to capture the exact attributes of personal information. These codes were important because they serve as the initial framework for developing the codebook. The initial list was discussed with an expert, and minor modifications were made.

Table 4-1: Preliminary attributes for codebook

Attributes	References
Full name	(Krishnamurthy et al. 2011; Lam et al. 2008)
Email address	(Krishnamurthy et al. 2011)
Photo	(Aguiton et al. 2009; Wang et al. 2010)
Location	(Lederer et al. 2003)
Salary	(Metzger 2004; Olson et al. 2005)
Telephone number	(Metzger 2004)
Physical address	(Krishnamurthy et al. 2011)
Biography	(Wang et al. 2010)
Occupation	(Krishnamurthy et al. 2011; Lam et al. 2008)

During the researcher’s preliminary study, few sources of information disclosure were identified which can give insights into the quality of dissemination of information. Since the medium of communication in this content analysis is the website, one recommended strategy of identifying variables is focusing on the medium-specific variables as suggested by Neuendorf (2002).

Therefore, instead of focusing solely on personal information attributes, specific website characteristics were also measured by the coders. With regards to the main objective of this research, coders considered the visibility of information, authority, updated-ness, and quality assessment of the websites including privacy and security policy matters. These criteria were among the criteria suggested by Pinto et al. (2007) to evaluate the quality of “dissemination of information” (p. 350) through websites. Another relevant criteria was findability, which was used to evaluate the easiness of finding or discovering an object from the website (Kopackova et al., 2010; White, 2003). In addition, these criteria were embedded within Panopoulou's et al. (2008) framework for evaluating e-Government websites. These criteria are expected to influence the disclosure of personal information of employees.

Visibility of information is to evaluate whether the specific information is visible and accessible from its homepage. In website evaluation study, this criterion was one of the two most important criteria to assess the quality of information (Pinto et al., 2009) and is related to the *accessibility* criteria in the evaluation framework (Panopoulou et al., 2008). In this research, accessibility of information about employees is evaluated based on the distance it is located from the homepage.

Website credibility depends on the identity of its owner. In the *website's content* dimension, this type of information is categorised under the *general content* criteria which relates to *authority*. *Authority* refers to the identity of the website owner. The presence of this information on a website increases its quality and validity of information (Pinto et al., 2007). For this reason, a public organisation's logo and department's identity were considered as the authorship of the websites. Since the sample was selected from an official government report, the authority of the websites can be assumed as being satisfied.

Websites have to publish information that is recent and keep this regularly updated in order to provide a high level of information quality (Gilbert et al., 2004). Information that is outdated or obsolete will deter the public from adopting e-Government (Shareef et al., 2011). Therefore, it is pertinent to focus on whether the website is up to date and users are aware of the date of last update (Pinto et al., 2009). This is the criteria for *updatedness*.

Quality assessment is applied to the assessment of specific features of the website. Website policies were analysed in order to assess the importance of the specific features of information posted on a website and the emphasis that was given to it from the person or entity in charge of the development of the website (Pinto et al., 2007). In this study, the aim is to explore the personal information of public employees and its relation to privacy, therefore privacy policy, security policy, disclaimer, and personal information charter were selected for analysis. These features were selected because it will enable website users to determine how personal information is processed, how the websites deal with the issues of privacy and personal information.

Findability is the ability to find a web page or resources and it is part of the *navigation* criteria. On a broader perspective, findability is can be seen as a website usability criteria (White, 2003; Kopackova et al., 2010). In order to evaluate findability capability of finding personal information from within the websites, a search feature presented on a website is coded. A specific feature or a characteristic that is relevant to the medium is known as *form attributes*. Form attributes may influence the underlying meaning of content attributes and it is important to consider making this specific feature available (Neuendorf, 2002). The *search* feature is used to generate searching for specific information available on a website. By having this feature on a website, information that is published can be conveniently searched and accessed.

Based on Neuendorf's (2002) suggestion to consider medium-specific as variables, this research identifies *search* feature, *employee directory*, *privacy* and *security policy*, *website disclaimer*, *personal information charter, calendar, notice of last updated, translation* feature and *website terms and condition* as medium-specific critical variable for this study.

Both codes that cover types of personal information and website's quality characteristics were included in the analysis. Finally, a list of 36 codes related to personal information and website features was developed as shown in Table 4-2.

As explained before, two techniques were used for analysing the manifest content of the websites. First, the variables for personal information (listed from number 1 to 23) were coded using ordinal_schema. For these variables, a value of '0' was assigned when no variables were found, '1' when partial information of the variable is available and '2' when information is completely disclosed.

Secondly, for website quality characteristics, a two-step process was implemented (Hsieh & Shannon, 2005). The first step is to measure the manifest content on the website by using a nominal schema. A value of '0' was assigned when it is not available and a value of '1' when it is identified on the website. Secondly, the latent content of the code was measured based on the outcome of the nominal response. The latent content requires the coders to interpret the findings based on coding guidelines.

For *employees' directory, employees search feature* and *general search feature,* coders coded the availability of the feature (if, any). If the features were identified on the websites, coders then assess the discoverability (Jones & Potts, 2010) of the features. Coders were instructed to code from the level of the homepage where those features become accessible. If it can be accessed from the homepage, then coders must state *homepage* in their response. If it is accessible on the next page after the homepage, then

Table 4-2: List of codes

No	Variable	Definition
1	Full name	Full name of employee
2	Photographic image	Identifiable image of employee
3	Ethnicity	Relating to a particular race of people
4	Gender	The state of being male or female
5	Marital status	State of relationship whether married or single
6	Date of birth	Day of one's birth
7	Birth place	The place where a person was born
8	Age	Period of time a person has lived
9	Education qualification	Fitness for purpose through fulfilment of necessary conditions
10	Awards	Recognition from the state or country
11	Personal ID	12 digits of national ID number
12	Working position	Job position within an organisation e.g. engineer, assistant secretary
13	Grade	Working grade
14	Salary	Payment received as employee
15	Work scope	The types of work, duties or responsibilities of employee
16	Email address	Electronic post box that can send and receive email
17	Telephone number	A number assigned to a telephone line to contact an individual
18	Fax number	A number dedicated to telephonic transmission of scanned printed material
19	Physical address	The physical address that points to a place
20	Direction	The instructions for how to reach the organisation
21	Location	A place or position where something is
22	Pre-event	An indication before an event take place
23	Post-event	An indication after an event take place
24	Opening hours	The times when an organisation is open for public
25	*Employees directory	Electronic database listing individuals in an organisation
	Discoverability	The degree to which the feature is easy to discover or locate
26	*Employees search feature	A feature that search for employees information on the website
	Discoverability	The degree to which the feature is easy to discover or locate
	Filtering menu	Types of criteria available to filter results
27	*General search feature	A feature that search for information on the website
	Discoverability	The degree to which the feature is easy to discover or locate
	Ability to search employee	Whether employee search can be conducted
28	*Organisation chart	A diagram of how an organisation is structured
29	*Privacy policy	A statement on privacy for website visitors
30	*Security policy	A statement on security of information
31	*Disclaimer	A statement to specify or delimit the scope of rights and obligations
32	*Personal information charter	Explanation of the process of personal information of website users
33	*Terms and condition	Information about the website content and how visitors are governed by it
34	*Calendar	A feature that shows the day, week, month
	Published activities	Activities/events that were filled in the calendar
35	*Date of last updated	Information about updating website content
36	*Language available	Availability of language for the websites
	Translation	Offering the users translation feature into different languages

**Website quality characteristics*

coders should code *second* as their response indicating that it is accessible on the second page after the homepage.

In addition, coders were required to code the *filtering menu* if it was included in the search feature. They were instructed to list all filters that were available. The inclusion of search filters increased the possibility of finding a particular employee. On the other hand, a general search feature (if it was found) was tested on whether it was possible to conduct a staff search.

The *organisation chart* was identified during the pilot study as one of the possible sources of disclosing information about employees. Coding of the *organisation chart*, if available, requires the coders to examine the organisation chart for whether it is a detailed organisation chart or a general organisation chart. A detailed organisation chart will disclose employees' information and coders were required to code the attributes that were disclosed. In contrast, a general information chart discloses the structure of an organisation without revealing the details of employees.

Privacy and *security policy*, *website disclaimer*, *personal information charter,* and *terms and condition* of websites are included in the codebook. To understand how these policies and statements provide coverage of personal information of employees, coders were required to state what was published and how it relates to employees' information.

Having a website requires it to be regularly updated. Hence, *calendar* feature and *information on last updated* was selected for the quality dissemination of information criteria. The calendar was analysed for its up-to-dateness by looking at information published and whether it was well-maintained. Another piece of information that was enumerated was information on the last update. This information was normally found on the homepage. Websites that inform its user of the 'date of last updated' will be seen as projecting a good image of an organisation. Both variables were scrutinised for their occurrence and information published.

Coders also coded the *languages* available for the websites. In addition, if the websites offered a translation feature, coders have to identify the number of languages that can be translated.

Table 4-3: Categories of personal information

Category	Definition	Example
Personal attributes	Information that could be directly related or associated with an individual	Full name, Photographic image, Gender, Marital status, Personal ID number
Personal achievement	Information regarding accomplishment of an individual	Education qualification, awards
Employment information	Information regarding full time job	Position, grade, level, work scope, salary, department
Contact information	Information that could be used to (directly) communicate with an individual	Email address, telephone number, fax number.
Geographical information	Information regarding the specific location of individual	Physical address, location map, direction to address
Timeliness information	Information regarding when any event or activities occur or references to specific time	Today, tomorrow, last week, date

The codes reflected the types of personal information which were then grouped into six categories at the highest level of measurement possible, based on how they were related and connected (Table 4-3). When developing categories, it is important to ensure that the categories are exhaustive and mutually exclusive to avoid missing codes and duplication of meanings (Neuendorf, 2002).

Given the importance of website characteristics for dissemination of information, six categories were developed to further understand the extent of disclosure. The categories for website quality are presented in Table 4-4 below.

The code book was then used to develop a coding form and coding guidelines. A standardised coding scheme (containing code book, coding category, coding form, coding guideline) was developed prior to coding the websites.

Table 4-4: Categories for website quality

Category	Definition	Example
Visibility	How easy the information can be accessed from the homepage	Existence of direct link from homepage
Authority	Information on the identity of the author of information / website	Organisation's name, logo
Updatedness	Information on website content that is recent	Calendar feature, notice of last updated
Findability	Ability to find webpages or resources	Search feature
Policies	The quality and emphasis on specific subject by those responsible for the website	Privacy policy, security policy, disclaimer, personal information charter

This research utilises manual coding, which is coding by humans instead of computers. While computer coding can save time, lower cost and can cover larger data sets (Duriau et al., 2007), human coders are better when working with complex codes and categories (Linderman, 2001). Personal information, such as individual's name and contact information, is unique and contextual. The role of humans in the content analysis process is undeniable to bring the contextual element to the content (Lewis et al., 2013). Besides, computers have limited capabilities in understanding latent meanings, (Conway, 2006) which paves the way for the decision to adopt human coding to perform content analysis.

When choosing coders, Krippendorff (2013) argues that it is vital to consider their backgrounds to ensure they possess a level of familiarity with the subject of investigation. In addition, the coders must have the ability to maintain consistency throughout an analysis which is difficult, especially when it involves a large amount of samples. He further stressed that it is best to select coders who can be easily available within the population of potential coders, in case other researchers ever want to replicate the research.

Based on the above cautions by Krippendorff, two coders who were not involved in the research were recruited to assist in the coding process (only for web content analysis). A general invitation request was posted in a small local Malaysian Facebook group and both of them responded positively to the request. They were both Malaysians and native speakers of the official language. Subsequently, choosing coders from the same cultural background helped to increase the reliability of the results (Peter & Lauf, 2002). In terms of academic qualifications, coder 1 possesses a Master’s degree while coder 2 had a Bachelor degree. Both coders did not know each other previously, and both have had working experience in Malaysia. As it was anticipated that the coding process would be very time-consuming, this study considered another characteristic of coders which was, availability. Both coders had plenty of spare time and were willing to contribute to this research.

The coder training procedure was implemented based on Neuendorf's (2002) guidelines. Before commencing the coding, both the coders attended a training session to learn the coding protocol. During this session, the coders were briefed on the objectives of the coding before they were presented with the coding scheme (containing code book, coding category, coding form, measurement technique). There was also a coding demonstration held to increase coders’ understanding.

4.2.2 Testing the coding scheme

After the training session, a pilot coding was carried out independently by the author and the two coders. Conducting a validation technique at an early stage may be useful in identifying inconsistency among the coders as well as allaying any doubts or confusion that may arise from the initial coding rules (Zhang & Wildemuth, 2009).

A Malaysian Government website, which is not from the sample, was selected. Results were gathered and discussed during the second training session. The training session was used to informally assess the coders’ reliability and any concerns which might arise from the pilot coding exercise. The author and coders reviewed discrepancies, and the coding scheme was improved. During the pilot coding exercise, it was discovered that some of the issues were overlooked during the training session, such as the language version of websites to be coded, was finalised. It was discovered that different versions of a website (i.e. Malay version and English version) produced different content. Hence, the results of the pilot coding exercise cannot be calculated for consistency. For the purpose of this study, it was decided that only the official Malay version of the websites were considered.

Therefore, a second pilot coding exercise was conducted using the same website. The coding by the researcher and the coders were assessed and compared. Inter-coder reliability was calculated and the results are shown in Table 4.7.

After undergoing two pilot coding practices and training, a final coding scheme was developed and consequently both of the coders were provided with the list of websites as the samples. The details of coding scheme are included in Appendix G. It was important to ensure that the researcher and the coders were comfortable with the coding scheme before commencing with the final coding (Neuendorf, 2002).

4.2.3 Coding process

This research uses human coding instead of computer coding because human coders is more reliable when interpreting latent content (Krippendorff, 1989) and to provide contextual sensitivity to the content (Lewis et al., 2013).

The first coder was assigned with 11 websites while the second with 12 websites. Both coders coded independently. Three websites were coded by both coders for the purpose of calculating inter-coder reliability. The three websites were Manjung Municipal Council, Penang State Government, and Ministry of Natural Resources and Environment. Inter-coder reliability will be discussed further in section 4.2.4.

It was observed during the preliminary study that all of the four websites of Malaysian Government agencies were organised in a hierarchical structure where the content was more specific when it was navigated further from the homepage. Therefore, the coders were instructed to start coding from the main homepage as the starting point of the coding process. This was due to the fact that the homepage served as the main identification of a website which should present the website overview and major sections, hence establishing the website's credibility by developing trust (Krug, 2006). Then coders navigated to the next level below the homepage and resumed coding the webpage. This process continued until the coders reached the end of the link and subsequently, coders restarted coding from the next link that was available from the homepage.

Table 4-5: List of coders and websites

Coder 1	1.	Manjung Municipal Council (MPM), *www.mpm.gov.my*
	2.	Gerik Disctrict Council (MDG), *www.gerik.gov.my*
	3.	Kajang Municipal Council (MPKj), *www.mpkj.gov.my*
	4.	Sarawak State Government (Sarawak), *www.sarawak.gov.my*
	5.	Penang State Government (Penang), *www.penang.gov.my*
	6.	Kelantan State Government (Kelantan), *www.kelantan.gov.my/v6/index.php*
	7.	Negeri Sembilan State Government (NS), *www.ns.gov.my/main.php*
	8.	Ministry of Finance (MoF), *www.treasury.gov.my*
	9.	Ministry of Natural Resources & Environment (NRE), *www.nre.gov.my*
	10.	Ministry of Housing & Local Government (KPKT), *www.kpkt.gov.my*
Coder 2	1.	Manjung Municipal Council (MPM), *www.mpm.gov.my*
	2.	Kang Municipal Council (MPK), *www.mpklang.gov.my*
	3.	Tapah District Council (MDT), *www.mdtapah.gov.my*
	4.	Besut District Council (MDB), *www.mdb.terengganu.gov.my/home*
	5.	Penang State Government (Penang), *www.penang.gov.my*
	6.	Selangor State Government (Selangor), *www.selangor.gov.my/main.php*
	7.	Pahang State Government (Pahang), *www.pahang.gov.my*
	8.	Prime Minister Department (JPM), *www.jpm.gov.my/post/modules/main/index.php*
	9.	Ministry of Natural Resources & Environment (NRE), *www.nre.gov.my*
	10.	Ministry of International Trade & Industry (MITI), *www.miti.gov.my/cms/index.jsp*
	11.	Ministry of Communication & Multimedia (KKMM), *www.kkmm.gov.my*

External factors that may influence the findings were controlled during the content analysis process (Baloglu & Pekcan, 2006). Both coders were instructed to use the same browser, same operating system, clear cookies and caches and similar timing for coding.

Both coders were supplied with the hard copy and soft copy of the coding scheme. This was in response to the fact that one coder preferred the hard copy while the other found the soft copy to be more convenient. The coding process took slightly more than one month for both coders to complete.

4.2.4 Inter-coder reliability

Due to the chosen strategy of coding i.e. human coding, it was essential to measure the extent of agreement and consistency among coders (Neuendorf, 2002). Since humans can have subjective interpretation towards an object, a reliability measurement is important to ensure that coders have similar judgement when making decisions (Neuendorf, 2002).

Failure to achieve a sufficient level of inter-coder reliability causes the data and its interpretation to be at risk of being invalid (Lombard et al., 2004). Moreover, coding the latent content is more difficult because it is prone to subjective errors and subjective human decision-making, whereas manifested content is fairly straightforward (Potter & Levine-Donnerstein, 1999).

To ensure the trustworthiness of the data, reliability tests were performed. One of the reliability tests that was performed was the inter-coder reliability test. Reliability is a concept that the same data is produced after repeated measuring process. The results were generated independently and free from biases, distortions and pollutants and remain consistent for everyone who utilises them (Krippendorff, 2013). Another reason for achieving an acceptable level of inter-coder reliability is to serve as a basic validation technique of a coding scheme (Neuendorf, 2002). Seven commonly-used indexes in assessing inter-coder reliability are shown in Table 4-6.

Table 4-6: Types of inter-coder reliability index
Source: Adapted from Taylor and Watkinson (2007)

Index	Metric	Chance agreement	Correlation/ agreement	Range expressed
Percentage agreement	Nominal	N	Agreement	0.00 – 1.00
Scott's *Pi*	Nominal	Y	Agreement	-1.00 - +1.00
Cohen *Kappa*	Nominal	Y	Agreement	-1.00 - +1.00
Krippendorff's *Alpha*	Nominal, Ordinal, Interval, Ratio	Y	Both	-1.00 - +1.00
Perreault's *Pi*	Nominal	Y	Agreement	0.00 – 1.00
Spearman's *Rho*	Ordinal	N	Correlation	-1.00 - +1.00
Pearson's *r*	Interval	N	Correlation	-1.00 - +1.00

In choosing a reliability index, there are a few factors that should be considered, such as variables' attributes including their level(s) of measurement, the number of coders and the expected distribution across categories (Lombard et al., 2002).

Taylor and Watkinson (2007) suggested that it is recommended to assess inter-coder reliability using more than one index and later compare both sets of reliability data to gain a better perspective. Lombard et al. (2002) stressed the need for a second index if the percent agreement was chosen in order to improve the quality of data reliability.

Both percent agreement and Krippendorff's *Alpha* were selected to assess inter-coder reliability. Percent agreement is simple, easy to calculate, easy to interpret, has strong intuitive appeal and can support any number of coders. It is calculated by adding up the total number of agreements between coders and dividing it by the total number of the coded units. For example, if both coder 1 and coder 2 agreed on 15 out of 30 codes in a codebook, the inter-coder reliability is calculated by dividing 15 from 30, which would result in 50% agreement. Although it is commonly used, this reliability index received criticism because it did not take into account the consensus that could occur solely based on chance (Lombard et al., 2002). Another drawback is the ability for the researchers to escalate reliability by adding pointless categories (Lombard et al., 2002). While Krippendorff (2013) is not keen on using percent agreement as an inter-coder reliability measurement, Lombard et al., (2002) suggested that it can be used, due to its advantages along with other reliability indexes that can take into account the issue of chance agreements.

To compensate the drawbacks from relying exclusively on percent agreement, another index was selected to increase inter-coder reliability (Taylor & Watkinson, 2007; Lombard et al., 2002). Krippendorff's *Alpha* was chosen because of its flexibility, suitability of data types, multiple coders and accounts for chance agreements. Moreover, it is accepted as a standard for reliability measurement (Neuendorf, 2002) although, Lombard et al. (2002) argued that there is no single best index. Nevertheless, this index is not without criticism. Most criticism is due to its complexity and difficulty to calculate by hand (Taylor & Watkinson, 2007). However, this index is able to accommodate multiple data types including ordinal data. which was used in this study to measure the level of disclosures.

There are disagreements among researchers in deciding an acceptable level of inter-coder reliability (Neuendorf, 2002). In general, Neuendorf (2002) pointed out that coefficient correlation with .90 or greater would be acceptable to all, .80 would be acceptable in most situations and below that disagreements exist. However, Krippendorff (2013) proposed α value of more than .80 for analysis within the communication studies, while α value of between .667 and .80 may still be used for drawing tentative conclusions. In fact, the coefficient value of.70 is often used for exploratory research (Lombard et al., 2002). Furthermore, Lombard et al. (2002) specifically suggested Krippendorff's α of .70 to achieve reliability.

As mentioned earlier, before the coders were presented with their main list of websites, one government website from within the population, was selected for pilot reliability assessment, but would not be included in the sample. Assessing pilot reliabilities is essential in content analysis and should be done before the main coding exercise (Neuendorf, 2002). This is another way to generally validate the coding scheme.

In order to determine inter-coder reliability, 16% of the websites were cross-coded by both coders to assess an overall level of inter-coder reliability without their knowledge. The amount of 16% exceeds the 5 to 10% that was suggested by Thayer et al. (2007) as a sub-sample to calculate inter-coder reliability. In addition, Lacy and Riffe (1996) proposed a sample size of no less than 10% of the full sample.

The inter-coder reliability was calculated using a manual approach i.e. by paper and pencil, for percent agreement and using an online utility, ReCal (Freelon, 2013) for Krippendorff's α. ReCal is also listed as one of the software suggested by Lombard et al. (2004) to calculate inter-coder reliability.

Table 4-7: Results of inter-coder reliability

Coding sample	Percent agreement	Krippendorff's alpha
Pilot coding (non-sampled)	0.85	0.704
Sample 1 – (council)	0.91	0.817
Sample 2 – (state)	0.86	0.843
Sample 3 – (ministry)	0.86	0.742

The inter-coder reliability for percent agreement was between 0.85 and 0.91, which is considered acceptable in most situations as suggested by Lombard et al. (2004) and Neuendorf (2002). In addition, results from Krippendorff's α satisfies the reliability conditions where Krippendorff (2013) recommends the value of 0.67 and 0.80, while more than 0.80 is considered achieving high reliability.

4.2.5 Decisions concerning the coding process

The final phase of content analysis is to report all decisions and practices made during the coding process (Zhang & Wildemuth, 2009). This is recommended when the analysis involved qualitative content analysis.

In this analysis, the content analysis was conducted on the Malay version of websites and it was assumed that similar disclosure occurred in the English version. This was despite the discrepancies in information between the two versions that were discovered during the initial training session with the coders. As an illustration, the published attributes about the same employee (senior management) were found to be disclosed differently on each version of the website. However, it should also be noted that the difference was minor and did not create confusion to website users about that particular employee.

Websites for the state Government mostly comprised of many state departments and agencies that operate in that particular state. To focus on the core operational agency within each state, it had been decided that the coding process of personal information was directed to each State Secretary Office (SUK). For the Sarawak State website, the coders coded data from the Chief Minister Department (Jabatan Ketua Menteri) which is similar to the State Secretary Office. By doing this, firstly, the sampling covered information on employees of the state administrative centre - where the development, maintenance, and operation of all IT-related functions of the state (including the state website) was under its jurisdiction - and, secondly, the coding process could be undertaken within a shorter period of time - which was important since this research had time limitations. The findings of the web content analysis are reported in the next chapter.

4.3 Semi-structured interview

This section involves analysis of the qualitative data from participants, which is the main case of investigation for this research. The analysis is adopted from the six-phase thematic analysis method, as suggested by Braun and Clarke (2006).

4.3.1 Data management

The participants' demographic properties form and consent form were manually checked by the researcher after each interview. These documents were then kept in an enclosed file and were brought along during each interview session.

Interview audios were played immediately after each interview session to ensure that it was recorded successfully. Data from the interviews was transferred from the recording device to the researcher's notebook. The data was stored in a designated folder in the notebook during fieldwork. Similarly, interview data was stored in a password-protected computer in the university, and the participants' documents were kept in a locked file cabinet to preserve their confidentiality.

4.3.2 Software analysis tool

Qualitative research produces a large amount of data for the researcher. Therefore, the researcher decided to use a software analysis tool to assist in analysing qualitative data. NVivo version 10 is a Computer-Assisted Qualitative Data Analysis Software (CAQDAS) that is normally used for analysing qualitative data, which was selected by the researcher for this thesis. The software was provided by the university. Although the main purpose of choosing NVivo was to analyse qualitative data, it has a built-in transcribing function. By using the same software for transcribing and analysing, the researcher was able to produce the transcripts in an automated timespan and synchronous with the audio data. Therefore, if the researcher was required to listen again to a selected conversation, the researcher could select the specific interview segment and the software would directly point out the selected audio that tallies with the transcript. It eliminates the need for audio searching and this saves a lot of time. Equally important is the ability to be familiar with the software at an earlier stage, which reduces the hassle of managing transcripts and audio between different software.

The audio data that was recorded was in .m4a file format. While the quality of recordings was high, the file format was not supported by Nvivo version 10. Therefore, the audio files had to be converted to a format that could be read by NVivo. A third party file converter tool was used to convert the file from .m4a to .mp3 format. The file converter tool was installed on the researcher's computer and subsequently, all files were successfully converted. The converted files were exported to the NVivo software.

4.3.3 Transcription process

All 24 interviews were transcribed faithfully by the researcher using the NVivo software. Transcribing was conducted using NVivo version 10. Since this research aimed to explore the meanings of investigated phenomenon from the participants, verbatim transcription was considered appropriate to uncover the underlying meanings. Transcribing was conducted in verbatim where the exact spoken words were reproduced from the audio recorded data. Besides capturing verbal words, the non-verbal interaction was also important to fully understand the communicative meaning of the speaker (Bailey, 2008). Hence, not only what is being said is important, but how it is said is particularly as important. Thus in this research, transcripts recorded nuances of the speakers such as the interviewee's tone of voice, pauses, speed, emphasis and laughter for data interpretation.

After each transcribing was completed, the transcript was reviewed again for cross-checking. This step was undertaken concurrently with the original audio file for accuracy purposes (Fasick, 1977). This process was to detect any missing words, spelling errors and to improve the quality of the first cycle of transcription. Next, the audio and transcript were listened to and read again to allow the researcher to immerse in the data and develop a greater depth of understanding of the data before analyses began. Thus, these steps increased the trustworthiness of the transcripts and ultimately reflected on the validity of the findings (Poland, 1995).

Although transcribing was a lengthy process, it allowed the researcher to be familiar with the data. By self-transcribing the interviews, the researcher was able to learn more about the participants (Richards, 2005) such as familiarising with participants' characters, developing profiles of the participants, and reflecting on the available evidence from the data.

4.3.4 Data analysis

Analysis of data is adapted from Braun and Clarke, (2006). Qualitative analysis, however, being not a straightforward step-by-step process, is cyclic with regular reviews throughout the analysis process (Vaismoradi et al., 2013).

Reading and listening to the data multiple times assist in developing codes during the analysis (van Manen, 1990). Coding is a process of assigning labels to parts of the data that capture the meaning of each segment of data (Savin-Baden & Major, 2013). This process allows the researcher to learn from the data, observing details and its underlying properties for identifying emerging themes, topics or relationships. Often, coding is repeated in order to review the coded data, reflect on the context and to familiarise with the data. Coding will provide links between the original 'raw data' and the researcher's theoretical concepts. It can be seen as one way of connecting the data to a particular idea or concept (Miles et al., 2014).

According to Saldana (2013), a code is "a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data" (p. 3). Codes were generated by selecting important segments of a line, phrase or paragraph from the transcript that is relevant to the research questions. While coding can be seen as a data reduction technique, it is an analytic process that identifies the features of the data (semantic or latent content) (Boyatzis, 1998). The process involved using transcripts that were exported into the NVivo software with selected segments of data highlighted and coded labels. This codifying process (i.e. arranging codes in a systematic order), as outlined by Saldana (2013), was applied to generate themes from codes as illustrated in Figure 4-1.

Data was coded either by open coding or in-vivo coding by the researcher. Open coding is the process of assigning codes to the data by conceptualising the data (Strauss & Corbin, 1990). Saldana (2013) describes it as first-cycle coding. The first cycle coding method is the process of assigning codes to the data for the first time. This process is to detect re-occurring patterns which are useful in the next coding method.

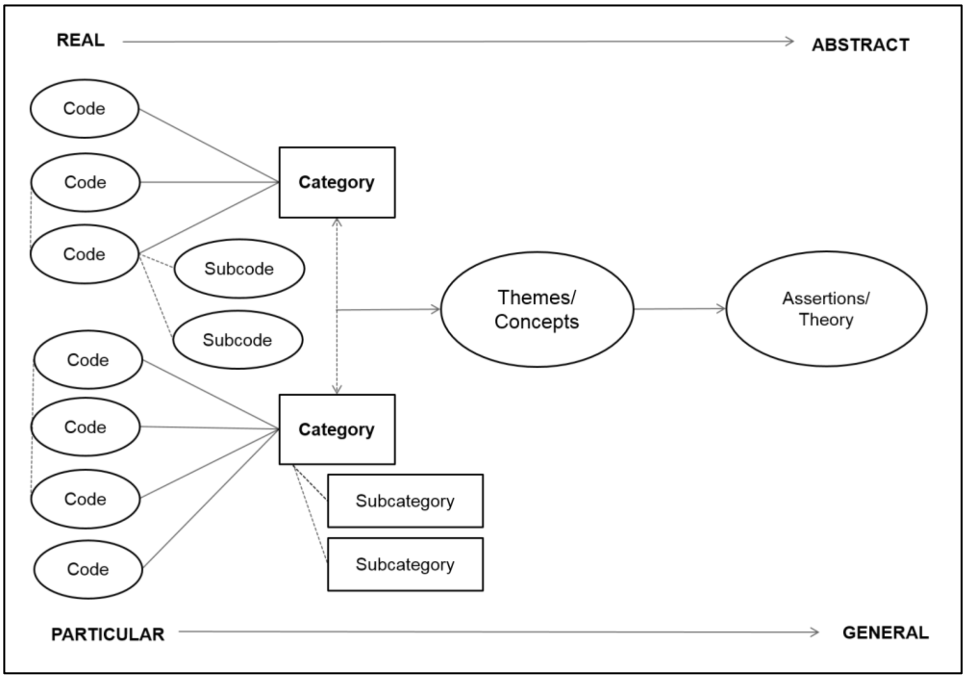


Figure 4-1: A streamlined codes-to-theory model for qualitative inquiry Source: Saldana (2013, p.13)

Meanwhile, in-vivo coding involves assigning code labels using the participants' own words (Saldana, 2013), which could reduce the possibility of misinterpretation by staying 'true' to the data (Ritchie and Lewis, 2003). Coding approaches can encompass descriptive coding, interpretative coding and analytical coding. In general, there are three different types of coding approaches that are usually adopted in research, which are descriptive coding, topical coding and analytical coding (Richards, 2014).

Descriptive coding, as the name implies, describes the attributes of a case. For example, the demographic properties of participants such as the interviewee's gender, working experience, salary scale or working category. Topic coding is assigning chunks of data according to topics or subjects. Topic coding is relatively straightforward, as the data is grouped according to the subjects. For example, anything that is related to *working experience* is sorted under it. Although this type of coding might look easy and unchallenging, it could be a starting point for a more advanced analysis (Richards, 2014). Analytical coding is a type of coding that requires interpretation, reflection and meaning.

This type of coding is one that develops new ideas, creates conceptual categories and explores meanings (Richards, 2014).

For the data analysis, the coding process is conducted in the original language of participants. The reason of doing this is to maintain the participants' words and the original meaning of participants. Later, when presenting results, the quotations of transcription were translated into English by an English language lecturer from Malaysia currently pursuing a PhD in the UK.

The researcher coded each transcript with phrases, words or sentences that captured its meaning. Using the NVivo software, the researcher selected relevant texts to identify the segments by extracting them to a meaningful code label guided by the research questions. An example of initial coding is presented in Table 4.8.

Table 4-8: Example of initial coding, participant P002

English transcription	**Initial codes**
P002: Erm the disadvantage is (the) phone will always ringing and it's like, other people's work will, erm yes I am the one who answers the phone so uh this and this. But to me, since I used to contact [department A], so I will get angry if they [department A] is not answering my call. *So it's like, it's like if they (not answering telephone calls), we can't get angry at them for not answering. So the public will feel the same towards us (when there is no answer) therefore if it rings (I) will try to assist where I can. Ah telephone will always ring when I was in [department B]. It's like there was no time, (because) they even call during break. Also when preparing to go home, they call even when I'm ready to carry my bag.*	Code: always receiving calls Code: doing other people work Code: experience as public contacting government office Code: angry with government service Code: angry with government service Code: assist public whenever possible Code: always receiving calls Code: receive calls outside office hours

During the interview process, while listening to participants, the researcher made notes of personal reactions of the participants, how the participants answered the questions, interesting issues to be pursued further and thoughts on revising interview questions and protocols. This, is called 'jottings', and assisted the researcher during the coding process because it points to specific issues that deserve analytic attention - which would eventually benefit the data analysis process (Miles et al., 2014).

With a long list of different codes that kept increasing, the codes needed to be organised and categorised. Individual codes were grouped together into a similar pattern. This phase is called categorising (Savin-Baden & Major, 2013). Categorising can be conducted either during the first-cycle or the second-cycle of coding and it is a continuous process as long as information can be clustered together according to specific criteria. The most significant patterns in the coded text segments were extracted to categorise the codes.

Thoughts of similar ideas began to develop after completing the coding process for a few transcripts. In the NVivo software, categories can be readily created to represent similar ideas. Similar patterns of codes were selected and grouped together with the relevant category created. Categorising data enabled the researcher to develop higher level analytic meanings from the data (Miles et al., 2014; Saldana, 2013).

After completing the coding process of five transcripts, the researcher presented the codes and categories for reviewing and refinement to the supervisors. Any code or category that was deemed unfit was recoded. By doing this at the initial stage of the analysis, the researcher was able to evaluate the accuracy of the codes, and revisited the developed code when the number of codes was much less. In fact, Saldana (2013) acknowledged the difficulties of coding by noting that it is rare for someone to code correctly in his or her first attempt.

Next, a higher level of analytic meaning for assertion, proposition, hypothesis and/or theory development was developed from the inter-relationship of the categories (Saldana, 2013). During this process, relevant categories were collated and sorted into different emerging themes. A theme is “a unifying or dominant idea in the data” (Savin-Baden & Major, 2013 p. 427). Themes were developed from lists of categories that had been identified in the data set. The list of categories and codes were compared and sorted in terms of similarities and differences. Categories that have similar meanings were refined and grouped together into themes that were non-repetitive and presented an accurate reflection of ideas in the categories. Likewise, the level of occurrence may have indicated the importance of the codes or categories to be merged into themes. In certain cases, codes which were “really rich and complex” were elevated to a theme (Braun et al., 2014). The difference between categories and themes is that a category can be a word or phrase that explicitly describe some segments of the data whereas a theme is a phrase or sentence that describes a more abstract process (Rossman & Rallis, 2011; Saldana, 2013).

Producing visual representation of initial themes may assist in classifying codes into different themes (Braun & Clarke, 2006). An example of an early thematic map for this research is presented in Figure 4-2.

Themes that were created based on five initial participants' data were presented to the researcher's supervisor for feedback on accuracy. Through this process, the validation of themes was implied during the early phase of the research, as suggested by Miles and Huberman (1994), by involving an external reviewer for the purpose of evaluation and identification of themes. It is important to ensure that the themes generated are relevant to the research questions, do not overlap and are internally coherent (Braun et al., 2014).

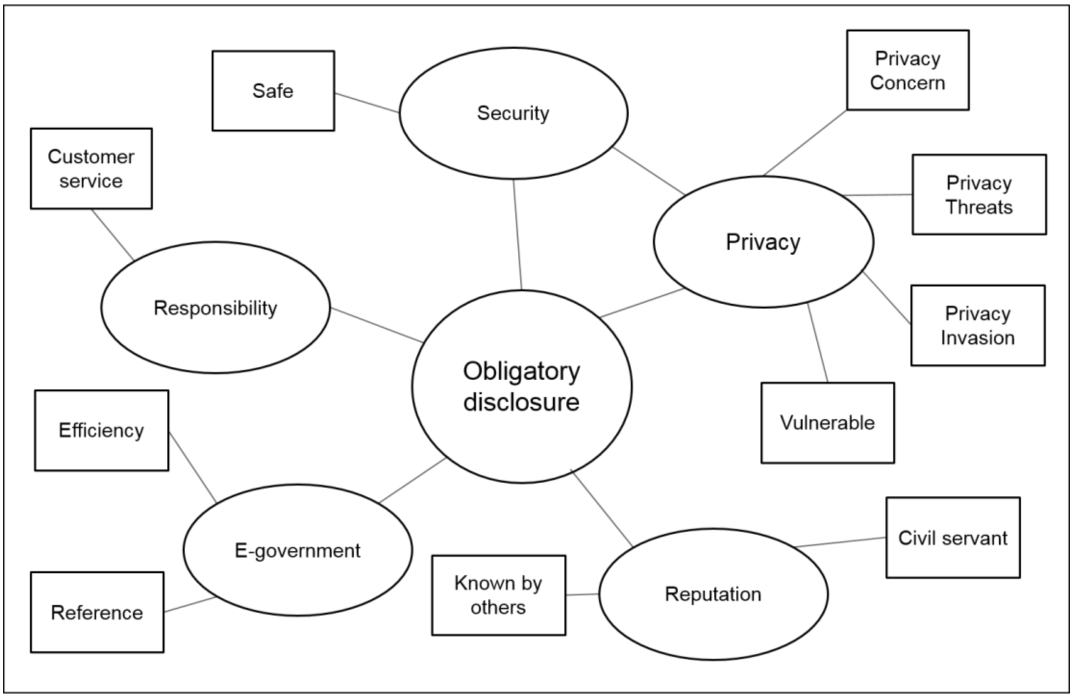
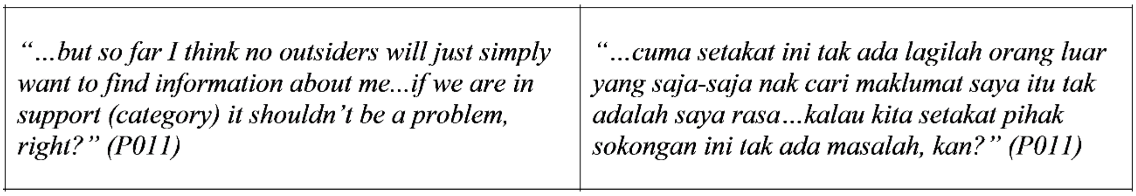


Figure 4-2: Initial thematic map for five participants

Up to this stage, the researcher was becoming more familiar with the coding process and proceeded with the codifying process (applied and reapplied code) for the remaining participants. All the transcripts were coded by employing Saldana's (2013) coding model, as shown in Figure 4-1, and analysed using the thematic analysis approach outlined by Braun and Clarke (2006).

As the study continued, the researcher encountered the re-arrangement and re-classification of coded data into either existing categories or by developing new categories to accommodate new codes. Some codes were recoded to ensure they captured the salient idea of the data. For example, the following excerpt:

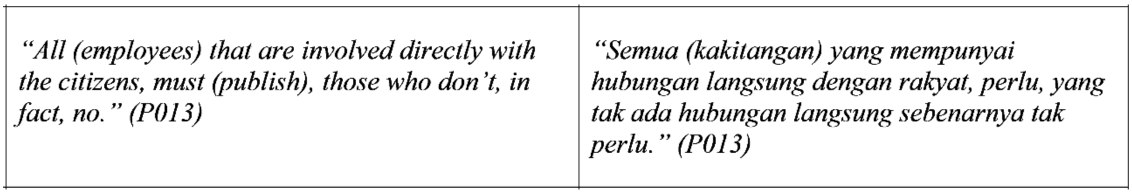


"...but so far I think no outsiders will just simply want to find information about me...if we are in support (category) it shouldn't be a problem, right?" (P011)	*"...cuma setakat ini tak ada lagilah orang luar yang saja-saja nak cari maklumat saya itu tak adalah saya rasa...kalau kita setakat pihak sokongan ini tak ada masalah, kan?" (P011)*

Box 4-1: Data analysis-P011

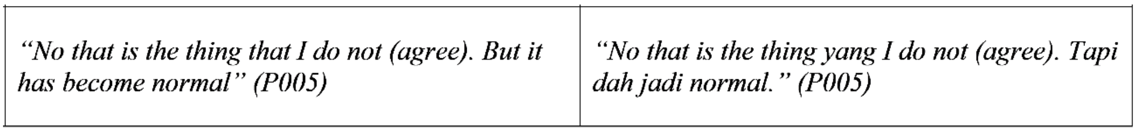
This quote from P011 was initially coded under *unimportant*. Then it was recoded to *not a target* to reflect the beliefs of the participant that he is not targeted by strangers or outsiders. The decision to recode *unimportant* was taken because the quote, although the highlighted elements of it being unimportant, the phrase *not a target* was chosen to represent a more relevant meaning in the context of the study. Here, the coding technique used was open coding to develop the code label, which the researcher composed as it displayed a better description of the information.

Another example of coding is to code using a participant's own words:



"All (employees) that are involved directly with the citizens, must (publish), those who don't, in fact, no." (P013)	*"Semua (kakitangan) yang mempunyai hubungan langsung dengan rakyat, perlu, yang tak ada hubungan langsung sebenarnya tak perlu." (P013)*

Box 4-2: Data analysis-P013



"No that is the thing that I do not (agree). But it has become normal" (P005)	*"No that is the thing yang I do not (agree). Tapi dah jadi normal." (P005)*

Box 4-3: Data analysis-P005

For participants P013, the data was coded as *dealings with public*. This code represented the participant's core reason in agreeing with the practice of obligatory disclosure. It captured the meaning appropriately and identified the interesting feature of the data. Therefore, it was decided to construct an in-vivo code to this data as they allowed the code to remain close to the data. Similarly, the categories were also reviewed to accurately reflect the meanings. This analysis is a continuous process where categories are brought together, organised and re-evaluated to ensure that it is relevant with the main idea of the category. The categories are also refined to ensure that it is non-repetitive and produces a more manageable data. Examples of the recoded categories are shown in Table 4-9.

Next, the interpretative analysis of the data is conducted to determine dominant ideas and themes emerging from the data. The main ideas (i.e. themes) that emerged from the categories should provide insights regarding the data and the meaning of it, which is related to the research questions (Braun & Clarke, 2006).

Table 4-9: Examples of the recoded categories

Initial categories	Recoded categories
False sense of security	Sense of security
Feeling safe	Harmless
Customer service	Increase service delivery

The themes were then reviewed with two levels of reviewing (Braun & Clarke, 2006). The first was to ensure that the themes fitted with the coded data and second involved checking the themes cohere meaningfully across the entire dataset. The researcher continuously assessed and examined the relevance of the themes during the analysis process, moving back and forth in order to ensure the ‘fittingness’ of the themes.

After collecting the reviews on themes, the researcher defined the themes. Writing a definition for each theme means identifying the essence of the theme and the dimensions within. It presents the analytical interpretation of the data and with the key concepts that surround the theme. The themes were then organised into a final thematic map and the results were reported in the next chapter.

CHAPTER 5

Results

This chapter reports on the results, which are divided into two sections. The first section presents the results from web content analysis, while the second section focuses on the semi-structured interviews.

5.1 Web content analysis

The population of this study are the Government websites in Malaysia from three different categories: a) federal agencies and ministries, b) state Government and c) local Government. Although the total number of available websites from this population is 182 (Malaysian Development Corporation, 2012), a sample size of 18 websites (9.9%) was selected for this study.

A purposive sampling technique was employed to select only the ‘best’ websites as evaluated in the MGPWA 2012 annual assessment. This would ensure only outstanding websites were included in this study. Not only that, these websites are not only foreseen to represent the organisations’ aspiration, but also the standard and quality expected for Malaysian Government’s websites.

This section presents the results of content analysis from 18 samples of top Malaysian Government websites where the coding was conducted from 9 November, 2013 to 10 December, 2013. Section 5.1.1 provides the descriptive results of government websites’ disclosure in general and of each three categories. Section 5.1.2 scrutinises the results, according to the attributes of personal information, by presenting a taxonomy of personal information disclosure. Personal information is then classified according to several categories in Section 5.1.3, and the result of this disclosure is presented. Section 5.1.4

looks into the medium specific features of websites that facilitate the disclosure of personal information.

5.1.1 Websites disclosure

This section describes the results from the content analysis of the selected Malaysian Government websites. The results were broken down into three, namely the disclosure of government websites with discussion on each category of government; the disclosure according to the categories of personal information and their attributes; and the website features that facilitate the disclosure of personal information. Before moving on to the results, it is appropriate to begin with the background of data analysis. Overall, a total of 4,965 web pages were coded from 21 websites (including three cross-coded websites). A total of 86 hours was spent by both coders with an average of four hours required by each coder to code a website.

As indicated previously, the focus of the website content analysis is to uncover the types of personal information from the websites but not the frequency. This technique also aims to explore the quality of personal information dissemination and how the disclosure from the websites transpired.

The numerical result (i.e. disclosure score and disclosure index) should be interpreted cautiously as there is a possibility of some elements of subjectivity. The disclosure score is assumed as an indication of quality of personal information disclosure. Higher scores can be translated into greater disclosure on the website. Content analysis researchers have been using this approach largely in assessing disclosure quality (Beattie et al., 2004; Botosan, 1997). Likewise, Gatfield et al. (1999) in their content analysis of university websites, interpreted that higher values correspond to deeper meaning while lower values correspond to lower meaning.

5.1.1.1 General disclosure assessment of government websites

In general, all categories of Malaysian Government websites, namely federal agencies, state agencies and local Government agencies, were found to disclose employees' personal information. In fact, all websites that were surveyed publish employees' personal information publicly.

In order to obtain a quantified measure for the level of disclosure, as has been mentioned before in section 3.4.1.4, the assigned numerical index was calculated. To evaluate the total disclosure for each category of government, a possible total score was calculated. The total disclosure score for each website was 48 from the 24 attributes of personal information. However, since *salary* was consistently missing from all of the websites, the attribute was removed from the calculation of the total possible score of disclosure. This resulted in the reduction of total possible score for each website from 48 to 46. By removing this attribute, the disclosure score presents the actual types of personal information found on the government websites and thus reflects on the quality of disclosure. The flexibility afforded by this methodological framework makes it easier for researchers to respond to opportunities and react to situations as they encountered. Therefore, the total possible score for a single category of government (consisting of six websites) was 276 instead of 288 (if salary was included).

Total possible score = Total possible score for a website x number of websites in a category

Higher scores can be assumed as having a higher level of disclosure (i.e. disclosing more of employees' information) while lower scores as having less disclosure of employees' personal information.

In general, Table 5-1 shows that the overall disclosure of employees' personal information attributes in 18 Malaysian Government websites was 60.7%. Based on the survey, state Government websites had the highest disclosure score followed by federal agencies websites. Meanwhile, local Government websites had the lowest disclosure score. The federal agencies websites' disclosure was 62.7%, the state Government websites' was 63.0%, whereas the local Government websites' was 56.5%. The scores between the state Government websites and the federal Government websites were almost similar, only separated by 0.7%. In contrast, the disclosure on local Government websites was found to be 6.5% lower than the highest disclosure recorded (i.e. state Government).

The disclosure of personal information of employees was expected, as this had been discovered during the pilot phase of the study. However, with the average disclosure score of 60.7%, it could suggest that the employees' personal information that was disclosed on government websites is on the high side. It could also be the case that it has been widely practiced, by acknowledging that the samples in this study are of the top ranked websites in Malaysia. Thus, they are considered as meeting the high quality of standards among Malaysian public sector websites.

Table 5-1: Website disclosure according to category

Category	Disclosure score	Disclosure index	Disclosure (%)
Federal	173	1.25	62.7
State	174	1.26	63.0
Local council	156	1.13	56.5
Mean	167.7	1.21	60.7

The disclosure index provides an indication of the extent of disclosure. As has been mentioned in section 3.4.1.4, a 0 score refers to non-disclosure, 1 for partial disclosure and 2 for full disclosure. To calculate the disclosure index for each category, the total disclosure score of each category was averaged by the total number of attributes, i.e. 138 (salary was not included).

Disclosure index = Disclosure score ÷ number of attributes

On average, Table 5-1 shows that the disclosure index for government websites was 1.21. This may indicate a partial to full level of disclosure of personal information. The disclosure index was highest for state Government followed closely by federal Government. Local Government websites appeared to produce a lower index with 1.13 and thus the least disclosed amount of personal information. Upon closer examination, several identified personal information attributes were not observed in local Government websites. Attributes such as *date of birth, birthplace, age, qualification, personal ID number* and *direction*, which had been coded in federal agencies' websites and state Government's websites were not detected in local Government websites. Therefore, this could be the reason why local Government websites scored much lower compared to the other categories.

From this data, those results seem to suggest that the Malaysian sample of government websites divulged a generous disclosure of personal information. A more detailed finding on each category of government is presented in the following section.

5.1.1.2 Federal agencies websites

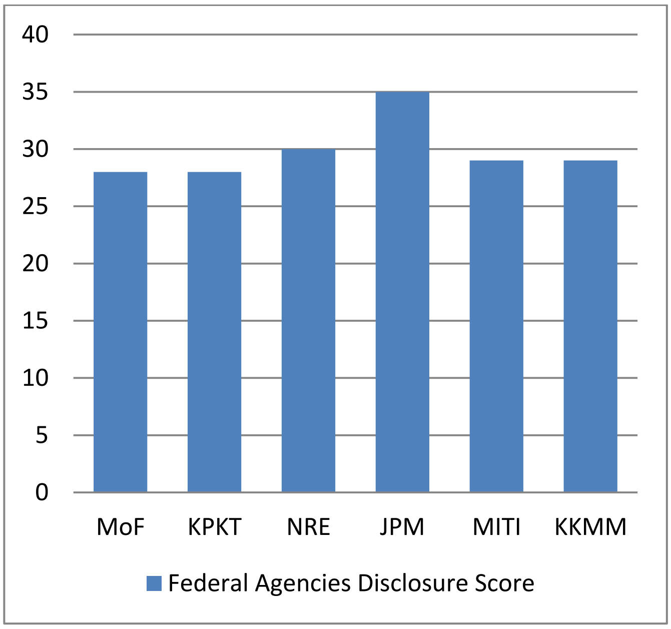


Figure 5-1: Federal agencies websites disclosure

For the federal agencies websites, six top ranked websites were selected. As mentioned earlier, the six websites are those that scored highest in their respective category for MGPWA 2012. The data shows that the disclosure for federal agencies websites was 58.7% to 73.9%. On average, the disclosure score was 62.7%. The highest disclosure score was recorded from the Prime Minister Department's (JPM) website while the lowest was from the Ministry of Finance (MoF) and the Ministry of Housing and Local Government (KPKT) websites.

Table 5-2: Federal agencies websites disclosure

Federal agencies	Disclosure score	Disclosure index	Disclosure (%)
MoF	27	1.17	58.7
KPKT	27	1.17	58.7
NRE	29	1.26	63.0
JPM	34	1.48	73.9
MITI	28	1.22	60.9
KKMM	28	1.22	60.9
Mean	28.8	1.25	62.7

Based on the disclosure index results, the highest index was 1.48 where it lies between partial disclosure and full disclosure. Except for JPM, other websites in this category were observed as having almost similar disclosure. As depicted in Table 5-2, the disclosure for JPM was 0.22 index point above the second highest website from this category and 0.31 from the lowest. The main reason for higher JPM disclosure is due to the discovery of employees' *date of birth*, *birthplace* and *ag*e from this website. Full disclosure of *date of birth* and *birthplace* as well as partial disclosure of *age* were recorded. In contrast, no other websites in this category were found to disclose these attributes. In fact, JPM scored the highest disclosure among all 18 government websites.

5.1.1.3 State Government websites

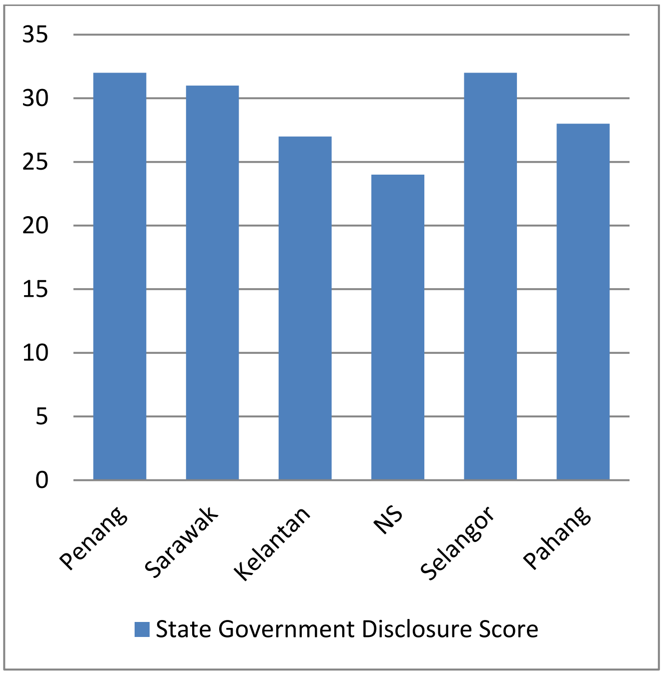


Figure 5-2: State Government websites disclosure

For the state Government category, six top ranked websites were selected, as previously. The highest disclosure score was recorded from Selangor and Penang with 69.6%, while the lowest disclosure was from State of Negeri Sembilan with 52.2%. The disclosure recorded for Negeri Sembilan was the lowest from all 18 samples. Other states' website disclosure was recorded between 58.7% and 69.9%.

Table 5-3: State Government websites disclosure

State Government	Disclosure score	Disclosure index	Disclosure (%)
Penang	32	1.39	69.6
Sarawak	31	1.35	67.4
Kelantan	27	1.17	58.7
Negeri Sembilan	24	1.04	52.2
Selangor	32	1.39	69.6
Pahang	28	1.22	60.9
Mean	29	1.26	63.1

The mean disclosure index for state Government websites was 1.26 with a mean disclosure score of 29.

5.1.1.4 Local Government websites

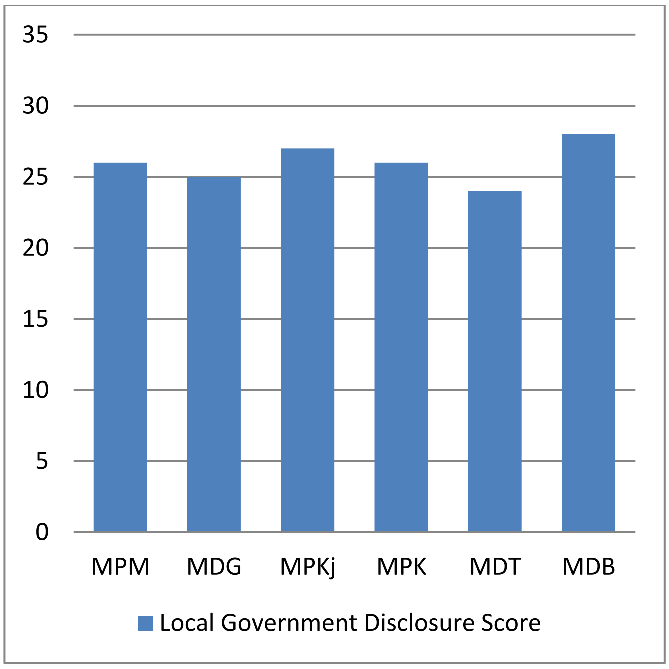


Figure 5-3: Local Government websites disclosure

From the local Government category, six top ranked websites were selected, as previously. The highest disclosure score was recorded from Besut District Council with 60.9%, while lowest disclosure score was from Tapah District Council with 52.2%.

Table 5-4: Local Government website disclosure

Local Government	Disclosure score	Disclosure index	Disclosure (%)
MPM	26	1.13	56.5
MDG	25	1.07	54.3
MPKj	27	1.17	58.7
MPK	26	1.13	56.5
MDT	24	1.04	52.2
MDB	28	1.22	60.9
Mean	**26**	**1.13**	**56.5**

Besut District Council recorded the highest disclosure index with 1.22, while Tapah District Council was with 1.04 as the lowest disclosure index. Tapah District Council also recorded the lowest disclosure score among the samples. The disparity between the highest and the lowest disclosure index was 0.18.

5.1.1.5 Summary

The highest disclosure index recorded was 1.48 (JPM) while the lowest was 1.04 (Negeri Sembilan and Tapah). It can be observed that there were variations in terms of how much disclosure each website produced, where on average the disclosure index was 1.21. Variations in disclosure among websites could suggest that each website may have their internal disclosure practice on information about employees. At the same time, on the macro level, obligatory disclosure was found to be generally the same across all categories of government. The lowest disclosure was recorded as 1.04 where this value resided slightly over 1. With regard to the coding index criteria, a score of 1 means that a particular attribute was found to be disclosed albeit not in a full form. However, this does not mean it is not identifiable. Thus, with the minimum score of 1.04 and the highest was 1.48, the disclosure of employees' personal information on Malaysian Government websites in this sample can be considered as favourable, in regards to disclosing employees' personal information.

More so, the inconsistencies of some attributes such as *date of birth, birthplace, age, qualification, personal ID number* and *direction* that were found in federal agencies and state Government websites but not in local Government websites could indicate the lack of a standard policy that covers across all categories of government. Thus, it can be suggested that while there could be a basic guideline or understanding on obligatory disclosure that all government websites seem to subscribe to, at the same time, each agency/organisation can establish their own internal practice.

Overall, results indicated that personal information of employees was abundantly discovered across all levels of government categories i.e. federal, state or local. With the average disclosure index of 1.21, government websites can be assumed to disclose information that is sufficient to identify individuals i.e. employees. The extent of disclosure for each attribute of personal information is presented in the next section.

5.1.2 Disclosure of personal information

One of the main objectives of this research is to discover the scope of personal information published on government websites. This section addresses part of the first research question on the types of personal information attributes that can be found on government websites. Out of 24 personal information attributes that were listed in the codebook, 23 personal information attributes were discovered from Malaysian public organisation websites. The only attribute that was not found on the Malaysian Government websites is *salary*. *Salary* was included in the codebook after being discovered in the UK's local Government websites during the pilot study. Besides *salary*, other attributes were available and coded accordingly.

Table 5-5: Personal information taxonomy found on public organisation websites

Categories of personal information	Information attributes
Personal attributes Information that could be directly related or associated with an individual	1. Full name 2. Photographic image 3. Gender 4. Ethnicity 5. Date of birth 6. Place of birth 7. Marital status 8. Age 9. Personal ID number
Personal achievement information Information regarding the specific accomplishment and success	10. Education qualification 11. Award
Employment information Information about full time work	12. Working position 13. Working grade 14. Work scope
Contact information Information that could be used to communicate with an individual	15. Email address 16. Telephone number 17. Fax number
Geographical information Information regarding the specific location of people	18. Physical address 19. Direction 20. Location
Timeliness information Information regarding when any events or activities occur or references to specific time	21. Pre-event 22. Post-event 23. Opening hours

This study further developed a taxonomy of employees' personal information that can be drawn out publicly from government websites as well as classifying different types of personal information into categories. The categories provide a common classification of personal information according to their specific functions. The objective of establishing a taxonomy is to determine the range of employees' personal information that can be gathered publicly on the Internet from a specific type of website (i.e. government websites). Table 5-5 presents the taxonomy of personal information and its category drawn from this study.

From the data, 23 different types of personal information were categorised into six categories. The first category is *personal attributes*. It is defined as any information that can be directly used to identify an individual. This information is vital in identifying individuals, as it could potentially identify a specific individual. The second category is information about *personal achievement*. This category presents information regarding individuals' specific accomplishments or recognition. *Employment* information is information that relates to an individual's job or occupational information. In this study, employment information was limited to employees' full time jobs. The fourth category is *contact* information by which any information that can be used to contact an individual. As for the fifth category, *geographical* information involves any information that can notify the whereabouts of an individual. The final category is *timeliness* which provides information about the occurrence of events or activities. As shown in Table 5-6, the taxonomy of personal information unveils the range of personal information that can be elicited from government websites.

To measure the extent of disclosure, this study applied a coding index. Each personal information attribute was coded with a score of 0, 1, or 2 according to the extent of disclosure. 0 refers to non-disclosure where no occurrence of the attributes was found, 1 refers to partial disclosure where some or part of the attributes were published on the websites and 2 refers to full disclosure where complete information of attributes was disclosed on the website.

Table 5-6: Distribution of personal information attributes published

No	Attributes	No of websites					
		Full disclosure	(%)	Partial disclosure	(%)	Non-disclosure	(%)
1	Full name	18	100	-	-	-	-
2	Photographic Image	17	94.4	1	5.6	-	-
3	Ethnicity	-	-	18	100	-	-
4	Gender	18	100	-	-	-	-
5	Date of birth	3	16.7	-	-	15	83.3
6	Birth place	2	11.1	-	-	16	88.9
7	Age	-	-	2	11.1	16	88.9
8	Marital status		-	18	100	-	-
9	Qualification	4	22.2	8	44.5	6	33.3
10	Award	-	-	14	77.8	4	22.2
11	Personal ID	2	11.1	-	-	16	88.9
12	Work position	18	100	-	-	-	-
13	Work grade	17	94.4	-	-	1	5.6
14	Work scope	3	16.7	15	83.3	-	-
15	Email address	4	22.2	14	77.8	-	-
16	Telephone no	12	66.7	6	33.3	-	-
17	Fax no	7	38.9	11	61.1	-	-
18	Physical address	11	61.1	7	38.9	-	-
19	Direction	1	5.55	3	16.7	14	77.75
20	Location	15	83.3	2	11.1	1	5.6
21	Pre-event	14	77.8	1	5.6	3	16.7
22	Post-event	17	94.4	1	5.6	-	-
23	Opening hours	6	33.3	4	22.2	8	44.5

Table 5-6 illustrates the extent of disclosure according to the personal information attributes found on the websites. *Full name, ethnicity, gender, working position, photographic image, marital status, work scope, email address, telephone number, fax number, physical address* and *post-event* information were found in all 18 websites. These 12 attributes consisted more than half of the total personal information attributes that were investigated in this study. In addition, another three attributes were found in more than 83% of the websites, i.e. *working grade, location, and pre-event*. In total, 15 attributes were easily available from most of the websites. Nevertheless, the four attributes that were least disclosed were *age, personal identification number, direction,* and *opening hours*.

Sensitive information, such as *date of birth*, was found in 16.7% of the websites while education *qualification* was found in 68.7% of the websites. Marital status was found in all of the websites, although only partial disclosure was noticed. Another three personal attributes, such as *birthplace, age* and *personal ID number*, were each found in 11.1% of the websites. Both *birthplace* and *personal ID number* were found to be fully disclosed while information about *age* was partially disclosed.

5.1.2.1 Summary

It was discovered that up to 23 different attributes of personal information can be found from government websites as displayed in Table 5-6. The taxonomy revealed six categories of personal information which can be used to capture a rich data set about an individual. These attributes can be used to identify an employee just by visiting his/her organisation's website.

It is also important to highlight *employer information* as another attribute that is available on the websites. Although this attribute could reside within the *employment* information category, it was not included in the taxonomy because by the nature of the organisation's website, this information is considered assured information. If this information were to be included, then the total number of attributes found on government websites would be 24.

5.1.3 Disclosure according to categories of personal information

From the total of 23 personal information attributes, six categories of such information were developed as shown in Table 4-3. Of these, the *personal attributes* category contributed 39.2% of personal information that was disclosed; hence, the largest category compared to others. Nine attributes contributed to this category. The next category that comprised 13% of personal information was *contact information*, *employment, geographical* and *timeliness* categories. The *personal achievement* category, with two attributes, was the smallest category of personal information.

Table 5-7: Distribution of personal information attributes and its category

Categories	Number of attributes	Disclosure (%)
Personal attributes	9	39.2
Personal achievement	2	8.8
Employment	3	13.0
Contact	3	13.0
Geographical	3	13.0
Timeliness	3	13.0

Thus, it can be seen that publication of employees' information on their organisations' website largely consists of employees' *personal attributes*. The above information presented categories of personal information and their contribution to the amount of disclosure. Nevertheless, the depth of disclosure of each category was not scrutinised here. To examine this, it is useful to utilise the disclosure index that was employed. To obtain the disclosure index for each category, the scores for each attribute (within each category) were summated and averaged (by dividing with the total number of websites i.e. 18). Next, the scores were divided according to the number of attributes in each category. The category with a higher index represents higher disclosure and vice versa (Gatfield et al., 1999). Table 5-7 presents the results.

Table 5-8 presents the disclosure index according to categories. Results showed that the *employment* category has the highest disclosure index with 1.69, which indicates that employment information was disclosed in a more complete fashion on public organisation websites compared to other categories. However, this could be expected from an organisation website, such as the government websites that is to provide the public with the employment details of their employees. Next was *timeliness* with a disclosure index of 1.48, followed by *contact* information (1.43), *geographical information* (1.22), *personal attributes* (0.98) and *personal achievement* (0.83). *Personal attributes* that scored highest with 159 interestingly had a lower disclosure index.

Table 5-8: Disclosure of personal information according to category

Categories	Disclosure score	Disclosure index
Personal attributes	159	0.98
Personal achievement	30	0.83
Employment	91	1.69
Contact	77	1.43
Geographical	66	1.22
Timeliness	80	1.48

Based on this result, a higher disclosure score does not necessarily mean that it will produce a higher index. Although a higher score may be contributed by a high disclosure from certain attributes, other attributes from this category might have a lower score and this could affect the outcome of the disclosure index for that particular category. Discussions on each category of personal information and its disclosure score are presented in the next few sections.

5.1.3.1 Personal attributes category

This category consists of nine attributes, i.e. *full name, photographic image, ethnicity, gender, date of birth, birthplace, age, marital status,* and *personal ID*.

The highest disclosure was found to be the *full name*, *gender* and *photographic image*. This was consistently available on all websites. Full disclosure of *full name* was evidently noticeable. Findings also discovered that the individual's names found were all the pairings of forenames and surnames. Any name with a forename and surname was coded as full disclosure. In Malaysia, *full name* is known by having an individual's name together with the father's name or the family name. It is uncommon to classify an individual's name by first, second or third name. First name is normally considered as the individual's given name, although it has more than one word. For ethnic Malay, *bin* or *b.* and *binti* or *bt.* is included in the full name. *bin* means 'son of' while *binti* means 'daughter of'. Likewise, for ethnic Indian or Bumiputeras, *a/l* or *a/p* means 'son of' or 'daughter of' respectively is normally included in the full name. As an example, for Zulfadhli Hashim bin Ismail, it is common to consider the individual's name is Zulfadhli

Hashim instead of separating those two with a first name or a second name. Also *bin* refers to 'son of' and Ismail is the father's name. From this *full name*, it is known that Zulfadhli Hashim is the son of Ismail. If such name is available in official government channels, the names of other employees were also considered as individuals' real names.

Similar findings were revealed for *photographic image*. All websites were found to clearly disclose photographic images of employees which can be used to link to individuals. Images were largely enumerated from the directories of staff, news, activities, reports and organisational charts. Most of the images were of passport type which focused on individuals' faces for easy recognition.

Table 5-9: Personal attributes disclosure index

Personal attributes	Disclosure score	Disclosure index
Full name	36	2.0
Photographic Image	35	1.9
Ethnicity	18	1.0
Gender	36	2.0
Date of birth	6	0.3
Birthplace	4	0.2
Age	2	0.1
Marital status	18	1.0
Personal ID	4	0.2

Disclosure of *gender* was noticeable in all websites. While there was no clear mention of an individual's gender, this attribute can easily be inferred from other attributes. For example, from the combination of a *full name* (Lansley & Longley, 2016) and a *photographic image*, the *gender* can be identified. Moreover, explicit *gender* information such as 'son of' and 'daughter of' provides cues for an individual's *gender*. Furthermore, by referring to an individual's *photographic image,* the *gender* can easily be deduced because visual image provides another important characteristic of a *gender*. Thus, *gender* attributes were coded as to be fully disclosed and were found to be available on all websites.

Ethnicity information of employees could be drawn from all websites. Despite none of the websites stating employees' *ethnicity* explicitly, this attribute is inferable from the combination of *full name* and *photographic image*. Researchers have shown that information on ethnicity can be inferred by using names to divide population into groups of common origin (Mateos, 2007; Nanchahal et al., 2001). In Malaysia, generally there are three major ethnic groups, namely Malay, Chinese, and Indian, with another more than 30 sub-groups - such as Dayak, Iban, Bidayuh, Melanau and Orang Ulu – that are largely concentrated in the east part of Malaysia. Each ethnic group has specific naming practices which can reflect social and cultural background (Mateos et al., 2011; Treeratpituk & Giles, 2012). In view of this, *ethnicity* was considered to be partially disclosed on all websites because although there was no clear indication of an individual's ethnicity, it is highly possible to profile it according to individuals.

Marital status was not revealed *per se*, but this information can be derived from the individual's salutation. Findings from content analysis found that the salutation of 'Mrs.' (*Puan*/*Pn.* in Malay) was available in front of the majority of female employees' names. Indirectly, this information implies that this person is married and thus revealed her marital status. Similarly, for unmarried women, Miss (*Cik*) was found to be added in front of a female employee's name. However, similar conclusion cannot be made for men where 'Mr.' does not give any meaning towards the marital status. As such, information about *marital status* was coded as partially disclosed and found in all websites.

Another four attributes were found to have a lower disclosure index, i.e. less than 0.4. However, the existence of such information in government websites cannot be taken lightly especially when it is considered sensitive information (Gupta et al., 2010; Nosko et al., 2010). Employees' *date of birth* was found in three websites with full disclosure of date, month and year, while employees' *birthplace* and *personal ID* number were available on two websites with full disclosure. *Age* was found to be partially disclosed on two websites where information about employees' year of birth was published.

5.1.3.2 Personal achievement category

Two attributes contributed to this category. Both of the attributes were *education qualification* and *state award*. Both attributes scored lower than one on the index with *education qualification* scored 0.89 and *state award* with 0.78, accordingly. Information on the qualifications of employees was found in four websites, clearly mentioning the institutions, courses, and years of graduation. In addition, eight websites partially mentioned some of the qualifications. Most of the eight websites displayed a doctorate title in front of their employees' names. The title *'Dr.'* gave an indication of a certain academic level of achievement of an individual.

Table 5-10: Personal achievement disclosure index

Personal achievement attributes	Disclosure score	Disclosure index
Education qualification	16	0.89
State award	14	0.78

State award mostly referred to the 'Datukship' award, which is an honorific title awarded by the Sultan of a state or the King in Malaysia on their birthdays. It is conferred to someone that has contributed to the country or the state. This title portrays the high social status of the title bearer (Hashim, 2007). 14 websites listed this information along with their employees' names, while the rest did not. It can be suggested that those websites that did not disclose this information may possibly have no current employee holding the state award. Notwithstanding, this attribute is most likely to be revealed if any of the employees were awarded with this title.

5.1.3.3 Employment attributes category

This category consists of four attributes which are *work position, working grade,* and *work scope*. *Working position* of individuals was found to be fully disclosed in every website. Among the positions that were discovered were Director General, Assistant Director, Administrative Assistant, Technical Assistant and Driver. Another attribute with a high disclosure index is staff's *working grade*, which appeared on all websites except for one. Staff's *working grade* normally is assigned with a letter followed by a number. For example, grade N17 - where N is the classification of scheme, and here it means administrative. The number that accompanies it denotes the work level and the salary scale of an employee. In the Malaysian civil service the support category is denoted with grade 1 to grade 40; management and professional category is grade 41 to grade 54; and the top management category is grade JUSA C to Turus I.

Employees' *work scope* was found in three websites with full disclosure, while 15 websites disclosed it partially. Full disclosure of *work scope* is where it states the role and job responsibilities of an employee, while partial disclosure specifies the role and job responsibilities of a certain unit or a division to which an employee is attached. Based on the result, it can be suggested that information about *working position* and *working grade* was revealed in most of the Malaysian Government websites with a full disclosure. Summary of the *employment attributes* disclosure index is presented in Table 5-11.

Table 5-11: Employment attributes disclosure index

Employment attributes	Disclosure score	Disclosure index
Work Position	36	2.0
Work Grade	34	1.8
Work Scope	21	1.2

5.1.3.4 Contact information attributes category

Contact information attributes comprised of *email address, telephone number,* and *fax number*. All of these attributes were detected in every website. In fact, all *contact information* attributes scored above one in the disclosure index which could suggest the importance of this category of information to the organisation. *Telephone number* scored highest in this category with 1.7. Besides official landline telephone numbers, mobile phone numbers were also discovered to be published on two-third of the websites. Another mode of communication is via fax. *Fax number* that can be directed to contact employees either directly (full disclosure) or indirectly (via unit/division, partial disclosure) was identified during the data collection.

Table 5-12: Contact information disclosure index

Contact information attributes	Disclosure score	Disclosure index
Email address	22	1.2
Telephone number	30	1.7
Fax number	25	1.4

Email address was discovered in all websites, but it scored a lower index compared to *fax number*. The reason behind this is because a full disclosure score was awarded when a personal email address was listed, while partial disclosure was awarded when an organisation's email was detected. Based on the data, four websites were found to publish employees' personal email address whereas the rest published official email address of employees.

5.1.3.5 Geographical attributes category

Physical address, direction to organisation and *location* of organisation were categorised as geographical attributes. This category of information provides information about the place or point and how to reach the place. *Location* information has the highest disclosure index. It basically answers the 'where is the office' question. In other words, this information particularly tells website users the office of an individual. A score of two is awarded when the information is up to the accuracy of level or block while a score of one is when the accuracy is up to a building or complex. This information was available in 94% of the websites surveyed.

Information on *physical address* was found in all 18 websites. This information answers the 'where is the organisation' question. A complete address of the organisation including its map was considered a full disclosure while disclosure of a complete address as partial disclosure. *Direction* refers to information about 'how to reach an organisation'. Websites that display complete directions to an organisation with supporting information such as parking space or public transportation will get a full score while websites that publish any directional guide to direct users will get one mark. Interestingly, only four websites had included some *direction* information to their organisations.

Table 5-13: Geographical attributes disclosure index

Geographical attributes	Disclosure score	Disclosure index
Physical address	29	1.6
Direction	5	0.3
Location	32	1.8

5.1.3.6 Timeliness attributes category

Timeliness attributes are formed of *pre-event, post-event* and *opening hours*. In the timeliness category, the concern is around information about an occurring activity. This information will inform website users regarding an event that will happen and or one that had taken place within the organisation. Information coded in this category was among others ranging from the organisation's monthly assemblies, announcements, publications (e.g. bulletins, reports), and minutes of meetings to the date of the documents being written. *Pre-event* is information about any event or activity that will take place or scheduled to take place while *post-event* is information about any event or activity that has occurred. *Opening hours* refers to the organisation's opening hours for dealings with the public. Highest *timeliness* attributes disclosure index was *post-event* at 1.9 and this information can be found in all websites. Following this was *pre-event* with 1.6 and finally, information about *opening hours* with 0.9. Table 5-14 presents the timeliness attributes disclosure index.

Table 5-14: Timeliness attributes disclosure index

Timeliness attributes	Disclosure score	Disclosure index
Pre-event	29	1.6
Post-event	35	1.9
Opening hours	16	0.9

5.1.3.7 Summary

This section summarises the results from section 5.1.3. The disclosure of *personal attributes* was found to be the highest among other categories of personal information with nine attributes that reached nearly 40% components of personal information. Other categories were found to reveal between two and three attributes each, where a wide disparity of disclosure between the *personal attributes* category and the other categories of personal information was observed.

With respect to the high number of attributes detected within *personal attributes*, its disclosure score was the highest compared to the rest. Next was the *employment* category, followed by *timeliness, contact, geographical* and *personal achievement*. While *personal attributes* obtained the highest score for disclosure, its disclosure index was among the lowest. This could mean that although *personal attributes* disclosure was found to be significantly higher on government websites, its quality, in general, was low (considering within the category). This could be due to the fact that although some attributes were consistently detected, others were only slightly available in a few websites. As presented in Table 5-9, five attributes from this category scored one and above for the disclosure index while four attributes scored less than 0.3.

Highest disclosure index was recorded from the *employment* category with a score of 1.69 although it only consisted of three attributes. Employment information such as *work position, work grade* and *work scope* was disclosed in detail to website users consistently across all attributes.

In summary, the extent of disclosure for certain attributes of personal information was intriguing in the sense that various categories of personal information were disclosed. Equally important was the discovery of few personal attributes which were less related with the function of the organisations.

5.1.4 Website features

This section also addresses the first research question on exploring how employees' personal information was disclosed via obligatory disclosure. Government websites offer certain website features to assist citizens when browsing through the organisation's website. As suggested by Neuendorf (2002), the specific features of the medium can be considered in the content analysis based on the research aims and objectives. This study had identified a few website features that were available and dichotomously coded. A dichotomous coding is a coding that has two possible values. In this case, the feature is coded as 1 if it is present and 0 when it is not. Features that are coded are investigated further according to the coding guidelines.

Table 5-15 presents the selected features of government websites which indicate the quality of information dissemination, particularly referring to employees' personal information. As shown, most of the website features were found in almost all government websites. *Employees search function, general search function, directory of staff, organisation chart*, *privacy policy* and *security policy* were found in all websites while *disclaimers* were found in 94.4% of the websites. Other specific features, such as *terms and condition, date of last update, calendar* and *auto-translation*, were identified in more than 60% of the websites except for one feature i.e. the *personal information charter* that was noticeably absent.

Table 5-15: Features of government websites

No	Features	No of websites			
		Present	(%)	Not Present	(%)
1	Employees' search function	18	100%	-	-
2	General search function	18	100%		
3	Directory of staff	18	100%	-	-
4	Organisation chart	18	100%	-	-
5	Privacy Policy	18	100%	-	-
6	Security Policy	18	100%	-	-
7	Disclaimer	17	94.4%	1	5.6%
8	Personal information charter	0	0%	0	0%
9	Terms and condition	11	61.1%	7	38.9%
10	Date of last updated	12	66.7%	6	33.3%
11	Calendar	14	77.8%	4	22.2%
12	Auto translation	11	61.1%	7	38.9%

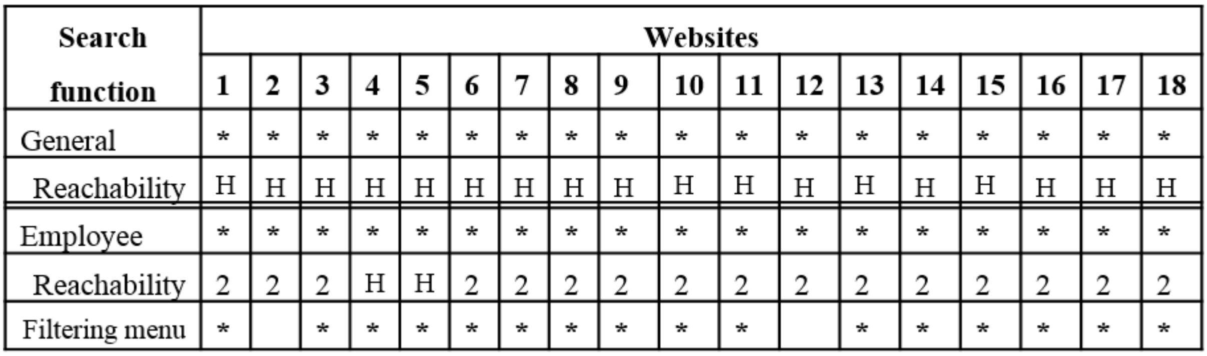
The personal information charter explains to website users the processing of personal information. This feature was included after being discovered during the pilot phase of the study. Nevertheless, only UK-based government websites were found to include this charter onto their websites. Thus, the result from the content analysis was found to be consistent with the findings from the pilot study where a *personal information charter* was not available in Malaysian Government websites.

5.1.4.1 Search features

Based on the content analysis, it was discovered that all websites provide two different types of search function to assist visitors or public in searching for information. One, is the general search function that is used to find information posted within the website, and second is the more advance search function that is specifically dedicated to searching employees. Coders were instructed to code both the general, and the employees' search function. If the features were available, coders were required to observe the discoverability of the search function. They had to observe the distance of that function from the homepage. Basically, the nearer the distance from the homepage made the functions easily noticeable and discoverable. Thus from the data, all websites offered general search and employee search functions to their users.

The general search box function was found to be available in all government websites and it was located at the homepage. The search interface is a single free text search to look for information within the website. Coders were asked to enter any one employee's name in order to assess the ability to search for employees. Results from the search revealed that the general search function cannot search for a specific employee. However, employees' information was found to be listed in the search result if the employee is highlighted in news, events or announcements.

Table 5-16: Search function on websites



Search function	Websites																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
General	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Reachability	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
Employee	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Reachability	2	2	2	H	H	2	2	2	2	2	2	2	2	2	2	2	2	2
Filtering menu	*		*	*	*	*	*	*	*	*	*		*	*	*	*	*	*

**: indicate availability on website*
H: homepage
2: second level from homepage

The employee search function was also found to be present in all websites (100%). This search function is specifically dedicated to searching for employees via a keyword (i.e. name). It is located on the second level from the homepage (i.e. one-click away) on most of the websites (89%). To access this function, users can locate the link from the homepage itself, and with a single click users are able to reach the feature. As a result, this feature is easily accessible from the homepage. In fact, two websites had organised their search feature to embed this function on the homepage, thus allowing higher visibility for employee searches.

Another characteristic observed was that this type of search function is more advanced, since it is equipped with a filtering menu option for more precise queries. It was noticeable that all of the websites except for two provided a filtering option for searching employees. Most of the filtering options offered are categorised according to name, position, department/section/unit and email address. A filtering menu allows for specific searches according to criteria requirement. Additionally, several organisation websites allow filtering up to the unit level while others up to the department level. This can mean that website users are able to observe a specific unit/division/department within an organisation, including the manpower that runs the specific unit/division/department.

Generally, this implies that within a single website there are two different search functions available for website users, i.e. one is the general search for content of the website while another is specifically for employee search. By having these functions closer to the homepage as shown in Table 5-16, the visibility of the functions is increased and users' direct access to the required information is performed quickly and easily.

5.1.4.2 Online staff directory

Similar findings were observed with the online staff directory. This feature is explicitly available in all websites surveyed. The online staff directory contains a list of staff and employees that are currently employed by the organisation. It listed all employed staff with their personal information, such as name, photograph, job title, telephone number, email address, unit/department, staff work scope and organisation's address. The employees are displayed either alphabetically according to their names, which is commonly found in large organisations such as the ministries or federal agencies, or by arranging them according to departments or units.

The link to the staff directory can be found on most of the organisations' homepage. The directory is located on the second level below the homepage and it can be accessed with a single click. However, on one website, the staff directory is located at the second level below the homepage - although the link to it appears on the homepage. In short, the staff directory is conveniently reachable from the homepage.

One interesting finding was a standard design pattern observed for both search functionality and online staff directory. Both features were found to be structured together in the same webpage. This allows website users to take advantage of the capabilities that both features can offer. It facilitates users in gathering a better picture of employees' personal information from the website.

With the availability of the online staff directory, this content analysis was able to identify the number of individuals working within a particular organisation. Details are shown below. In total, 13,410 individuals were identified from 18 government websites. State Government published 8,598 staff, followed by ministries and federal agencies with 3,816 staff and local Government with 996 staff. On average, one website discloses 745 individuals (i.e. government employees) on the Internet.

It is clear that local Government, which is the smallest category (in terms of organisation size), relative to the other two government categories, disclosed the smallest number of staff. Gerik District Council has the lowest number of employees disclosed in this study at 47, while the Negeri Sembilan state Government website disclosed 3,793 employees which makes it the highest among the 18 websites surveyed.

Although the number of individuals disclosed can be assumed as representing the total strength of an organisation, this research did not attempt to clarify whether the number of employees disclosed is equivalent to the total strength of the organisation, because it is beyond the scope of the study.

Table 5-17: Total number of employees disclosed on official government websites

Government categories	Agencies	Individuals disclosed	Total individuals
Ministries/Federal agencies	NRE	464	3816
	MoF	1194	
	KPKT	712	
	JPM	500	
	MITI	344	
	KPKK	602	
State Government	Penang	2125	8598
	Sarawak	588	
	Kelantan	1119	
	NS	3793	
	Selangor	537	
	Pahang	436	
Local Government	MPM	178	996
	MDG	47	
	MPKj	149	
	MPK	401	
	MDT	70	
	MDB	151	

5.1.4.3 Organisation chart

The organisation chart was disclosed on all websites. The content analysis discovered that published organisation charts can be categorised into two, which are a) the general organisational chart and b) the detailed organisational chart. The general organisational chart is defined as a chart that lists the structure of the whole organisation i.e. department/divisions within the organisation and without mentioning any post holder or employee. On the other hand, a detailed organisation chart is a chart that listed individuals and their corresponding personal information. Five websites (27.8%) chose to publish only their general organisation chart while 13 websites (72%) publish a detailed one.

Twelve websites (66.7%) publish both general and detailed organisational charts. One website publishes only their detailed organisational chart.

In addition, the results showed that a detailed organisational chart is another source of employees' personal information disclosure. Nine personal information attributes were able to be identified from the organisation chart, which comprised 39.1% of the total personal information attributes found on government websites. *Full name, photographic image, ethnicity,* and *gender* from the personal attributes category, *qualification* and *award* from the personal achievement category and *work position, work grade and work scope from* the employment category were the attributes discovered. The distribution of organisational chart disclosure is presented in Table 5-18.

Full name represents the most disclosed attribute and was available in all detailed organisation charts. Half of the websites revealed their employees' *photographs* on the chart. The *photographs* were similar to passport photos, where they portrayed clear and identifiable images of the employees. The photographs were displayed according to specific individuals in relation to their position in the organisation. The structural nature of a chart exhibits employees' hierarchical positions.

Whilst *gender* and *ethnicity* were not explicitly stated, they could be identified in 13 websites (72%) by inferring from other attributes, either from the title (e.g. Mr/Mrs), middle name (*bin*, son of) or visual image.

Working position appeared in 11 websites. Among the examples of job title were Director of Administration, Senior Assistant Director, Administrative Assistant and Finance Assistant. Nonetheless, three websites that published a detailed organisation chart did not include any *working position* information.

Qualification and *award* were found in 10 websites. Apparently, qualification information was limited to information regarding PhD qualification, stated as salutations accompanying the employees' names. Similarly, awards were identified from the salutations to the employees and limited to the state or federal titles conferred by the King or Sultan.

Working grade was found in half (50%) of the total websites surveyed while w*ork scope* was the least piece of information provided on organisational charts.

Table 5-18: Distribution of organisation chart disclosure

Organisation chart	Websites																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a. General	*	*	*	*	*	*	*		*	*	*	*	*	*	*	*	*	*
b. Detailed		*	*	*	*	*	*	*	*			*		*		*	*	*
Name		*	*	*	*	*	*	*	*			*		*		*	*	*
Photograph		*	*		*	*		*	*					*		*	*	
Ethnicity		*	*	*	*	*	*	*	*			*		*		*	*	*
Gender		*	*	*	*	*	*	*	*			*		*		*	*	*
Qualification		*	*	*	*	*	*	*	*			*				*		
Award		*	*	*	*	*	*	*	*			*				*		
Position		*	*	*		*	*	*				*	*			*	*	*
Grade		*	*	*		*			*			*	*	*		*		
Work scope					*	*	*		*								*	

** indicate availability on website*

In general, an organisation chart may be considered as an important element in public organisation websites, because evidently it was found embedded in all of their official sites. The fact that more than 70% of government websites published a detailed organisation chart could imply that this feature is widely published, and a possible source of personal information disclosure. Nine attributes can be acquired from a single organisation chart. Besides that, the hierarchical characteristic of a chart provides information on the employees' jobs and responsibilities. This information will assist in identifying the structural power within the organisation. Key individuals and important post holders are easily identified.

5.1.4.4 Privacy policy

Privacy policy on websites was found to assist in alleviating the privacy concerns of website users (Andrade et al., 2002). In the field of e-commerce, organisations that published a privacy policy on their websites were found to perceive higher trust of users

(Kim et al., 2008). Hence, this study decided to observe privacy policy on government websites since it has been demonstrated to have an impact on users' privacy concerns.

All websites surveyed were found to have included privacy policies. The policy is located in the homepage and situated at the footer of the webpage. Details of the privacy policy can be accessed in a single click from the homepage. From sampled websites, it was discovered that the privacy policy was intended to protect users or visitors to government websites about the organisation's data collection and practices. This was clearly stated in the privacy policy:

> ***"Your Privacy***
> *This page explains our privacy policy which includes the use and protection of any information submitted by visitors.*
>
> *If you choose to make any transaction or send an e-mail which contains personal information, this information may be shared where necessary with other Government agencies so as to serve you in the most efficient and effective manner. An example might be in terms of resolving or addressing complaints that require escalation to other Government agencies."*

Specific reference was also made to users' personal information, with the assurance of not collecting any visitor's personal information when using the website.

> ***"Information Collected***
> *No personal information will be gathered while you are using this website except for information given via e-mail."*

As this study was interested in employees' personal information, the privacy policies were analysed from the internal users' perspectives i.e. the employees. As presented above, the focus of the policy was geared towards the website visitors' privacy and their personal information. While all government websites placed and disclosed their privacy policies clearly, the policies did not attempt to cover information published on the websites. As this research was focusing on employees' personal information, none of the privacy policies made any reference to this type of information. Therefore, protection of personal information published on the websites was not observed.

5.1.4.5 Security policy

Security policy was also found in all websites. Some websites stated security policy as a standalone policy while some combined it with privacy policy. Security policy was also found on the homepage of the organisation and located at the footer of the page in a similar location with the privacy policy. The security policy statement consisted of two elements which are *data protection* and *storage security*. The statements as viewed on the websites were;

> ***"Data Protection***
> *The latest technology includes data encryption to protect data and compliance to strict security standards are maintained to prevent unauthorised access."*

> ***"Storage Security***
> *All electronic storage and personal data transaction are protected and stored using appropriate security technology"*

Therefore, security policy serves as a pledge to protect and store data with the standard security guidelines in order to gain the trust of website users. The policy was found to provide assurance to website users that adequate measures have been taken in order to protect data against intrusion and unauthorised access. Nevertheless, protection for information published on the websites was not addressed by this policy.

5.1.4.6 Disclaimer

It was observed that all websites stated a disclaimer notice on their homepage. The disclaimer notice was similar for all websites. It reads;

> *"The Government of Malaysia and (name of the organisation) is not liable for any loss or damage caused by the usage of any information obtained from this website."*

In addition, there was also another version of the disclaimer which dealt with the auto-translation features which some of the websites had embedded. The auto-translation feature was adopted from Google Translate and embedded on the websites. Two websites, i.e. one from the ministry and another from a local Government, displayed an additional disclaimer statement in their notice specifying that they are not responsible for the accuracy of the translation and are not liable for any loss or damage caused by usage. Five websites positioned the disclaimer on a different page dedicated as a translation disclaimer.

5.1.4.7 Terms and condition

Another assurance mechanism that was identified is the website *terms and conditions*. The terms and conditions inform users of their rights and obligations when accessing and/or using the websites. 44% of the websites were found to have listed the terms and condition statements. It was also noticeable that all websites from the local Government category published this statement while it was displayed on one each from the federal agencies and state Government categories.

Under the limitation of liability clause, website owners are relieved of their responsibilities to damages caused by the usage of the websites. This could indicate that all contents on the websites, including personal information of employees, are beyond the responsibilities of the website owners i.e. the Government. If any loss occurred to the employees from the information obtained on official websites, the website owners are not accountable.

5.1.4.8 Date of last updated

Accuracy of information is an important factor for users when perceiving the quality of information on a website (Kim et al., 2008). Websites with accurate and up-to-date information are perceived to be of a higher quality, hence gaining higher trust from the users (Escobar-Rodríguez & Carvajal-Trujillo, 2014). In this sample, 12 websites (66.6%) published their date of the last update on their homepage while six websites did not share this information. This information informs the users whether the website is being regularly maintained or not. In other words, information that is presented on the website should be the latest and up-to-date.

5.1.4.9 Calendar

The calendar feature was found incorporated in 14 websites (77.8%). The calendar feature displayed monthly view and can be accessed from the homepage. The main purpose of this calendar is to inform the public of any related events organised by the organisations. Users can click on a particular date to view any event scheduled on that date. Unfortunately, most websites that included a calendar in their homepage had left it blank. Only one website was found to make use of the calendar feature by listing their events i.e. KPKT.

5.1.4.10 Language

In general, all websites were bilingual. Both Malay and the English language were included as options to users. Malay is the official language of Malaysia and also the main language for government communication. Meanwhile, English is the second language and widely spoken. Users were able to choose the language that they preferred when using the websites.

In addition, support for translating a few world languages were also identified. 61% of government websites embedded a translation feature from a third party ranging from one to 12 different languages. Users may choose which language to be translated into from a drop down menu of options and the webpage will be translated into the chosen language. In total, 18 languages were offered for automated machine translation. Seven websites did not provide any automated machine translation feature. The accuracy of the translation services was not investigated because it is beyond the scope of this study.

5.1.4.11 Summary

This section summarises the results from section 5.1.4. It appears that the specific features of government websites were found to facilitate disclosure of employees' personal information. Dedicated *employee search* engines and *directory of staff* were offered in all websites surveyed. The availability of these two features assists the findability of employees' personal information. Another source of disclosure is through the publication of an *organisation chart* where more than 70% of the websites chose to publish a detailed organisation chart which includes their employees' personal information. Furthermore, the practice of 61% of websites in embedding an auto-translation feature increases the degree of accessibility to the largest possible range of people. A total of 18 different languages were offered for auto-translation services.

In response to the privacy concern of personal information disclosure, websites normally provide statements or policies displayed on their websites. Therefore, five statements in relation to personal information and privacy were scrutinised. *Privacy policy* and *security policy* were found in all websites, while *disclaimer* was available in 17 of 18 websites. *Terms and condition* were found in 61% of the websites while a *personal information charter* was not available in any of the websites. Although the websites were consistent in displaying their privacy and security policies, none of the policies provided references towards information published on the websites. Instead, the policies emphasised protecting visitors'/users' privacy and personal information. Similarly, the *disclaimer* and *terms and condition* did not provide any indication on protecting information that originated from the websites. Thus, it can be suggested that protection of employees' personal information is not a priority for government websites.

A *calendar* function was available in 77% of the websites. However, only one website was found to upload updated information regarding their events and activities on the calendar. For other websites, the information on the calendar was incomplete, resulting in mostly blank spaces. On the contrary, information on *date of last updated* was significantly present on 12 websites which gives an indication to users that the website was regularly maintained.

5.2 Semi-structured interview

This section presents participants' demographic properties, their awareness of obligatory disclosure, understanding of the concept of personal information and privacy as well as the themes that emerged from in-depth semi-structured interviews. There are three categories of interviewees in this study, as detailed in section 3.4.4.1. First are the participants that refer to the government employees, second are the commentators and thirdly the IT stakeholders.

5.2.1 Demographic characteristics

As discussed in chapter three, participants were handed the demographic information form before the interview commenced. The demographic form was returned to the researcher and kept in a secure location during the data collection phase. Nineteen interviews were conducted with government employees selected from the support service category, professional and management category and top management category. To protect the anonymity of participants, limited demographic characteristics were presented. The table below summarises the demographic characteristics of the participants.

Table 5-19: Participants' demographic characteristics

No	Age Group	Gender	Ethnicity	Marital Status	Working Experience (years)	Working group	Highest Education
P001	36-40	Male	Malay	Married	11-15	Support	Degree
P002	20-25	Female	Malay	Married	6-10	Support	SPM
P003	31-35	Male	Chinese	Single	6-10	P&M*	Master
P004	20-25	Female	Malay	Single	1-5	Support	Diploma
P005	46-50	Male	Malay	Married	21-25	Top Mgmt.	PhD
P006	31-35	Female	Indian	Married	6-10	P&M	Master
P007	31-35	Male	Malay	Married	6-10	Support	Diploma
P008	36-40	Male	Malay	Single	11-15	P&M	Degree
P009	51-55	Male	Malay	Married	26-30	P&M	Master
P010	26-30	Female	Malay	Single	6-10	P&M	Master
P011	26-30	Female	Malay	Married	1-5	P&M	Degree
P012	51-55	Female	Malay	Married	26-30	Support	Diploma
P013	46-50	Male	Malay	Married	21-25	P&M	PhD
P014	51-55	Female	Indian	Married	26-30	Support	Diploma
P015	26-30	Male	Malay	Married	6-10	Support	SPM
P016	31-35	Male	Malay	Married	6-10	P&M	Degree
P017	51-55	Male	Malay	Married	31-35	Top Mgmt.	Master
P018	41-45	Male	Malay	Married	11-15	P&M	Master
P020	56-60	Female	Chinese	Married	31-35	Top Mgmt.	Master

**Professional and Management*

5.2.1.1 Gender

The participants (excluding commentators and IT stakeholders) consisted of 58% males and 42% females. Past research showed that gender differences influence individuals' privacy perception, where women tend to have higher privacy concerns than men (Joinson et al., 2010; Youn, 2009; Janda & Fair, 2004; Hoy & Milne, 2010; Fogel & Nehmad, 2009). A balanced distribution of gender will deliver equal findings in examining participants' similarities and differences around obligatory disclosure.

Table 5-20: Gender of participants

Gender	No. (n)	Percentage (%)
Male	11	57.89
Female	8	42.11

5.2.1.2 Age group

Participants were categorised into eight age groups. Since age has been identified to have an influence in individuals' concerns and responses in information privacy (Janda & Fair, 2004; Joinson et al,. 2010; Laric et al., 2009; Nosko et al., 2010), this data enables this research to potentially understand the results from this factor.

Of 19 participants, four participants each were in the 31-35 and 51-55 age group (21% each), which had the highest number of participants. Three participants were from the 26-30 age group, two participants from the 20-25, 36-40 and 46-50 age groups respectively, while the least number of participants were from the 41-45 and 56-60 age groups with only one participant each. No participants were from the below 20 and above 60 age groups. As shown in Table 5-21, most of the age groups were represented to benefit from the understanding of different ages.

Table 5-21: Age groups of participants

Age group	No. (n)	Percentage (%)
Below 20	0	0
20-25	2	10.53
26-30	3	15.79
31-35	4	21.05
36-40	2	10.53
41-45	1	5.26
46-50	2	10.53
51-55	4	21.05
56-60	1	5.26
Above 60	0	0

5.2.1.3 Ethnicity

The ethnicity characteristic of participants was collected as an individual’s race was found to impact on an individual’s concern about privacy (Laric et al., 2009). Participants’ ethnicity represented the three largest ethnic groups in Malaysia. Almost two-third of participants (78.9%) were identified as Malays while there were two participants each from the Chinese and Indian ethnicities. A higher number of participants from the Malay ethnicity is representative of the current composition in the public sector, which is at 78.8% as of 2014, Chinese at 5.2% and Indian at 4.1% (Bernama, 2015). The rest comprises of Sabah Bumiputera (6.4%), Sarawak Bumiputera (4.8%), other Bumiputera (0.3%) and other ethnicities (0.7%). Although the percentages of ethnic Bumiputera Sabah and Bumiputera Sarawak were almost at the same level as Chinese and Indians, most of them were attached in to organisations in east Malaysia. Since the location of this research was in Putrajaya, which is in west Malaysia, it was difficult to locate participants of these ethnicities.

Table 5-22: Ethnicity of participants

Ethnicity	No. (n)	Percentage (%)
Malay	15	78.94
Chinese	2	10.53
Indian	2	10.53

5.2.1.4 Marital status

Most of the participants are married while the remaining were reported being currently single. Past research had found that Internet users perceived online risks differently according to their marital status (Liebermann & Stashevsky, 2002) and thus, reflected in their online usage behaviour. Married users perceived higher risks compared to unmarried Internet users.

Table 5-23: Relationship status of participants

Relationship status	No. (n)	Percentage (%)
Married	15	78.95
Single	4	21.05

5.2.1.5 Working experience

In relation to working experience with the government, participants were found to have served the government for between 1 and 35 years. Thus, the sample comprises of participants that were relatively new in service (two participants) to long-serving employees (two participants). Most participants reported to have been working for between 6-10 years. The diverse range of participants' length of service provides a better understanding on the exposure of obligatory disclosure and their experiences with it. The participants' working experience is depicted in Table 5-24.

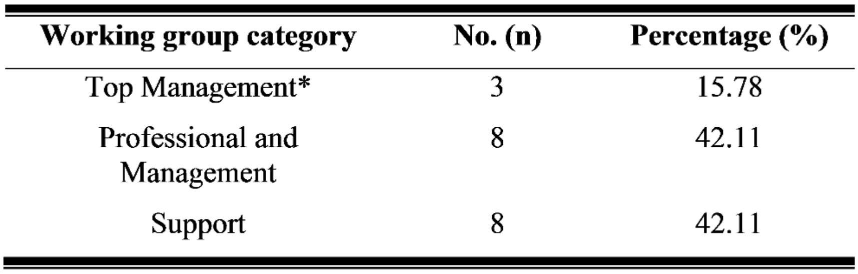
Table 5-24: Working experience of participants

Years of service	No. (n)	Percentage (%)
1-5	2	10.53
6-10	7	36.84
11-15	3	15.79
16-20	0	0
21-25	2	10.53
26-30	3	15.79
31-35	2	10.53

5.2.1.6 Working category

Participants were further categorised into three working groups. The working categories were applied in the MFPS, namely Top Management, Professional and Management, and Support. Participants were recruited from these three groups because each group represents the different levels of responsibility and roles in the MFPS. The Top Management category was represented by three participants while the Professional and Management category and Support category were represented by eight participants each. The low number of participants in the Top Management category was due to the low number of employees in this category and the difficulty in getting them to be interviewed. In addition, the lower number of government employees in that category commensurates with the lower sample recruited.

Table 5-25: Working group of participants



Working group category	No. (n)	Percentage (%)
Top Management*	3	15.78
Professional and Management	8	42.11
Support	8	42.11

**Super scale grade (Malay acronym is JUSA)*

5.2.1.7 Highest level of education

The sample offered a wide variation of education background. Most of the participants were post-graduate degree holders. Seven participants had acquired a master's degree while two were Ph.D. holders. Four participants each had obtained a bachelor degree and diploma while two participants had graduated with a secondary school qualification. The distribution of the participants' level of education is shown in Table 5-26.

Table 5-26: Education level of participants

Highest education	No. (n)	Percentage (%)
Secondary	2	10.53
Diploma	4	21.05
Degree	4	21.05
Masters	7	36.84
PhD	2	10.53

5.2.2 Commentators

Three commentators were included in this study. All of them are academics and they were selected based on their area of expertise related to the topic of investigation. The commentators' views enabled important input from the Malaysian context and their comments could serve as a verification of the findings from the participants. Commentator P019 is from the International Islamic University (IIU) specialising in data protection, privacy and law, whereas commentators P022 and P024 are both from the Faculty of Computing in the Department of Information System at University Technology of Malaysia (UTM). P022's expertise is on social media, e-Government and security, while P024 focuses on social media, online communities and business informatics.

5.2.3 IT stakeholders

Two participants (or commentators) from IT stakeholder agencies were recruited to get their views regarding obligatory disclosure. Views from stakeholders allow for a complete understanding of the phenomena, because they provide data from the government's perspectives. Furthermore, data - from supplementary sources as this - can be used as a cross-validating technique in obtaining trustworthiness (Creswell, 2013b). MAMPU and MDeC were selected since both agencies play an important role in the MGPWA evaluation assessment. In addition, MAMPU is a federal agency that is responsible for ICT development across all Malaysian Government agencies. It is also worthy of attention that few participants highlighted MAMPU as an important agency when discussing obligatory disclosure during the interview.

Participant P021 is an executive from the Multimedia Development Corporation. P021 is involved with the MGPWA process. Another participant, P023, is a Principal Assistant Director from MAMPU. P023 oversees the MGPWA and Malaysian public sector websites.

5.2.4 Awareness of obligatory disclosure

This section presents participants' awareness of obligatory disclosure. Participants' awareness of the investigated phenomenon is important in assessing participants' views towards their privacy. Their familiarity with the government website, disclosure of employees' personal information and their own information emerged during the data collection process.

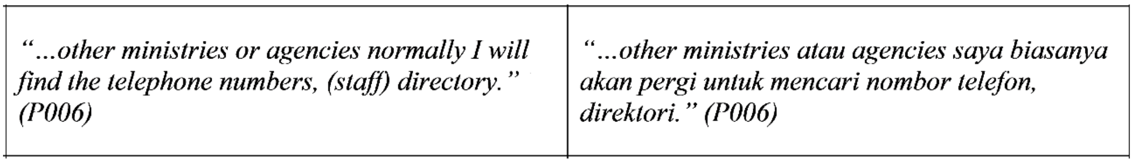
5.2.4.1 Importance of government website

All participants agreed that government websites are an important tool for the government to deliver efficient and better services to the public. Participants were able to elaborate on the functions and objectives of the websites, both from the citizens and the government's points of view.

As government employees themselves, most participants mentioned that they visit government websites regularly. Their motivation for visiting government websites was mainly as a source of information for completing their work. This was repeatedly mentioned by participants during the interviews. Other reasons for visiting government websites are regarding their personal civil service issues - such as transfers - staff promotional exercises, salary information, in-service training and examination application. In line with the concept of e-Government, issues related to human resources are increasingly being transferred from paper-based to the online platform. For example, the monthly salary slip is available online and can be downloaded, as can examination schedules and examination applications, applications for training or skills upgrading and information on promotion exercises can be conducted through websites. Hence, besides assisting their work, civil servants visit government websites to access matters related to their service in the government.

5.2.4.2 Awareness of employees' information

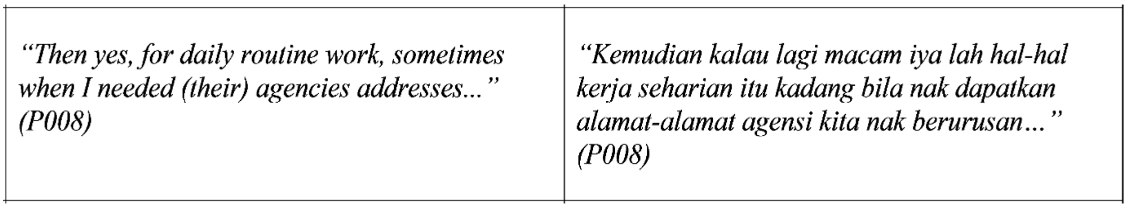
Participants mentioned that they search for information such as circulars, guidelines, functions of relevant departments or ministries and other agencies in relation to their scope of work. In doing this, participants stated that they have noticed that information about government employees is published on the websites. Participants provided examples that can be found on organisation websites, such as information about employees and their contacts.



"...other ministries or agencies normally I will find the telephone numbers, (staff) directory." (P006)	*"...other ministries atau agencies saya biasanya akan pergi untuk mencari nombor telefon, direktori." (P006)*

Box 5-1: Result-P018

Hence, this information is then used mainly to assist them in their duties. Largely, participants responded that identifying the person-in-charge is the main reason when searching for information about employees and their location.



"Then yes, for daily routine work, sometimes when I needed (their) agencies addresses..." (P008)	*"Kemudian kalau lagi macam iya lah hal-hal kerja seharian itu kadang bila nak dapatkan alamat-alamat agensi kita nak berurusan..." (P008)*

Box 5-2: Result-P008

Another participant added that information about employees on an organisation's website allows future employees to reach the relevant officer in getting initial information prior to reporting for duty:

"That's why for example, before I was recruited by the government and let's say I'd received the offer letter, so I (need) to contact the person-in-charge asking for information such as how to report for duty and all kind of things, so I surfed the website and found their names, telephone number so I can call them directly…" (P011)	*"Itu sebab contohnya, kalau dulu sebelum saya nak masuk government ini katalah waktu itu saya dah dapat offer letter dah, so saya (perlu) nak kontak person in-charge untuk tanya macam mana nak lapor diri apa semua itu memang saya buka website itulah so saya jumpalah nama dia, nombor telefon dia memang saya boleh direct…" (P011)*

Box 5-3: Result-P011

Meanwhile, a participant reiterated that the benefit of obligatory disclosure is not limited to new recruits. Existing government employees also make use of information about employees in a particular organisation to capture a general overview of a new department, in order to understand the scope of responsibility as well as to gain information about the strength of the organisation before being posted to their new department.

"One of the reason was to know their business, their scope, scope of department. In addition, the (organisation) chart, haa their strength, support, yes support how many (employees). We have to know that." (P001)	*"Salah satunya pasal kita nak tau dia punya bisnes tu, dia punya apa orang kata apa orang kata apa skop, skop dia tu, jabatan tu dia buat apa. Lagi satu carta (organisasi) tu, haa dia punya kekuatan, support, support dia kan,ha berapa orang, berapa orang. Kita kena tau jugak kan." (P001)*

Box 5-4: Result-P001

This response was referring to the detailed organisational chart that contains employees' information. An organisational chart presents a visual depiction of an organisation's structure. Thus, future employees may able to identify which sections or units that are available for them to be assigned to and get to know who they will be working with in advance. As presented in the web content analysis result, an organisational chart was found to be commonly published by most of the websites. Furthermore, detailed organisation charts (with employees' information) were available for public knowledge.

Also, a large number of participants admitted that they intentionally search for employees' information through government websites but claimed that it is only for official reasons (as stated above).

"Ah sometimes one of the purpose of visiting (government) websites is to get their telephone number [laugh]. (Staff) directory." (P002)	*"Ah kadang-kadang kalau macam kita nak ca err bukak laman web tu pun salah satu jugak tu kita cari nombor telefon orang [ketawa]. Direktori (kakitangan)." (P002)*

Box 5-5: Result-P002

They seemed to use the staff directory as their main strategy of finding information about employees. After all, almost all participants referred to the staff directory when describing employees' information. To them information about employees is important to be published on the websites.

"...to me it is very important, it's really important!" (P007)	*"...bagi saya sangat penting, memang benda itu sangat penting!" (P007)*

Box 5-6: Result-P007

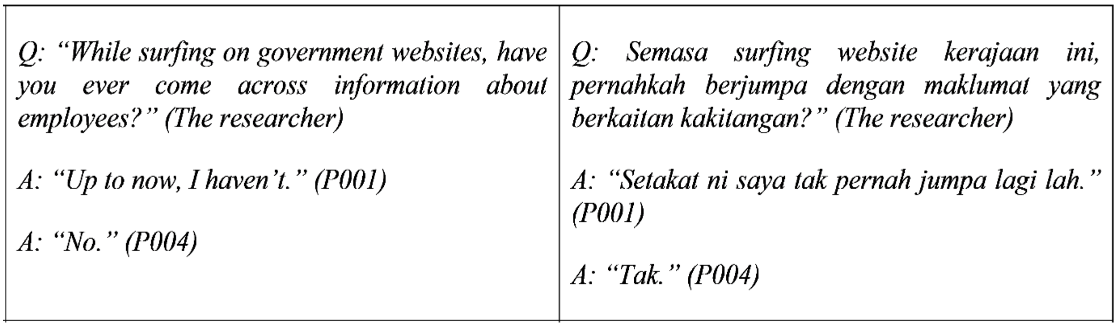
Additionally, they explained reasons for visiting government websites:

"To search for directory, to search directory for contacting officers responsible (and) to get information..." (P003)	*"Untuk ah cari direktori, untuk cari direktori untuk menghubungi orang yang berkenaan tu untuk mendapat er informasi..." (P003)*

Box 5-7: Result-P003

Therefore, employees seemed to search for other employees' information on purpose. This is because employees' information posted on their organisation's website facilitates the government employees in conducting their daily tasks. It can be suggested that participants are familiar with the investigated phenomenon and are actively utilising that information directly.

However, there was also an indication that some employees were unaware of the availability of employees' information on government websites. Two participants seemed to overlook this type of information. At the early stage of the interview, participants claimed that they had not encountered any employees' information on the organisation's website.



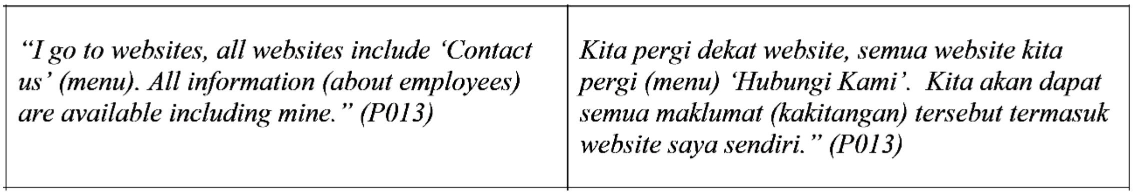
Q: "While surfing on government websites, have you ever come across information about employees?" (The researcher) *A: "Up to now, I haven't." (P001)* *A: "No." (P004)*	*Q: Semasa surfing website kerajaan ini, pernahkah berjumpa dengan maklumat yang berkaitan kakitangan?" (The researcher)* *A: "Setakat ni saya tak pernah jumpa lagi lah." (P001)* *A: "Tak." (P004)*

Box 5-8: Result-P001, P004

The researcher, who could sense that the participants might fail to notice the central subject of the question, rephrased the question by repeating certain keywords. Shortly, both participants realised that they did come across such information and were then able to provide examples of it. In fact, participants viewed that information about employees (other employees) as beneficial to them in assisting their work. It could also be that under normal circumstances, participants did not regard 'information about employees' as the kind of information that is pertinent to them, which is why this could slip from their mind. Both remarks could suggest the commonness in circumstances of this phenomenon, whereby this supports undertaking a single-case method in this research (Yin, 2014).

5.2.4.3 Awareness of self-information

Likewise, participants were also aware of their own information being published on the websites. They clearly stated their observation:



"I go to websites, all websites include 'Contact us' (menu). All information (about employees) are available including mine." (P013)	*Kita pergi dekat website, semua website kita pergi (menu) 'Hubungi Kami'. Kita akan dapat semua maklumat (kakitangan) tersebut termasuk website saya sendiri." (P013)*

Box 5-9: Result-P013

In general, all participants were aware of their own information being published by their respective organisation. When asked, participants spontaneously admitted, and were able to state, the different types of information about them on their organisation's website. Table 5-27 illustrates the types of personal information belonging to participants, as mentioned by them.

Based on the table, a total of ten attributes of personal information were listed by participants. On average, four attributes of an employee were disclosed on the websites. Most of the stated attributes were names, telephone numbers and email addresses. The plausible reason for these attributes being highlighted is the high usage among employees in contacting other employees. At the same time, this awareness hinted that participants were concerned over their personal information disclosure. However, some participants did not seem to acquire detailed information disclosure about themselves by listing only three types of personal information. While this could suggest how employees perceived the importance of personal information on government websites, there was also an uninterested employee.

In contrast, one participant stated that obligatory disclosure was not an important issue to him. In fact, he was unsure whether his personal information was published on his organisation's website. It could be seen that this participant was not bothered by it and at the same time he admitted that he seldom visited government websites including his own organisation's site. While he was aware that his organisation had assigned him an official email address, he confessed that he rarely used it. In fact, the participant revealed that he had long forgotten his password and had not been using his official email address for quite some time. As a general office assistant, the participant mentioned that most of his job responsibilities required him to work outside of the office. This could possibly be the reason why he was not interested with obligatory disclosure. Therefore, it can be suggested from this that there was a possible case of employees who did not need or require obligatory disclosure in exercising their duties.

Table 5-27: Participants' personal information attributes that were disclosed by their organisation's website

Participants	Name	Position	Telephone number (office)	Email address	Division	Section/unit	Photograph	Work scope	Fax number	Department
P001	*		*	*						
P002	*	*	*	*						
P003	*	*	*	*			*			
P004	*	*								*
P005	Did not ask									
P006	*	*	*	*						*
P007		*	*	*	*	*			*	
P008	*		*	*	*					
P009	*		*	*	*					
P010	*		*	*	*	*				
P011	*		*	*	*					
P012	*	*	*		*					
P013	*	*	*	*						
P014	*		*		*			*		
P015	None									
P016	*	*		*	*		*			
P017	*	*					*			
P018	*		*	*				*		
P020	*	*	*							

In the case of participant P005, the question was not posed to him because the direction of the discussion required the researcher to probe further into the topic of privacy, based on his response. This is the advantage of using a semi-structured interview technique, which allows probing additional information for discussions or clarifications depending on the direction of the interview (Savin-Baden & Major, 2013).

In view of this, it can be suggested that on the whole, almost all participants were aware and highly familiar with obligatory disclosure. Their awareness was considerably high, demonstrated by participants showing interest towards other employees and also their own information. It can be seen that participants made use of this phenomenon wisely and even actively searched for information about particular employees through the websites.

5.2.5 Understanding of the concept of personal information and privacy from an individual perspective

Individuals' understanding of personal information and privacy concepts in general is important to be explored. This is because by exploring their understanding of these two concepts will provide a better construction of the participants' knowledge of the topic. Consequently, this will assist in explaining and interpreting participants' perceptions and views of obligatory disclosure. A full list of interview quotes is presented in Appendix H but key quotes are included in the main body of thesis.

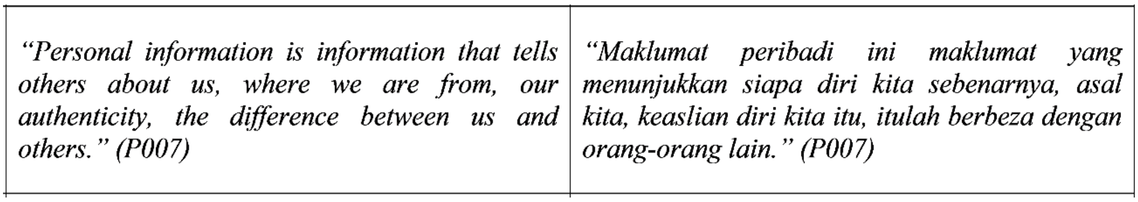
5.2.5.1 The concept of personal information

On the whole, all participants understood the concept of personal information. However, initially, most participants had difficulties when asked to define personal information. Participants chose to give examples of personal information instead when they were doubtful, with more than half of the participants (12) displaying this reaction when defining personal information. Of those, five participants found it strenuous to define personal information, thus sticking to their examples.

Three participants contradicted themselves when explaining personal information. They initially explained that personal information is information that cannot be disclosed to others (e.g. the public), but later suggested that some of it could be shared. Another participant , while suggesting that any information related to work is not considered as personal information, later gave working position as one of the examples of personal information.

Upon further questioning, several participants defined several different meanings for the term. Most participants viewed it as information about themselves. Five participants stated that it was information about themselves, while one referred to it as a ‘profile’.

Two participants responded by defining that personal information is information that shows our originality/authenticity, and it can be used to identify employees (see example below and Appendix H – Box 5-11: Result-P001).



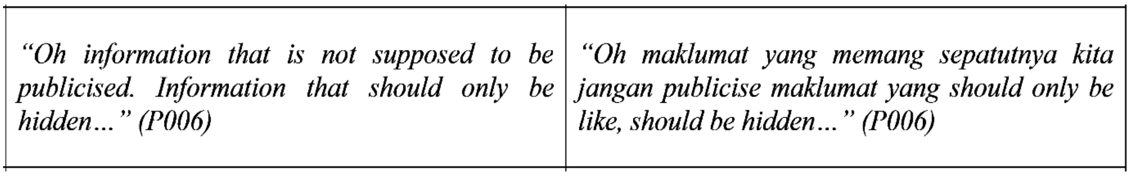
“Personal information is information that tells others about us, where we are from, our authenticity, the difference between us and others.” (P007)	*“Maklumat peribadi ini maklumat yang menunjukkan siapa diri kita sebenarnya, asal kita, keaslian diri kita itu, itulah berbeza dengan orang-orang lain.” (P007)*

Box 5-10: Result-P007

Another position was the understanding of personal information as a secret. For instance, they viewed personal information as a confidential information that cannot be shared with others (for example Appendix H - Box 5-11: Result-P012).

They gave salary and personal life as examples of personal information. Despite defining personal information as secret and confidential initially, some participants was seen as inconsistent when suggesting that some personal information, such as date of birth and hometown, could be shared. They later explained that this information was not at the same level of confidentiality as salary and personal life. In fact, different types of personal information were found to have different levels of sensitivity (Phelps et al., 2000; Sheehan & Hoy, 2000).

Meanwhile, another participant defined personal information as information that cannot be publicised, and should not be revealed.



“Oh information that is not supposed to be publicised. Information that should only be hidden…” (P006)	*“Oh maklumat yang memang sepatutnya kita jangan publicise maklumat yang should only be like, should be hidden…” (P006)*

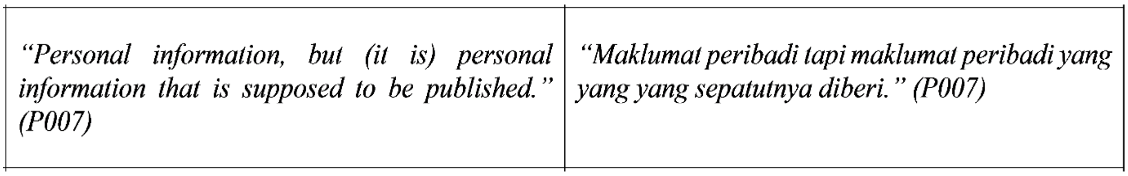
Box 5-12: Result-P006

To explore their understandings further, examples of personal information were sought from the participants. While personal attributes and family were among the most commonly given examples, employment information, e.g. workplace, occupation, working experience, salary, and working position, was also listed by eight participants among the examples of personal information.

5.2.5.2 Sensitivity of personal information

Personal information may comprise of different types. The sensitivity of personal information varies by type, and could influence the level of privacy concern displayed (Phelps et al., 2000; Sheehan & Hoy, 2000). The concept of categorising personal information was mentioned by 7 participants. . They drew a distinction between information that can be shared and information that has to be kept confidential.

Published information on official government websites is considered as personal information that has to be disclosed to the public by the government. A participant, while agreeing that obligatory disclosure reveals his personal information, still believed that it was acceptable for the government to publish employees' personal information.



"Personal information, but (it is) personal information that is supposed to be published." (P007)	*"Maklumat peribadi tapi maklumat peribadi yang yang yang sepatutnya diberi." (P007)*

Box 5-13: Result-P007

To differentiate among different types of personal information, they categorised them as high and low security. The high security category refers to information that should not be shared, while low security category refers to information that may be shared with others.

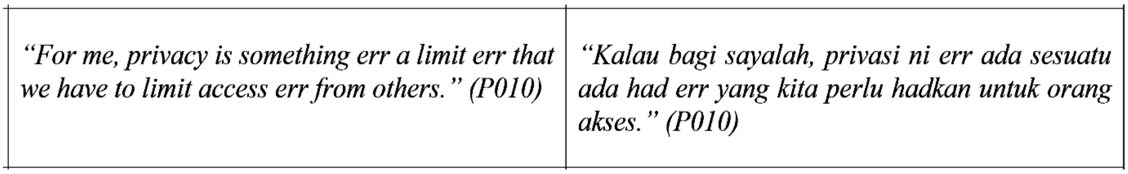
Four participants disagreed that anything related to work is considered personal information. To them, anything related to work-life is not considered personal information. Family and home-related information were among the most frequently discussed attributes in personal information.

Overall, the participants exhibited knowledge on the concept of personal information. Despite some struggling to define the term, they had the idea of what constitutes personal information. In general, the participants agreed that information found on their organisation’s website can be considered as personal information including employment information. However, it can be suggested that the participants’ knowledge of personal information was limited as they had difficulty in soliciting a clear and focused meaning although they were familiar with the term.

5.2.5.3 The concept of privacy

With regard to privacy, participants were found to understand privacy differently. Most of them needed some time to think when asked about privacy. However, they appeared to confidently relate the concept of privacy with personal space and personal information. Concerning personal space, participants linked it to home, friends and family which should be protected against undue interference. On the other hand, privacy of personal information was identified by most of the participants when discussing this question. It can be seen that participants referred to online environments in particular when discussing personal information and privacy. As such, and in line with the objective of this research, this section will only focus on participants’ understanding of information privacy.

Participants revealed three concepts when explaining privacy. The first of these concepts, which was articulated by most participants, is limiting access to information, and is illustrated by the following example:

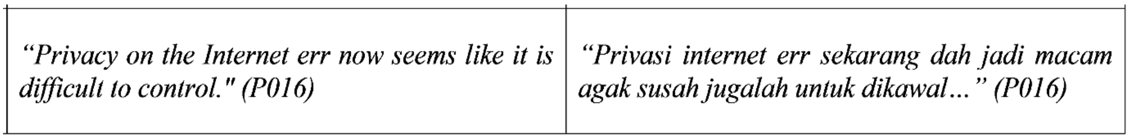


“For me, privacy is something err a limit err that we have to limit access err from others.” (P010)	*“Kalau bagi sayalah, privasi ni err ada sesuatu ada had err yang kita perlu hadkan untuk orang akses.” (P010)*

Box 5-14: Result-P010

Privacy, as a state of limited access, refers to the ability of protecting personal information from unauthorised use (Laufer & Wolfe, 1977).

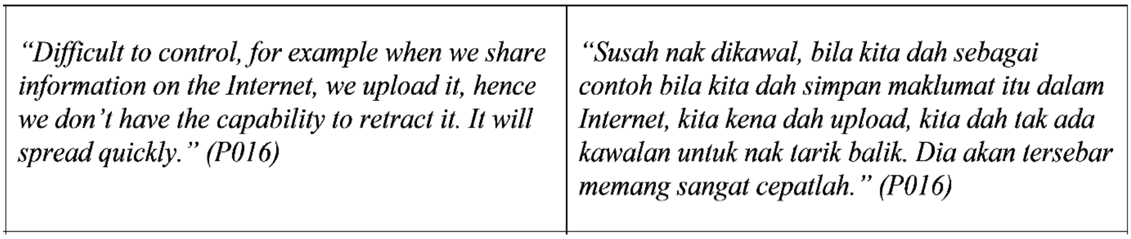
Secondly, privacy is the ability to control distribution of personal information. The participants associated this concept with the online environment, and noted that controlling information on the Internet is challenging and difficult. One participant shared his views about privacy on the Internet:



"Privacy on the Internet err now seems like it is difficult to control." (P016)	*"Privasi internet err sekarang dah jadi macam agak susah jugalah untuk dikawal…" (P016)*

Box 5-15: Result-P016

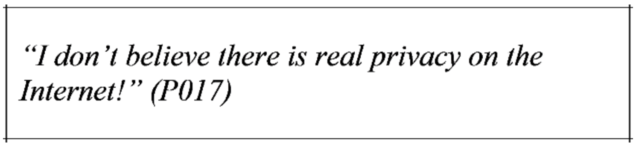
Lack of control correlates with concerns over privacy. Once personal information is posted on the Internet, it is difficult to keep track of it as it might then be circulated, shared, stored, processed, disseminated, or collected.



"Difficult to control, for example when we share information on the Internet, we upload it, hence we don't have the capability to retract it. It will spread quickly." (P016)	*"Susah nak dikawal, bila kita dah sebagai contoh bila kita dah simpan maklumat itu dalam Internet, kita kena dah upload, kita dah tak ada kawalan untuk nak tarik balik. Dia akan tersebar memang sangat cepatlah." (P016)*

Box 5-16: Result-P016

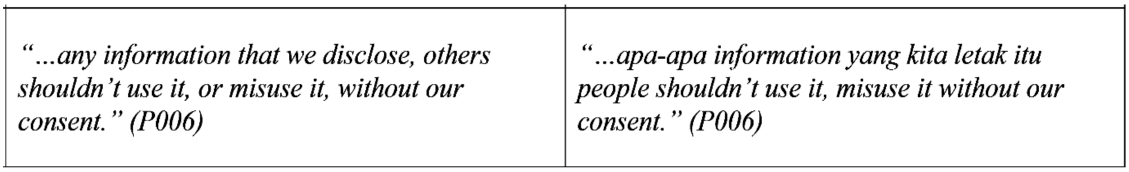
Information can also be misused and abused easily by anyone in the online environment and that is why they stressed that they do not think there is any privacy on the Internet due to the abundance of personal information scattered on the Internet and the difficulty of controlling it (Appendix H – Box 5-17: Result-P020). In fact, some participants doesn't think there is any privacy on the Internet:



"I don't believe there is real privacy on the Internet!" (P017)

Box 5-18: Result-P017

They attached the idea of giving consent with their concerns over unauthorised use of personal information. This idea was forwarded by two participants, for example:



"...any information that we disclose, others shouldn't use it, or misuse it, without our consent." (P006)	*"...apa-apa information yang kita letak itu people shouldn't use it, misuse it without our consent." (P006)*

Box 5-19: Result-P006

The concept of control in privacy was suggested by Westin (1967). He defined information privacy as "the claim of individuals or groups to determine for themselves when, how and to what extent information about them is communicated with others." (1967, p. 7). The findings suggested that the participants' belief in the ability to control over their personal information influences their privacy concern.

Another privacy scholar in social and psychology field defined privacy as: "the selective control of access to self" (Altman, 1975, p. 24). He utilised both the concept of control and limited access to define privacy.

The third concept was of privacy as a right, and P005 stated it in particular. He strongly believed that every individual should have their own privacy regardless of who they are - including civil servants. The idea that privacy is a right was originally defined in a legal context by Warren and Brandeis (1890) as: "the right to be let alone".

Overall, the participants have a general understanding of the concept of privacy. Despite the fact that they have not encountered privacy issues before, the participants were aware of the consequences of privacy violations, as highlighted during their attempts to describe privacy. To them, any violations of privacy may create disturbance and an uncomfortable situation.

5.2.6 Themes

This section reports on the themes that emerged from the data using the analysis described in chapter four. In this study, the main objective is to explore how public employees describe organisational disclosure and its relation to their privacy. After conducting rigorous data analysis as reported in chapter four, six themes emerged from the data. The themes are presented in the final thematic map as shown in Figure 5-4.

As shown in the thematic map below, six themes and two sub-themes were developed based on the data from the participants. The emergent themes are as follows:

1. Privacy concern and privacy awareness regarding obligatory disclosure.
2. Separation of social and professional in online environment.
3. Violations of employee's privacy.
4. Higher vulnerabilities for individual.
    4.1 Characteristics of obligatory disclosure (sub-theme).
5. Commitment to public service ethos.
    5.1 Trust to organisation (sub-theme).
6. Lack emphasis on privacy.

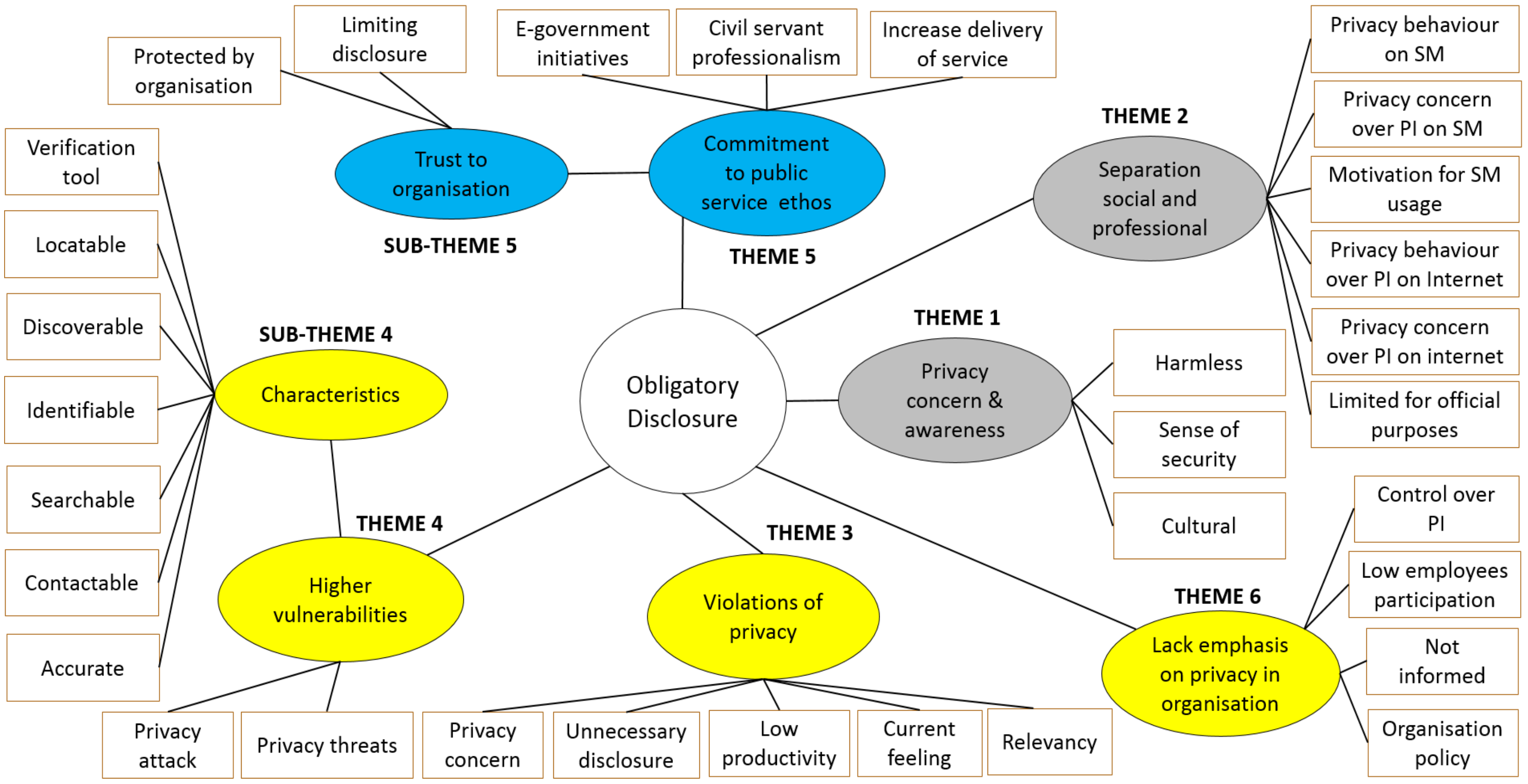


Figure 5-4: Final thematic map

While the themes are presented in the next section, it only represents the analysis of data from the in-depth semi-structured interviews. For this reason, research findings that comprise results from both methods (i.e. content analysis and in-depth semi-structured interview) are not presented here. The research findings, in relation to the research questions and literature reviews (chapter two), are presented in the next chapter i.e. chapter six.

5.2.6.1 Theme 1: Privacy concern and privacy awareness regarding obligatory disclosure

This theme represents how the participants perceived obligatory disclosure. This theme consists of three categories and nine code labels as shown in Table 5.28. The majority of the participants perceived obligatory disclosure as harmless and consequently safe. The reason for regarding it as safe is because only a little information about themselves is disclosed by the website. Thus, low risk of exposure was expressed by the participants. Furthermore, the information was only related to details about their office. To most of the participants, information about their home and family will generate higher concerns. In addition, some of the participants viewed the disclosure as 'slightly hidden' because their information was 'not directly displayed' on the homepage.

From their personal safety point of view, most participants considered themselves as not attracting anyone with malicious intent. While they were aware that their personal information is publicly available (as discussed in section 5.2.4), the participants showed confidence of not being targeted. The participants resorted to believing that they are not an important person and therefore exhibited a high sense of security.

Obligatory disclosure was found to be commonly practiced in Malaysian Government websites and the participants regarded it as mandatory information. All of them agreed that obligatory disclosure has become a normal phenomenon and this could suggest that the participants' perception was due to the organisational culture.

Table 5-28: Codes, categories and excerpts for Theme 1

Categories	Code label	Excerpt from participants' quotes
Harmless	Not directly displayed	*"Because to me it is (like) not published. It's because we have to search, search then click search then only it is found on the database, it's not displayed conspicuously." (P008)*
	Limited disclosure	*"The information listed from the directory was not more such as telephone number, email (address) like that, not detail." (P007)*
	Low risk	*"I believe if it's because (of that information), it cannot be used (for bad purposes), because it is only name, extension number, unit, email address, email only, official email." (P001)*
	Information related to office	*"Because they only listed names and email. Moreover, the email is organisation's email, telephone number with organisation's extensions. For me so far it's ok." (P001)*
Sense of security	Not a target	*"...but so far I think no outsiders will just simply want to find information about me...if we are in support (category) it shouldn't be a problem, right? (But) what about the top management?" (P011)*
	Ordinary person	*"...because I think I am just an ordinary person so the effect is not big." (P007)*
Cultural (organisational)	Commonly practiced	*"Yes, most of the time it's there." (P017)*
	Mandatory	*"It must be included" (P007)*
	Normal	*"But it has become normal" (P005)*

During the interview, topics about the publication of employees' information on organisation's website precede other topics as discussed in section 3.4.4.3. There might be a possibility of bias if participants had a preconceived idea about privacy if privacy issues were brought up at the beginning of the interview. Therefore, in order to get an honest opinion from the participants regarding obligatory disclosure, the researcher was looking for an open answer from the participants by not leading the questions to the topic of privacy early on during the interview. Hence, data from the participants revealed that the majority of employees did not see obligatory disclosure as a reason for their privacy concern.

However, there was also a high concern around privacy expressed by some participants due to obligatory disclosure. This sentiment was consistent throughout the interview sessions that indicated some participants had contrasting views of obligatory disclosure though they were the minority.

5.2.6.2 Theme 2: Separation of social and professional in online environment

The issues of privacy behaviour towards personal information were observed throughout the research. This theme represents a participant's personal information-related behaviours online including social media (e.g. Facebook) and on the Internet in general. This theme consists of six categories and 23 code labels as shown in Table 5.29.

On social media, most participants admitted to using Facebook as their preferred social media provider. Out of 19 participants, three participants admitted to not having a Facebook account. The reasons for this were due to two being uninterested and one (P020) stating that privacy concern is the main justification for not subscribing to Facebook. Therefore, for these participants, their personal information behaviour was focused only towards the availability of their personal information on the Internet.

The use of social media, i.e. Facebook, unearthed the participants' privacy behaviour which contradicted with the findings in the previous section. The participants expressed concerns over their personal information on social media. They were concerned with the disclosure of personal information to outsiders (12 participants), misuse of information (four participants), safety (two participants), and collection (two participants).

For this reason, they employed several strategies. Four main strategies were derived from the participants. The participants chose to disclose their personal information selectively on their Facebook profile such as withholding their occupation, education qualification, date of birth and relationship status. In fact, some participants withheld information about their feelings or observations. 68% of the participants had configured their Facebook's privacy account to a private setting while five participants made theirs public. Even so, among these five participants, three were active users of Facebook. One participant claimed that he was not active on Facebook while another used a fictitious profile on his account. One third of the participants falsified their information as a strategy for privacy protection. Similarly, several participants employed an unidentifiable strategy to ensure that they could not be identified through their personal information. However, this strategy was only obvious for certain types of attributes e.g. full name and photograph. The participants had the tendency to use nick names or photographs that belonged to a family member e.g. children.

Five reasons were generated for the participants' motivation in using Facebook. Most of them stated that their primary use was to keep in touch with family and friends, which indicates the social function of Facebook. Other identified purposes were using Facebook as a platform for discussions, sharing of personal information, getting updated on news and releasing stress.

Table 5-29: Codes, categories and excerpts for Theme 2

Categories	Code label	Excerpt from participants' quotes
Privacy behaviour on social media	Unidentifiability	*"Even in name, I use a nickname." (P007)*
	Falsify information	*"The only thing that I always change will be my profile picture. Initially the photo was my face but now no more [laugh]." (P006)*
	Privacy configuration	*"I fill in all but I, I set privacy [laugh]." (P005)*
	Withholding information (social media)	*"Employment information, no. I didn't disclosed." (P001)*
Limited for official purposes	Official mode of communication	*"The purpose is to simplify official duties or official relations like what I said before." (P014)*
	Associated to work	*"...just to contact only related to work" (P008)*

Categories	Code label	Excerpt from participants' quotes
Privacy concern on social media	Disclosure to outside parties (social media)	*"If others wanted to investigate about me, it's easy. If I share everything, then if someone who doesn't like me, from the Internet they can gather a lot of my information especially Facebook." (P002)*
	Misuse of information	*"Because people can misuse the information… Many people use it using other's name, my name (for example), then create slanders to the king, it's an abuse…" (P013)*
	Safety (social media)	*"In another aspect, err aspect if we look from the other perspectives, more importantly is the safety." (P018)*
	Collection (social media)	*"Everybody knows where we go, who our family members are, our friends…it's too easy to collect information about us." (P007)*
Motivation for social media usage	Get in touch with family and friends	*"Because I want to link with my school friends, to get along with my friends…" (P002)*
	Platform for discussions	*"Social media is for discussing certain issues…" (P001)*
	Sharing personal information	*"It's more appropriate if they're willing to share, it's on Facebook" (P001)*
	To release tension/stress	*"And then sometimes, I like to share err it's like a channel for me to release tension…" (P017)*
	Get updated on news	*"One more, I get updated on news by using Facebook, because sometimes I didn't have time to watch news (on tv)." (P011)*
Privacy behaviour over personal information on the Internet	Self-search	*"I check. I key in my name…" (P020)*
	Withholding information (Internet)	*"…you'll be particular with this. You'll disclose less (information)." (P001)*
	Avoid insensitive friends	*"For example, I know that my friend is Internet savvy, always upload photos so I'll try to avoid him." (P016)*

Categories	Code label	Excerpt from participants' quotes
Privacy concern over personal information on the Internet	Accuracy	*"I always make sure only (my) accurate information is on the Internet." (P013)*
	Collection (Internet)	*"Secondly, I wanted to know how they get that information." (P018)*
	Disclosure to outside party	*"[Mmm] One I wanted to know whether it appears anywhere, any websites my names." (P018)*
	Safety (Internet)	*"…then they can post something or like that. I am worried but I am not really sure what will happen." (P014)*
	Misuse of information (Internet)	*"Just to see, no, just to see how far in case people misuse." (P009)*

With regard to information on the Internet, the participants exhibited a concern for the availability of their personal information. This was attributed to their privacy behaviour about the availability of their personal information on the Internet. More than half of the participants raised concerns about their information on the Internet. Most of them referred to their concerns on the possibility that their information can be viewed by anyone, collection, accuracy, misuse of personal information, the secondary usage of their information and personal safety. Therefore, a large number of participants (12 participants) demonstrated information-seeking behaviour of their own information that may suggest some privacy concerns (Madden et al., 2007). Of these, one participant each resorted to withholding information and avoiding insensitive friends as a measure to protect their privacy.

The difference in participants' privacy behaviour towards their personal information on an organisation's website seems to be reasoned out from their perception that information on an organisation's website is for official purposes. The participants stated that it is exclusively for the official channels of communication, either among government employees or with the public. Thus, the usage of their personal information is limited to their work.

5.2.6.3 Theme 3: Violations of employee's privacy

This theme emerged from six categories and 25 code labels. The theme revealed that employees' privacy was violated as a result of obligatory disclosure. Despite most of the participants not exhibiting concern with privacy issues at the beginning of interview, a large number of them shared their experiences of privacy violation. Some participants were observed to be more critical of disclosure after issues of privacy and personal information were discussed.

Most of the participants (73%) highlighted their privacy concerns with the disclosure. They stated disclosure of information to outsiders, information error, unauthorised secondary use of information and personal safety as their main concerns.

The participants cited unnecessary and irrelevant disclosure of employees' personal information as two factors that triggered their concern. Information about employees was overly published, and at times too detailed information was available. Participants believed that this disclosure should serve the purpose of employees in discharging their duties, and at the same time it should be scrutinised to ensure that relevant employees were published on the website.

Participants expressed an inclination towards negative feelings with the disclosure (at the current stage), which was opposite to what they felt when the disclosure had just occurred.

Participants shared their experiences of privacy invasion on receiving unsolicited calls, receiving spam emails and paper-based spam. In view of this, participants reported that their work was disturbed and affected.

Table 5-30: Codes, categories and excerpts for Theme 3

Categories	Code label	Excerpt from participants' quotes
Relevancy	Dealings with public	*"All (employees) that are involved directly with the citizens, must (published), those who don't, in fact, no." (P013)*
	Not for every employee	*"...only specific employees should be published on the web, not all..." (P009)*
	Top management	*"...of course it is appropriate to publish firstly is their top management, which can be displayed all,it's fine as well..." (P018)*
	Work scope	*"Investigation officer no need, prosecutor no need" (P013)*
	Working category	*"...but if it's up to the extent of support staff as administrative assistant, I don't think so." (P009)*
Privacy concern	Disclosure of personal information to outside party	*"It feels like, (my) personal details are exposed to outsiders" (P003)*
	Error	*"One of the issue is sometimes it is incorrect, no, incorrect, the phone number. I didn't realise my number was wrong. In my directory it should be 1473 but it was mistakenly written as 1573, so sometimes it's like carelessness I suppose." (P011)*
	Misuse of information	*"The misuse is like what I've said earlier for example, for business promotion, personal loan (advertisement) and so on." (P007)*
	Unauthorised secondary used of information	*"It occurred to me during one of our investigation, we came across an advertisement that pictured us (our staff) without asking for permission. I've come across cases like this once a while." (P009)*
	Personal safety	*"My work, I will patrol places, catch those people, so it will endanger me if my photograph is there (on the website)." (P003)*

Categories	Code label	Excerpt from participants' quotes
Unnecessary disclosure	Over disclosure	*"Sometimes there are also passport photos, right? That also I think sometimes it is unnecessary." (P006)*
	To serve the purpose	*"But if it's just for publication to others, public, there is no need for profile photo, just name is enough." (P006)*
	Too detail information	*"…I found (the top management) level of education, date of 'Datukship' conferred, working experience, number of children and else. That has reached privacy level." (P003)*
Privacy invasion	Unsolicited calls	*"Loans or the personal loan, or products, the product that they will sometimes call us." (P001)*
	Spam emails	*"Ish! This is official email so what is this? So I got negatively affected by it….That's why I think my privacy is violated a bit." (P008)*
	Paper based spam	*"Haa after letters, then it's by fax…" (P014)*
Low productivity	Disturbing	*"When ok, and I want to start work again then there are calls even during discussion and you know it is like a bit of disturbance" (P006)*
	Jeopardise investigation	*"…if they look at that photo they simply knew that this is the enforcement coming and it might jeopardise our investigation." (P003)*
	Emails capacity exceeded	*"I am afraid it will exceed my email (hard disk) quota, then (I) will miss other important emails…" (P014)*
	Unrelated communication	*"Supposedly all calls must be for important matters only and not for things like this." (P001)*
	Wasting time	*"Sometimes it is disturbing, it bothers me actually because I have to read (the spam emails) and also because I have other things to do." (P012)*
Current feeling	Reluctant	*"After reflecting on my long service, I felt like never mind no need for others to know my number because I am tired of this." (P006)*
	Vulnerable	*"I feel like, (my) personal details are exposed to outsiders." (P003)*
	Normal	*"Now the feeling is that I'm used to it, it's already three times seeing this, oh still the same [laugh]." (P007)*
	Worried	*"But when [laugh] I received scams, scams like this, I am not (happy) [laugh]. I am sort of worried when I receive letters sometimes,… advertisements requesting this and that." (P014)*

5.2.6.4 Theme 4: Higher vulnerabilities for individuals

This theme consists of one-sub theme. The main theme comprises two categories and 11 code labels. The theme describes the vulnerabilities of employees when information is disclosed via obligatory disclosure. The vulnerabilities stemmed from the characteristics of obligatory disclosure that emerged as a sub-theme.

Table 5-31: Codes, categories and excerpts for Theme 4

Categories	**Code label**	**Excerpt from participants' quotes**
Privacy attack	Fake account	*"Worried they can use it to create fake accounts, right?" (P008)*
	Social engineering	*"...then people may identify (you) anywhere let's say that person is a procurement officer, then if people like contractor identified him, 'Oh this is the one, this is the person.' They might talk to him, or approached him..." (P006)*
	Virus	*"I think this is also dangerous because sometimes it's like a personal loan advertisement but when we click on it, it can be a virus or Trojan or whatever I'm not sure!" (P007)*
	Physical attack	*"My work, I will patrol places, arrest those people, so it will endanger me if my photograph is there (on the website)." (P003)*
	Phishing	*"...because sometimes they asked for account number, address, numbers this and that. If we disclose, they will do something right. Withdraw money from my account or something else." (P014)*
	Spam email (attack)	*"Yes, there are because I always receive err emails. Although it is an official email, I received promotional emails, personal loan, holidays and so on, a lot even few times this month..." (P007)*

Categories	Code label	Excerpt from participants' quotes
Privacy risks	Misuse of information (risks)	*"To [P012], information on the website can be manipulated, he can by asking, 'Oh that day I ask that officer he said can?'. 'Ha who is the officer?', 'so, so and so.'" (P012)*
	Invisible audience	*"When (information is) public, it is difficult to authorise whether it is a real authorised phone call from bank or fraud…" (P001)*
	Misinterpretation	*"So maybe, for a third party when we're inclined towards the other, they will have misconceptions when seeing our information is (published) there…" (P009)*
	Disclosure by colleague	*"He can find through the operator or his next colleague or someone within the organisation that he knew and ask for the number." (P014)*
	Government's confidential information	*"Because if your privacy is exposed too much, it will expose the government's (confidential information)…(you) know…So the government loses." (P005)*

Privacy attacks and privacy risks were two categories that represent the vulnerabilities of employees. Six types of privacy attacks appeared from the data analysis, and five risks were discussed by the participants as presented in Table 5-31. Thirteen participants discussed privacy attacks, and personal attack was highlighted by most of the participants. Other than that, fake accounts, social engineering attacks, spam emails, phishing, and computer viruses were listed as forms of attacks resulting from obligatory disclosure.

The data analysis was able to identify five privacy threats that might transpire to the employees. Disclosure by colleagues was noticeably expressed by most of the participants. The participants elaborated on this technique, explaining that it is when someone is trying to get information about other employees. Next, information leakage about the government's confidential information was stated by four of the participants. Other threats were misuse of personal information, misinterpretation and invisible audience.

Sub-theme 4: Characteristics of obligatory disclosure

This sub-theme describes the characteristics of obligatory disclosure. As obligatory disclosure was defined as *"any information about an individual that is shared via any form of communication by an organisation (of which they are employee or member)"* in chapter two, it is characterised by locatable, discoverable, identifiable, searchable, contactable, accurate, and verifiable information. These characteristics assist in the dissemination of employees' personal information as well as providing an easy means to find an employee.

Table 5-32: Codes, categories and excerpts for Sub-theme 4

Categories	Code label	Excerpt from participants' quotes
Verifiable	Confirming status of employee	*"If (someone) presents their (government) card, people can make a confirmation by calling (the agency), they can refer to the website to verify whether the division exists..." (P007)*
	Point of reference	*"Sometimes when the public calls and we don't know the extension number, I advise them to refer to our website" (P012)*
	To establish authenticity	*"I think it is good which means they get what they want and confirms it's true." (P007)*
Locatable	Organisation's information	*"...my name is included in [Department J] organisational chart…. The website will disclose where I work..." (P004)*
	Physical location	*"Got the names (from the website), then came to the office and look at (our) car's number plate so they will follow and things like that." (P010)*
	Whereabouts	*"Mmm, can detect that this person is here." (P004)*
Discoverable	Can be found	*"...the advantage? Easy to find (by the public)." (P004)*
	Listed	*"...so they can't say 'I don't know your office number' because by right they can look for it on the website." (P006)*

Categories	Code label	Excerpt from participants' quotes
Identifiable	Provide clues to identity	*"But those who are good in analysis, they are able to analyse who he is, who he was. So it is not, not good for those individuals." (P005)*
	Can be identified	*"Auditor will be targeted. 'Oh this is the person who failed us'. Saw his name, gotcha!" (P010)*
	Easy to recognise	*"Because felt like ah, they knew our face, better don't [laugh] later they will able to recognise (me) anywhere..." (P006)*
	Linked information	*"Then, sometimes the news hid the name, but let say it publishes the work position. So when the public read the news, they will know the person, right?" (P008)*
Searchable	Accessibility of information through search engine	*"If you search using Google, try to search my name [P010]. It will point to the directory err [Department C], [Department C] staff directory." (P010)*
	Internal search feature on organisation's website	*"...but if we don't have (names) or we just want to search within a division, we click that division and it will appear..." (P016)*
Contactable	Direct to specific employee	*"I browse (websites) there are names, I can contact directly that's all." (P009)*
	Improved communication	*"...easy for others to contact me. Communication will be easier." (P011)*
	Unexpected contact	*"So when I was in [Department D], occasionally I received calls from friends which I didn't expect, when I asked them where (did they get my contact number)? Directory [laugh]..." (P007)*
Accurate	Exact spelling	*"...for me I think maybe because sometimes I don't know the exact spelling of that person's name." (P008)*
	Precise information	*"So far the information is correct, name and email is correct." (P008)*
	Review mechanism	*"...I noticed some time ago, once they (P008 organisation) conducted an exercise to reconfirm, reconfirm the correctness of information." (P008)*
	Regularly updated	*"Once a while I need to know updated (staff) information because the book (directory) is not. So I browse the website because it is supposed to (be updated)." (P014)*

5.2.6.5 Theme 5: Commitment to public service ethos

This theme comprises of one sub-theme which is *trust in organisations*. Three main categories were analysed in the main theme, while two categories reside in the sub-theme. The theme portrays the high commitment of participants in exercising their duties. In upholding the civil service professionalism, most participants cited *responsibility* and providing *services* to the public as their main duties at work. As government employees, participants were expected to *follow orders* of the government and at the same time act as *government's agent* in facilitating services to the public. Furthermore, becoming a government employee corresponds to being viewed as public property.

It can also be seen that obligatory disclosure was viewed as a means for increasing service delivery because it could provide faster services, easy communication between the employee and the public, and assist in contacting relevant employees directly.

Table 5-33: Codes, categories and excerpts for Theme 5

Categories	Code label	Excerpt from participants' quotes
Civil servant professionalism	Responsibility	*"...but I think positively because everyone has responsibilities. For me what is important is the feeling of responsibility..." (P011)*
	Follow orders	*"It's not to say I am happy but [laugh] we follow the policy...We are just following orders." (P001)*
	Service oriented	*"...because it is our job is to give the best to the public." (P009)*
	Public property	*"...as a public servant, it's understandable that we are like in a way public property..." (P006)*
	Government's agent	*"Easy to inform the public...Because we represent the government." (P002)*

Categories	Code label	Excerpt from participants' quotes
E-Government initiatives	Right to information	*"... and they have the right to know about certain information..." (P006)*
	Transparency	*"Especially with the government servant. We have to be even more to be seen as, even more honest because the public will look at us..." (P020)*
	Access to relevant employees	*"So we have to know who should be contacted, which unit, which section, because like us... of course every, err agency has their own person in charge." (P010)*
Improve efficiency	Faster service	*"Err so when we speak with the respective officer directly, it's easier for me to get confirmation..." (P002)*
	Easy communication	*"...for me, easy for communication." (P011)*
	Direct contact	*"...they don't want (their calls) to be passed around so they want to contact directly, want a faster action." (P007)*

The participants stated that it is important for the public to have access to information while some of them mentioned it as the public's right to know certain information. *Transparency* emerged as another factor concerning obligatory disclosure. Two participants highlighted this concept. All in all, these three code labels were combined to generate the *e-Government initiatives* category.

Sub-theme 5: Trust in organisation

Trust in organisation is a sub-theme that consists of two categories: *organisation is limiting disclosure* and *protected by organisation.* Almost half of the participants pointed out that organisations were disclosing basic information, which is not detailed about employees. As such, information published should be limited just to serve the purpose of delivering services to the public.

The participants added that their organisations had taken reasonable steps to handle security and safety precautions to prevent any untoward incidents. Examples such as 'filtered information' were put forward to express confidence in the organisation in publishing an employee's information. Likewise, increased security surges participants' trust in the government for protecting its data. Henceforth, this theme represents the employees' trust to the government (i.e. their organisation).

Table 5-34: Codes, categories and excerpts for Sub-theme 5

Categories	Code label	Excerpt from participants' quotes
Organisation is limiting disclosure	Basic information	*"Information (that was disclosed by organisation) was basic..." (P008)*
	Not detail	*"But information that government disclose is not much, just names (and) email addresses…" (P011)*
Protected by organisation	Safety precautions	*"I think on most of our websites, they're selective, they've screened (the information)… On government websites, I, I told you earlier there is not much…it's filtered." (P020)*
	Increased security	*"…because nowadays, especially after government's website was hacked, hacked since months ago, and government have increased their firewall and from what I see our data is very protected. Then protection has improved. So I don't feel (worried), not feeling (worried)." (P003)*

5.2.6.6 Theme 6: Lack emphasis on privacy

Four major categories emerged in this theme: *organisation policy*, *not informed on the process of disclosure, low employees' participation*, and *control over personal information disclosure*. A prominent category in this theme is *organisation policy,* that could inform how the disclosure was conducted in the government's organisation. It was discovered that the disclosure of employees' information depended on each agency's decision. It can be seen that agencies were inconsistent in disclosing employees' information. Thus, five participants believed that there was no policy on obligatory disclosure. In some agencies, all employees were disclosed, but in others only selected employees were published on their websites (refers to the staff directory).

Table 5-35: Codes, categories and excerpts for Theme 6

Categories	Code label	Excerpt from participants' quotes
Not informed on the process of disclosure	Unsure of the process	*"I think it started when I dealt with the IT unit, they updated staff's directory, I think it is like that." (P007)*
	Tried to explain	*"But as far as I know, when a new employee reports for duty, err IT unit will upgrade, update, our new employee automatically on our website." (P004)*
Organisation policy	Depends on agency	*"[Ministry A] is difficult to find, while [Division B] is easier. [Ministry A] is difficult, others such as (district) council, so far is ok." (P003)*
	Disclose all employees	*"They (past department) requested to lists all their employees…" (P001)*
	Disclose selected employees	*"But err for certain departments, such as [Department A] it's according to work level. Maybe up to EO or category B or category C or up to chief clerk, according to work level." (P014)*
	No disclosure policy	*"No, there is no circulars." (P009)*
Low employees' participation	Consent not sought	*"No, not informed (of the disclosure)" (P009)*
	Decide by organisation	*"Because it is the organisation's right [laugh]." (P013)*
Control over personal information disclosure	Cannot do anything	*"If it is the government's policy to publish photo, then I can't do much." (P003)*
	Filtered information	*"Those (information) that is not important, I wouldn't allow (it to be published). So I check it on my own."(P005)*

The participants mentioned not being informed on the process of obligatory disclosure. More than half of the participants were in the dark about the obligatory disclosure process. However, three participants tried to explain what they understood it to be, based on what they heard after being in the public service. In addition, consent from employees was not sought for publication of their information. Two-thirds of the participants admitted to not being consulted, while four participants reported that it was decided by the organisation. *Control over employees' personal information disclosure* emerged as a category based on four participants' data, involving failure to interfere with the disclosure of personal information and capability of controlling the disclosure.

5.2.7 Summary

This section summarised results from the semi-structured interview data. The thematic analysis undertaken assisted in categorising and thematically grouped data into providing descriptions and perceptions about obligatory disclosure. Furthermore, the analysis of data usefully identified the norms, behaviours, privacy related issues, organisational factors and practices about the phenomenon including risks and threats posed to government employees. The next chapter presents the findings which provide explanations about the phenomenon of interest to a greater degree.

CHAPTER 6

Findings

6.1 Introduction

This chapter presents the research findings from the data collection i.e. documentation, in-depth semi-structured interviews and web content analysis. Following the analysis of the results in the previous chapter, this chapter investigates how obligatory disclosure can affect employees and explores the implications for privacy. This current chapter will further discuss the research findings, in relation to relevant literature, particularly from the context of privacy.

6.2 Findings

The previous chapter reported the results of web content analysis, uncovering different types of employees' personal information and the quality of information disseminated from government websites. Six themes have emerged from in-depth semi-structured interviews, and this section will provide interpretations of these themes by combining the results from documentation and web content analysis with those of the in-depth semi-structured interviews.

6.2.1 There is low privacy concern and lack of privacy awareness among employees regarding obligatory disclosure

Although in general participants showed awareness about the publication of their personal information on their official organisation's website, most of the participants have little concern about privacy around the availability of their personal information on their organisation's website.

During the initial stages, when answering questions about employees' information disclosure, and later when considering their own information being disclosed on their official organisation's website, a large number of participants were not concerned about privacy. Although they were highly aware of obligatory disclosure (including their own), as presented in section 5.2.4, except for a few participants the key focus regarding obligatory disclosure was towards the benefits of it rather than any issues around privacy issues.

The participants' awareness of the disclosure of their personal information was evident with their ability to discern the different types of personal information and attributes that were disclosed about them and where these disclosures occurred (i.e. on which section of the website). However, most of the participants referred to the 'staff directory' when discussing obligatory disclosure. As example:

"...in the Ministry (website) there is (my information) err directory style the staff directory, my name and what I do." (P018)	*"...di (laman web) Kementerian tu dia memang ada (maklumat saya) err apa ni style direktori tu kakitangan direktori kakitangan tu, nama saya dan juga apa tugas saya." (P018)*

Box 6-1: Theme 1-P018

Indeed, the staff directory feature was found to have high visibility in all websites. The feature is visible from the homepage and meeting Basu's three clicks guidelines (Basu, 2002). Further questioning over the attributes that were available revealed that names, telephone number (official), email address (official), working position, division or unit, work scope, and photograph were listed as the common types of information disclosed. This information is similar to what was found on the websites, as reported in section 5.1.4.2.

While the 'staff directory' was identified during the content analysis as a major contributor to disclosing numbers of individuals in an organisation, it was not the only source of disclosure. Disclosure of employees' information was discovered to come from multiple sections of the website, such as news, organisation chart, activities, announcements, documentations and reports. However, only a few employees were aware of other possible contributions to disclosure other than the staff directory.

Harmless

A large number of participants viewed the disclosure as only revealing ‘basic’ information about them. Most participants were certain that the published details were limited to specific information only, e.g. name, telephone number (official), email address (official), and working position. As a result, the personal information revealed was regarded as ‘not detailed’ and ‘basic’. They described it nicely using the phrases ‘not detail’ and ‘basic’ to illustrate the extent of disclosure.

“Ha it’s enough because basic information is enough, we only need to know name, working position, telephone number and email (address).” (P010)	*“Haa cukup dah sebab maklumat basic cukup lah, kita perlu orang tau nama, jawatan, no telefon dengan emel.” (P010)*

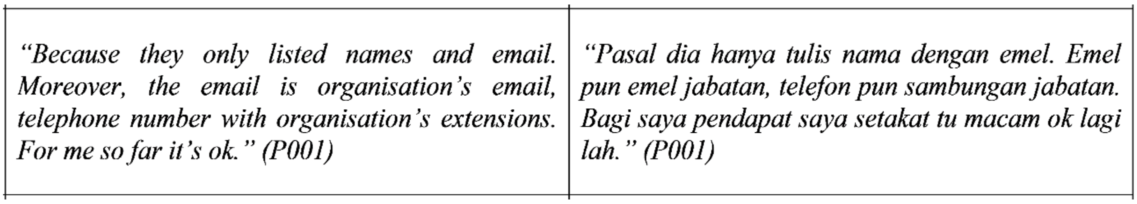
Box 6-2: Theme 1-P010

From the participants’ point of view, they indicate that the details revealed are not exhaustive and consist of only basic information. As a result, they assumed that the disclosure may not pose any privacy risk to the employees. Additionally, participants explicitly argued that the disclosure of ‘limited’ information may be too inadequate for fraudulent purposes.

“I believe if it’s because (of that information), it cannot be used (for bad purposes), because it is only name, extension number, unit, email address, email only, official email.” (P001)	*“Saya rasa kalau dia pasal, saya rasa tak boleh tak boleh diguna pakai pun, sebab dia pasal dia kat sini pun dia ada cuma nama, nombor sambungan telefon, dengan unit, err emel. Emel saja, emel emel jabatan.” (P001)*

Box 6-3: Theme 1-P001

This remark gave some indication that personal information disclosure may lead to a privacy risk. They further justifies their view regarding the limited information that is published on an organisation’s website:



"Because they only listed names and email. Moreover, the email is organisation's email, telephone number with organisation's extensions. For me so far it's ok." (P001)	*"Pasal dia hanya tulis nama dengan emel. Emel pun emel jabatan, telefon pun sambungan jabatan. Bagi saya pendapat saya setakat tu macam ok lagi lah." (P001)*

Box 6-4: Theme 1-P001

This view could suggest that the personal information that is related to organisations or professionals would not have a significant privacy impact on individuals. They seem to share the view that it's the organisation that should be more worried instead of the employees. This highlights differing perceptions of personal information and professional information, before they were brought to the attention of ECtHR (Stahl, 2008).

Similarly, one participant holds the opinion that the employees' personal information is not openly displayed and thus this may deter people with malicious intentions because of the complexity of compiling the details (Appendix H – Box 6-5: Theme 1-P008).

The participant emphasises the fact that employees generally feel safe with obligatory disclosure. The potential reasons for this were stated, particularly around the limited type of personal information that was disclosed, and the purpose and manner of the disclosure, which leads to the perception that obligatory disclosure is safe for employees. Although personal information was available publicly, this was not seen as a crucial problem with regards to safety and privacy. Potential attacks and possible exploitation of personal information were not seen as threats on this basis.

Thus, these perceptions may influence employees' decisions around deciding on whether obligatory disclosure has any risk. In contrast, research findings on web content analysis discovered that 23 different types of personal information were available publicly on high-ranked Malaysian Government websites. This large number presents a wide scope of personal information disclosure and could heighten concerns around privacy and security. This indicates a lack of concern around privacy and a low degree of awareness among employees on the extent of obligatory disclosure.

Sense of security

In addition, participants held the view that they would not be targeted because they are ‘nobody’ and not an important person.

“...but so far I think no outsiders will just simply want to find information about me...if we are in support (category) it shouldn’t be a problem, right? (But) what about the top management?” (P011)	*“...cuma setakat ini tak ada lagilah orang luar yang saja-saja nak cari maklumat saya itu tak adalah saya rasa...kalau kita setakat pihak sokongan ini tak ada masalah, kan? Kalau pihak atasan, kan?” (P011)*

Box 6-6: Theme 1-P011

This response was more evident among employees within the support group category, where participants assumed that nobody is interested in their personal information, since they – unlike top management - did not hold important positions in the organisation. Participants seem to be suggesting that their personal information disclosure will not attract malicious parties, and hence this made them feel safe. As expressed:

“...because I think I am just an ordinary person so the effect is not big.” (P007)	*“...sebab saya rasa saya manusia biasa so saya tak nampak ‘effect’ itu terlalu besarlah.” (P007)*

Box 6-7: Theme 1-P007

Another participant captures this idea and links it with the limited amount of information that was disclosed.

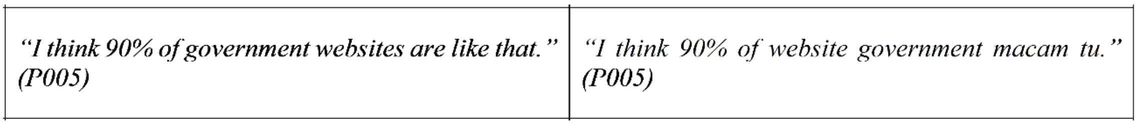
“Maybe for me as a normal person and a civil servant, to me privacy is not a big issue because in terms of exposure, my information is not much (being revealed).” (P016)	*“Mungkin bagi kita sebagai orang biasalah dan juga penjawat awam bagi saya privasi itu tak menjadi satu isu yang besarlah sebab kalau dari segi pendedahan pun agak kurang pasal maklumat kita tadi.” (P016)*

Box 6-8: Theme 1-P016

The responses by participants suggest that employees feel a high sense of security, despite their personal information being disclosed. This appears to be on account of the assumption that they are not being targeted as they are a normal and ordinary civil servant.

Cultural

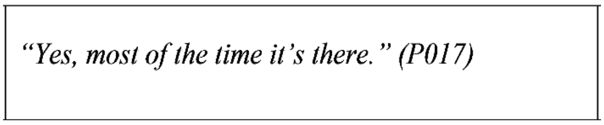
Another reason that could influence privacy concern are cultural factors (Bellman et al., 2004). Based on the interviews, it was clear that participants perceived obligatory disclosure as a normal and natural practice with Malaysian Government websites. Indeed, participants had clearly got used to obligatory disclosure, up to the extent that participants saw it as part and parcel of being a public employee. Furthermore, some participants saw the practice as an extension and important element of government websites. Phrases such as *"It's a must"*, *"That is normal"*, and *"must have."* can be interpreted to mean that the practice of disclosing employees' information is widely implemented. In an explicit attempt to illustrate the extensiveness of obligatory disclosure, a participant stated:



"I think 90% of government websites are like that." (P005)	*"I think 90% of website government macam tu." (P005)*

Box 6-9: Theme 1-P005

Similarly, another participant concurred and shared their thoughts that it is widespread:



"Yes, most of the time it's there." (P017)

Box 6-10: Theme 1-P017

The participants' remarks are in accordance with the findings from the web content analysis, which discovered that all government websites reveal their employees' information generously. As participants were accustomed with this disclosure, they generate a set of beliefs and assumptions around the practice. The belief implies that obligatory disclosure is viewed as a normal 'thing' for government websites. This set of beliefs and norms, which dictates the way in which people define things, influences their perception around privacy concerns (Bellman et al., 2004; Milberg et al., 2000). As norms and practices are considered to be part of culture (Stahl & Elbeltagi, 2004; De Long & Fahey, 2000), from the context of this study, the culture of an organisation can be suggested to influence participants' views on obligatory disclosure.

Since Malaysia has been characterised as a collectivist country (Hofstede, 2001), it has the tendency to portray a characteristic society that has a strong and close relationship with others, and is more sharing of information and togetherness. As a collectivist society, it may suggest that people will not prioritise privacy. Drawing from Hofstede's cultural dimension, this could suggest that cultural values may influence concerns around information privacy for employees.

When participants were queried about the process that led to their information appearing on their organisation's website, most of them were unsure because they were not informed about it. Interestingly, while participants were left in the dark about how their personal information was being processed, there was also no effort from them to make enquiries on this subject with their organisation.

"...so IT division will publish it. I am not sure because I didn't ask at all." (P011)	*"... so Bahagian BTM yang siarkan benda itu. Saya pun tak pasti sebab saya tak pernah tanya pun." (P011)*

Box 6-11: Theme 1-P011

It can also be observed that they have limited knowledge about the process and at the same time were not concerned about how their information was disclosed on the organisation's website. This could indicate that participants might think that obligatory disclosure was less important because every employees' name was also being published. Furthermore, as the phenomenon was widely observed by the participants, they will perceive it is as a natural and common practice - as described above. Thus participants believe that there is no necessity in asking about what is considered to be normal and natural within the organisation. Therefore, most participants take this disclosure for granted and show less interest in enquiring for reasons.

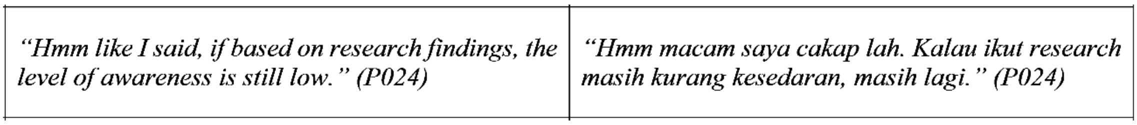
Theme conclusion

Here, the assumption deduced from participants' responses is that privacy was not emphasised as an important issue in the context of obligatory disclosure, and was instead seen as a natural process. This can be seen when participants only discussed privacy issues after privacy and personal information topics were brought forward, while for the rest obligatory disclosure did not raise any privacy concerns except for in a few cases. Although aware of obligatory disclosure, participants instead focused largely on staff directory as the source of this. There are three key reasons for a lack of privacy concern and awareness. First is the perception that obligatory disclosure is safe; second is the high sense of security among government employees; and third is the organisational culture that was experienced by the employees.

However, there was an indication that some participants were more concerned than others. Based on the interviews, only a small number of participants demonstrated a high level of concern around privacy around the disclosure of their personal information, either on the Internet or organisation’s website. Three participants showed concern with the publication of personal information on their organisation website and two participants held the consistent view that obligatory disclosure affected the privacy of employees, right from the beginning of the interview.

Commentators

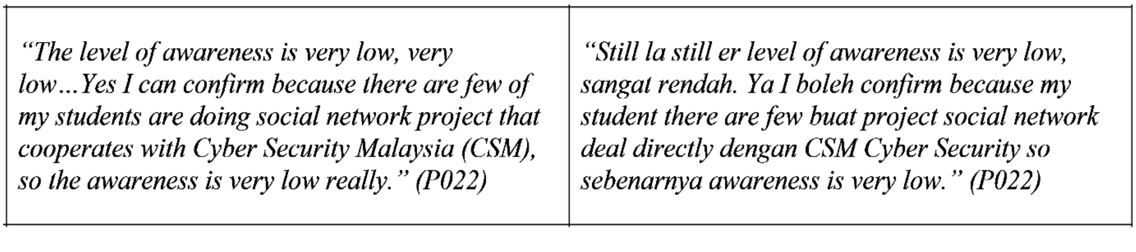
All three commentators unanimously agree that in general privacy awareness among Malaysians is still low.



“Hmm like I said, if based on research findings, the level of awareness is still low.” (P024)	*“Hmm macam saya cakap lah. Kalau ikut research masih kurang kesedaran, masih lagi.” (P024)*

Box 6-12: Theme 1-P024-commentator

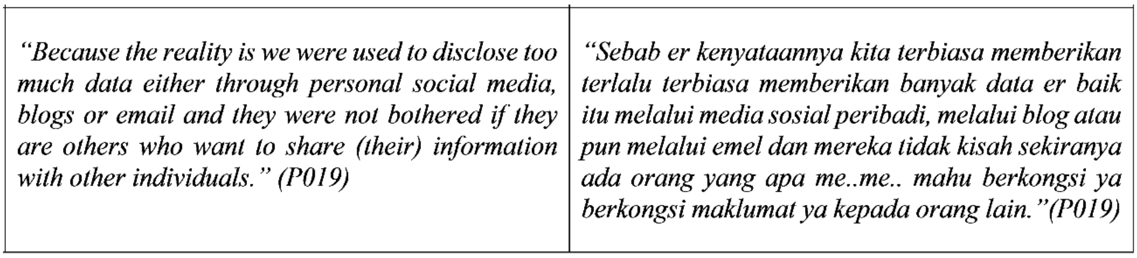
Another commentator concurred and supported it with their research findings:



“The level of awareness is very low, very low…Yes I can confirm because there are few of my students are doing social network project that cooperates with Cyber Security Malaysia (CSM), so the awareness is very low really.” (P022)	*“Still la still er level of awareness is very low, sangat rendah. Ya I boleh confirm because my student there are few buat project social network deal directly dengan CSM Cyber Security so sebenarnya awareness is very low.” (P022)*

Box 6-13: Theme 1-P022-commentator

Malaysians were accustomed towards disclosing information to other individuals in many ways, and this practice was observed with their online behaviour.



"Because the reality is we were used to disclose too much data either through personal social media, blogs or email and they were not bothered if they are others who want to share (their) information with other individuals." (P019)	*"Sebab er kenyataannya kita terbiasa memberikan terlalu terbiasa memberikan banyak data er baik itu melalui media sosial peribadi, melalui blog atau pun melalui emel dan mereka tidak kisah sekiranya ada orang yang apa me..me.. mahu berkongsi ya berkongsi maklumat ya kepada orang lain."(P019)*

Box 6-14: Theme 1-P019-commentator

Although the commentators conclude that the level of privacy concern is low among Malaysians, it should be noted that the basis of the commentator's statement is based on general privacy concerns, whereas this research is examining a situation-specific phenomenon that may further lower people's privacy concerns and awareness.

According to the commentators, the lack of privacy concern and privacy awareness may also be largely contributed to by cultural factors. As this research discovered, cultural factors may influence employees' privacy concern and awareness. It is worth noting that lack of privacy concern and privacy awareness were identified in incidences of obligatory disclosure and not in general. The privacy behaviour and concern of participants is presented in the next finding.

6.2.2 Employees' privacy concern is influenced by specific context

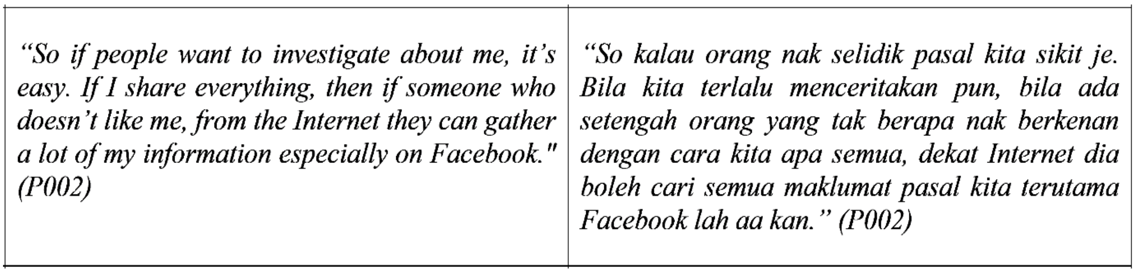
Privacy concern over personal information on social media.

As observed during the interviews, in general participants understand what privacy is although this differs in definition. Participants associated the concept of privacy with personal information. Although most participants struggled to define what constitutes personal information, generally they referred to it as information about themselves.

In order to assess participants' privacy perception and their approach to their personal information, an investigative inquiry into their privacy behaviour on social media and the Internet was held. This then enabled the researcher to provide a contrasting view of each perspective and provide insights into the differences in attitude towards privacy within different contexts.

Most of the participants admitted to having at least one social media account, which invariably included Facebook. Therefore, Facebook was chosen as a sample for social media usage in this study. From a total of 19 participants, 16 participants owned a Facebook account and 11 participants had configured their account to private, while five allowed public access to their profile. The final three participants did not have a Facebook account.

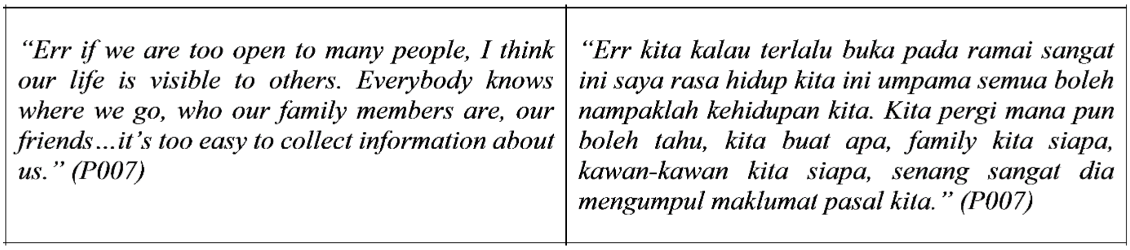
Findings showed that all participants who used Facebook displayed similar concerns over their privacy on social media. All participants that had configured their account to private showed consistent concern with the disclosure of their personal information to outsiders, and improper usage of their personal information. They raised concerns over the collection of their personal information by unwanted parties and preferred not to disclose everything on their Facebook account:



"So if people want to investigate about me, it's easy. If I share everything, then if someone who doesn't like me, from the Internet they can gather a lot of my information especially on Facebook." (P002)	*"So kalau orang nak selidik pasal kita sikit je. Bila kita terlalu menceritakan pun, bila ada setengah orang yang tak berapa nak berkenan dengan cara kita apa semua, dekat Internet dia boleh cari semua maklumat pasal kita terutama Facebook lah aa kan." (P002)*

Box 6-15: Theme 2-P002

In addition, another participant gave similar reasoning:

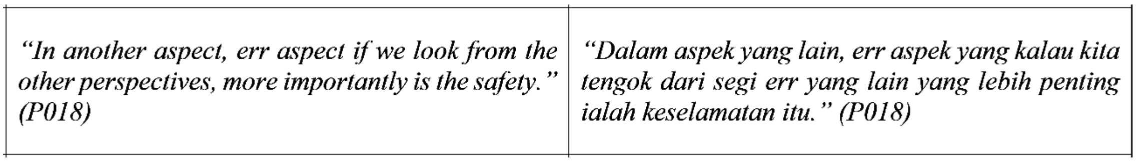


"Err if we are too open to many people, I think our life is visible to others. Everybody knows where we go, who our family members are, our friends…it's too easy to collect information about us." (P007)	*"Err kita kalau terlalu buka pada ramai sangat ini saya rasa hidup kita ini umpama semua boleh nampaklah kehidupan kita. Kita pergi mana pun boleh tahu, kita buat apa, family kita siapa, kawan-kawan kita siapa, senang sangat dia mengumpul maklumat pasal kita." (P007)*

Box 6-16: Theme 2-P007

This suggests that participants understand that personal information available on their social media account can be collected by anyone who can view that information. The phrase: *"too open to many people"* indicates that participants were concerned that their information was publicly available, and that this can invite privacy risk. Another concern that was highlighted by participants is the collection of personal information. The participant phrase: *"...it's too easy to collect information about us."* suggests that the awareness of the ability of their personal information in OSN to be collected was high. Therefore, participants are cautious about their personal information on OSN (Appendix H – Box 6-17: Theme 2-P013).

There was also evidence that participants could relate that the disclosure on Facebook may influence their real-world safety:

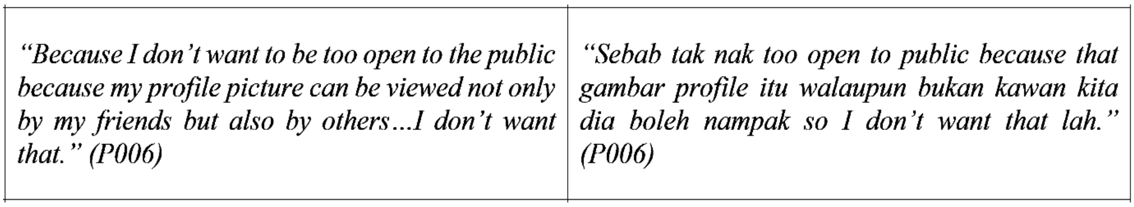


"In another aspect, err aspect if we look from the other perspectives, more importantly is the safety." (P018)	*"Dalam aspek yang lain, err aspek yang kalau kita tengok dari segi err yang lain yang lebih penting ialah keselamatan itu." (P018)*

Box 6-18: Theme 2-P018

Most of the participants were of the view that personal information can be collected and be used beyond the intended purpose (Smith et al., 1996). Another concern regarded the availability of their personal information online (Madden & Smith, 2010; Rainie et al., 2013).

In addition, to understand the participants' perception and privacy behaviour towards their personal information on social media, the researcher delved into the participant's Facebook profile attributes. Many participants expressed concerns over their privacy when speaking about their information on Facebook. They were fairly careful about disclosing their profile information publicly. For example, when asked why they didn't upload photographs of themselves onto Facebook, they stated:

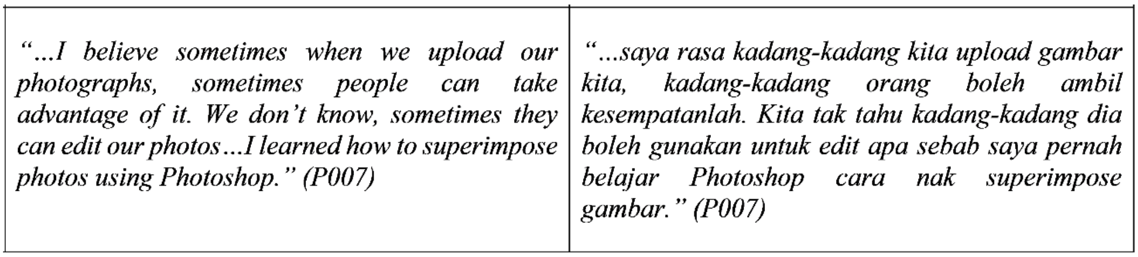


"Because I don't want to be too open to the public because my profile picture can be viewed not only by my friends but also by others...I don't want that." (P006)	*"Sebab tak nak too open to public because that gambar profile itu walaupun bukan kawan kita dia boleh nampak so I don't want that lah." (P006)*

Box 6-19: Theme 2-P006

In addition, they explain that their concerns is regarding the collection and use of their photographs (Appendix H – Box 6-20: Theme 2-P006).

Another concern is related to the improper use of personal information. One participant, due to his informal knowledge in IT, gave examples of the improper use of personal information:



"...I believe sometimes when we upload our photographs, sometimes people can take advantage of it. We don't know, sometimes they can edit our photos...I learned how to superimpose photos using Photoshop." (P007)	*"...saya rasa kadang-kadang kita upload gambar kita, kadang-kadang orang boleh ambil kesempatanlah. Kita tak tahu kadang-kadang dia boleh gunakan untuk edit apa sebab saya pernah belajar Photoshop cara nak superimpose gambar." (P007)*

Box 6-21: Theme 2-P007

Further investigation discovered that nine participants were avoiding using either their full name or an identifiable photo of themselves. Out of the five that allowed public access, as mentioned earlier, three participants were employing this strategy. Thus, a total of 14 participants were involved in a strategy that avoided direct identification on their Facebook account. This leaves only two participants who disclosed their real name and photographs on their publicly available profile page.

It was evident that participants understood the risks of disclosing personal information on their social media accounts. Their personal information could be collected and used for unintended purposes (Smith et al., 1996). Participants held the view that personal information, if it fell into the wrong hands, would invite violations of their privacy. This could be the reason why most participants configured their Facebook account to private - in order to limit the exposure of their personal information.

In addition, participants decided to use other privacy protection strategies in order to limit exposure about themselves. For instance, the practice of falsifying personal information was considered by more than half of participants to limit their exposure on social media. Participants were found to use fictitious information on their profiles. Most of them disclosed inaccurate or false information in regard to two different personal attributes. The first was the 'name' of the profile holder, and the second was the profile pictures. Participants admitted to using different names from their real name in their profile.

"Even my name, I use a nickname." (P007)	*"Nama pun dah pakai nama samaran." (P007)*

Box 6-22: Theme 2-P007

Apart from names, images that could be used to identify them were also avoided in their profiles (for example Appendix H - Box 6-23: Theme 2-P006).

A total of six participants chose to present different profile pictures, such as photographs of their family members (e.g. children) or other images not related to them. The privacy behaviour of the participants suggest that they were avoiding being identified.

"Because I think err if people search for my name they can't find me, but they can identify me through photographs. So I don't, I don't want that to happen, both." (P010)	*"Sebab saya rasa kalau err sa, sa, kalau orang cari nama tak jumpa, orang boleh kenal kita melalui gambar. So saya tak nak, saya tak nak dua-dua tu biar boleh saya tak nak." (P010)*

Box 6-24: Theme 2-P010

It can be seen that despite participants having configured their Facebook profile to private settings, they still resorted to using a different name (or pseudonym) or unidentifiable photograph in their profile. This could be a strategy to alleviate their privacy concerns. Participants tried to avoid being identifiable by not using their full name and also falsifying information (e.g. name) to protect their privacy. Fabricating personal information is one of the individual strategies to maintain privacy and at the same time allow people to participate in and receive the benefits of disclosure (Petronio, 2002). In a study of e-commerce, individuals especially used these strategies with sensitive information (Metzger, 2007) and when perceived risks and privacy concerns are high (Lwin & Williams, 2003).

Employment information

In relation to the investigated phenomenon - which is disclosure by organisations - a participant's privacy behaviour towards their employment information was investigated. It basically refers to whether their employment information (e.g. occupation, organisation, working position) was disclosed on their profile. As presented in section 5.1.3, employment information scored highest on the disclosure index on government websites, which means that the extent of disclosure for this type of information is high. As employment information in obligatory disclosure is available to anyone, it is relevant to uncover how employees responded to this attribute on the OSN. Findings from participants showed that employment information was consistently selected to be kept hidden from public view on social media.

Three participants chose not to disclose employment information. Meanwhile, those who had disclosed their employment information had also included some additional form of privacy protection such as private settings, using a pseudonym, or profile pictures of others. In summary, there were only two participants whose profile uses their real name, real profile picture and provides employment information (in public view) as opposed to nine participants that admitted to filling in their employment information. Although some participants disclosed their workplace, they did not disclose their working position.

Similarly, some participants chose to withhold their employment information on their public profile. They cited privacy issues due to Facebook's ability to link users with similar characteristics. Interestingly, another participant that had their profile also publicly accessible (public settings) chose to hide his employment information from public view. The participant has instead decided to conceal their employment information from public view and explains why:

"Ok for example like err social media but (they) want to know about my work, where I work? To me it's like err privacy if public want to know because I am afraid it's sensitive." (P008)	*"Oklah contohnya kalau macam err sosial media tapi nak tahu pasal kerja saya dekat manakan? Bagi saya benda itu err privasi sikitlah kalau public nak tahu sebabnya takutnya sensitive." (P008)*

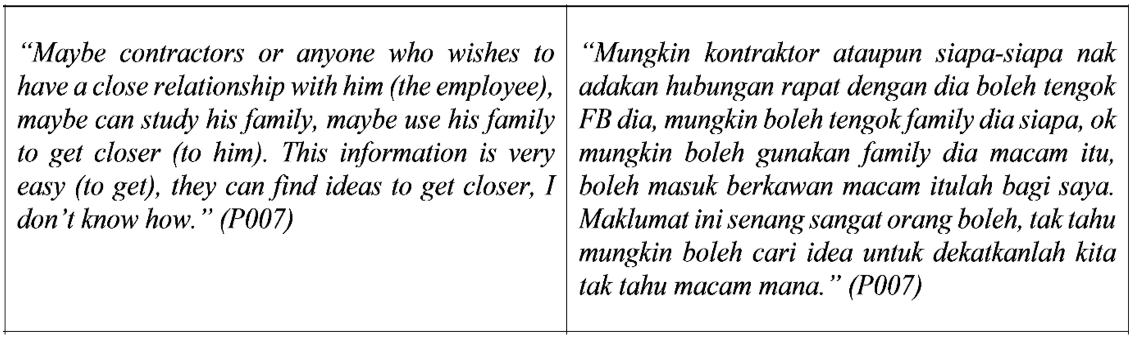
Box 6-25: Theme 2-P008

From participants' behaviour towards employment information it could be surmised that most of them were of the view that this information should not be easily made known to others. This assertion can be attributed to the fact that most of them have made an effort to limit this information on their personal Facebook profile.

As mentioned in section 5.2.5.2, some participants did not consider employment information as personal information. However, only one of these participants, allowed a public view of her employment information while others did not. This behaviour suggested that while others did not regard it as personal information, they may consider it as sensitive information. Thus employment information has a unique position on a Facebook user's profile page. Therefore, employment information has been perceived as a sensitive type of information for government employees.

A number of studies have indicated the sensitivity of employment information. Findings from 400 Canadian Facebook users revealed that employment information was disclosed publicly by less than 36% of their sample (Nosko et al., 2010). In fact, employment information was categorised as sensitive information (Aïmeur & Lafond, 2013; Nosko et al., 2010) and was the second least disclosed detail (after email address) among other types of sensitive information (i.e. profile pictures, photo albums, viewable friends, relationship status and medical and criminal records).

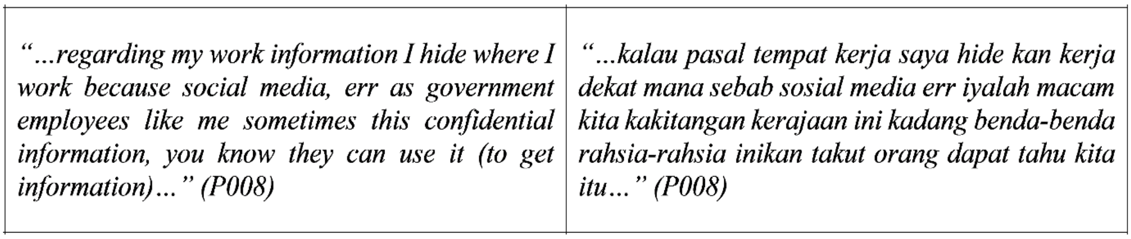
This could suggest that there are risks to government employees when using social media if their employment status is made known to public. They gave an example of using information from Facebook to target government employees, for the benefit of the attacker:



"Maybe contractors or anyone who wishes to have a close relationship with him (the employee), maybe can study his family, maybe use his family to get closer (to him). This information is very easy (to get), they can find ideas to get closer, I don't know how." (P007)	*"Mungkin kontraktor ataupun siapa-siapa nak adakan hubungan rapat dengan dia boleh tengok FB dia, mungkin boleh tengok family dia siapa, ok mungkin boleh gunakan family dia macam itu, boleh masuk berkawan macam itulah bagi saya. Maklumat ini senang sangat orang boleh, tak tahu mungkin boleh cari idea untuk dekatkanlah kita tak tahu macam mana." (P007)*

Box 6-26: Theme 2-P007

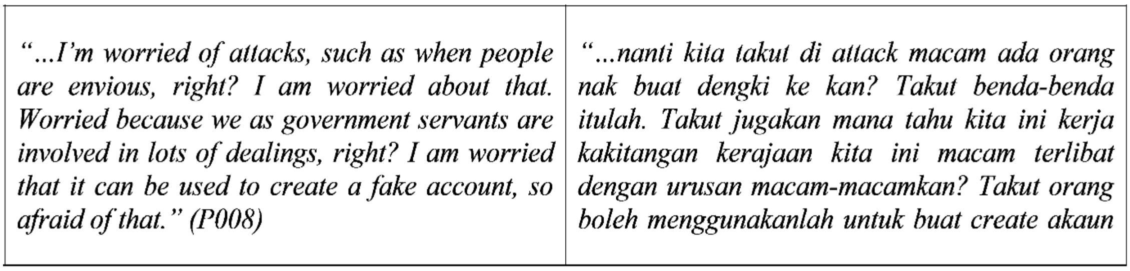
Another participant concurred, and attributed this to confidential information that government employees may have.



"...regarding my work information I hide where I work because social media, err as government employees like me sometimes this confidential information, you know they can use it (to get information)..." (P008)	*"...kalau pasal tempat kerja saya hide kan kerja dekat mana sebab sosial media err iyalah macam kita kakitangan kerajaan ini kadang benda-benda rahsia-rahsia inikan takut orang dapat tahu kita itu..." (P008)*

Box 6-27: Theme 2-P008

By revealing employment information on social media, both participants presented the risks that might be faced by government employees. They further expressed the vulnerability of this situation:



"...I'm worried of attacks, such as when people are envious, right? I am worried about that. Worried because we as government servants are involved in lots of dealings, right? I am worried that it can be used to create a fake account, so afraid of that." (P008)	*"...nanti kita takut di attack macam ada orang nak buat dengki ke kan? Takut benda-benda itulah. Takut jugakan mana tahu kita ini kerja kakitangan kerajaan kita ini macam terlibat dengan urusan macam-macamkan? Takut orang boleh menggunakanlah untuk buat create akaun*

Box 6-28: Theme 2-P008

Given the abundance availability of personal information that can be misused, concerns on an individual's safety and privacy issues have surfaced in the research. It can be seen that, when an employee is identified as a person in charge of an issue, besides searching through official means (e.g. department or official website), the public could also be searching through an unofficial platform (i.e. social media). One participant highlighted their experience of being harassed by members of the public through their personal Facebook account, receiving messages and requests from the public. The participant was surprised by the fact that the public hadn't contacted them through their department.

The public may see openly displayed employment information as an opportunity to communicate about official matters with government employees via their personal Facebook account. One participantoffered a good example of their personal experience:

"Because [Individual A] promoted my name boldly...So in his blog he published 'please contact [P010 name, P010 position]'...He did this as if he wanted to set me up, but err the result was that people attacked me on Facebook. Lots of people requested to become my friend and send me private messages. They message me about everything, asking about the issue. Instantly after that I changed all my security." (P010)	*"Sebab [individu A] mempromotekan nama saya dengan begitu gahnya...jadi blog dia semua dia letak hubungi [P010]... Dia buat macam tu seolah-olah macam sengaja nak kenakan saya tapi err kesannya pada saya orang akan attack di Facebook. Ramai sangat orang add untuk jadi friend dan inbox. Haa mesej saya apa semua tanya pasal [isu]. Ha terus saya memang lepas tu memang saya tukar security semua." (P010)*

Box 6-29: Theme 2-P010

In addition, the participant also changed the Facebook account name. The participant believed that by using their real name on Facebook, it increased their exposure to the public. Recalling their experience, they noted that the public might be able to identify them through their Facebook account by searching for their name. This could explain why all government employees choose to hide, or not disclose, their employment information publicly on Facebook.

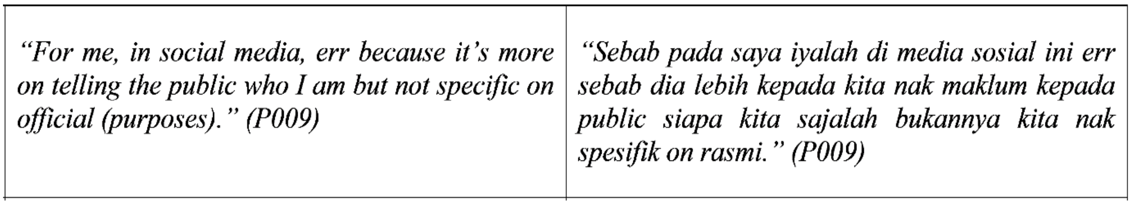
Social media usage

Analysis on the purpose of social media usage yielded five clear reasons given by participants. Participants were consistent in their usage of social media mainly for a social purpose. Most of them stated that their main purpose on social media was to get in touch with friends and family, followed by using it as a space for discussion, then to get updated on news and also as a channel to release tension.

"My main purpose is to get updated on my friends. Then one more thing sometimes Facebook will update news that I am (not) able to watch (on television)." (P011)	*"Tujuan utama dia saya nak tahu perkembangan kawan-kawan saya. Lepas itu satu lagi Facebook ini kadang-kadang dia akan update benda-benda yang kadang-kadang kita (tak) sempat tengok berita." (P011)*

Box 6-30: Theme 2-P011

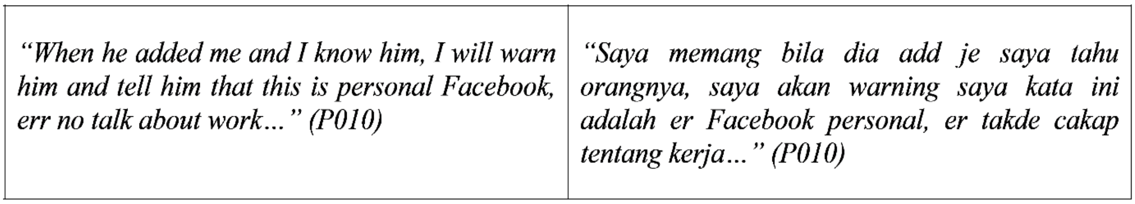
In fact, they explicitly mentioned that social media is not a platform for official purposes.



"For me, in social media, err because it's more on telling the public who I am but not specific on official (purposes)." (P009)	*"Sebab pada saya iyalah di media sosial ini err sebab dia lebih kepada kita nak maklum kepada public siapa kita sajalah bukannya kita nak spesifik on rasmi." (P009)*

Box 6-31: Theme 2-P009

As indicated by participants (for example Appendix H – Box 6-32: Theme 2-P010), they viewed their social media account as their social representation on the web. This could be another reason (besides risks) as to why they did not reveal their employment information on their Facebook profile. Another result suggested that participants were actively trying to separate their social and professional lives on social media. As an example, a participant was very clear about this:



"When he added me and I know him, I will warn him and tell him that this is personal Facebook, err no talk about work..." (P010)	*"Saya memang bila dia add je saya tahu orangnya, saya akan warning saya kata ini adalah er Facebook personal, er takde cakap tentang kerja..." (P010)*

Box 6-33: Theme 2-P010

Thus the use of social media, e.g. Facebook, by government employees was intended for a social purpose. The way they emphasised this, using the word 'warned', indicates the seriousness employees feel about creating boundaries on two different contexts. The most commonly mentioned reason for using Facebook by the participants was to keep in touch with friends and family. This indicates that employees are using Facebook mainly for building and maintaining relationships (Krasnova et al., 2010). Similarly, other research found that keeping in touch was consistently regarded as the main motivation for using Facebook (Joinson, 2008; Lampe et al., 2006). In addition, the findings of this study are consistent with a similar study in the Malaysian context where the primary motive for Malaysian Facebook users veers more towards the social aspect (Balakrishnan & Shamim, 2013).

Official purpose

Meanwhile, the purpose of obligatory disclosure was clearly understood by participants. As one participant stated:

"The purpose is to simplify official duties or (official) relations like what I said before." (P014)	*"Tujuan dia adalah untuk menyenangkan urusan rasmi atau perhubungan (rasmi) macam yang saya kata tadi." (P014)*

Box 6-34: Theme 2-P014

It could be surmised from this that participants perceived that the disclosure of details are directed only to those who require assistance and will need help from government officials. Hence, the information published was meant to be used solely for work purposes.

"...just to contact only for work purpose only" (P008)	*"...just untuk boleh berhubung dari segi kerja sajalah." (P008)*

Box 6-35: Theme 2-P008

Similarly, they viewed that their personal information is for the benefit of the public that need services or related information in a short space of time, and emphasises that it is purely for work purposes.

"If information on the (government) website, it's only for government related purposes." (P016)	*"Kalau setakat maklumat di laman web (kerajaan) ini, memang untuk tujuan urusan kerajaan sahajalah." (P016)*

Box 6-36: Theme 2-P016

Even when information about them appeared on the official website under 'current activities', they found it acceptable.

"... so when we clicked, it surfaces on official website, as official, it's not an issue for me." (P009)	*"... jadi bila (kita) klik keluar itu sebagai web, official, dia pada saya tak jadi satu masalah." (P009)*

Box 6-37: Theme 2-P009

Apart from the public, participants also admitted the importance of disclosure of employment details to other agencies, departments or ministries in the course of performing their work. Communication between different organisations and information sharing is undeniably important in meeting public expectations.

"...this is for other government departments for example [department A], our branches, [department B], (and) [department C] which are those that we normally deal with." (P014)	*"... ini untuk antara jabatan kerajaan lain, macam [jabatan A], cawangan-cawangan kita, [jabatan B], (dan) [jabatan C] yang selalu kita dealing." (P014)*

Box 6-38: Theme 2-P014

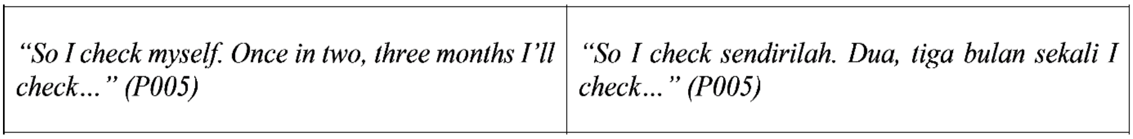
Based on participants' responses, it suggests that the purpose of disclosure plays an important role in shaping individuals' privacy perception and concerns. Different contexts, such as the social context, were found to influence individuals' privacy concern where participants had expressed higher concerns towards their information being viewable on OSN. However, when the same information was available on an organisation's website, participants did not project the same concern. As discussed in the literature review, the sensitivity of information depended on the context where it was observed (Nissenbaum, 2004). Employees saw OSN as a forum that may pose a risk towards them due to the abundance of personal information – both theirs and that of others. Conversely, information disclosure on an organisation's website was thought to be for specific purposes and intended only for customers/public for official reasons.

Disclosure on the Internet

Besides understanding the participant's privacy perception and behaviour on social media, it is also imperative to understand their privacy perception and behaviour on the Internet in general. This is to uncover the participants' underlying factors that may influence their privacy in a similar environment to obligatory disclosure (i.e. the Internet in general). Furthermore, information on the Internet is considered 'publicly available,' as anyone can see it, which is the same for information displayed on organisation websites.

Data suggests that participants showed an understanding that a large amount of their personal information was scattered throughout the Internet over various sources. As an Internet user, many participants mentioned that they normally conducted self-searches on themselves using search engines such as Google and Yahoo. Most of the participants chose Google as their preferred search engine while only one participant gave an example of using the Yahoo search engine. When querying about themselves, all participants reported that they used their full name as the query object. This was the only technique adopted by participants to gather information about themselves online.

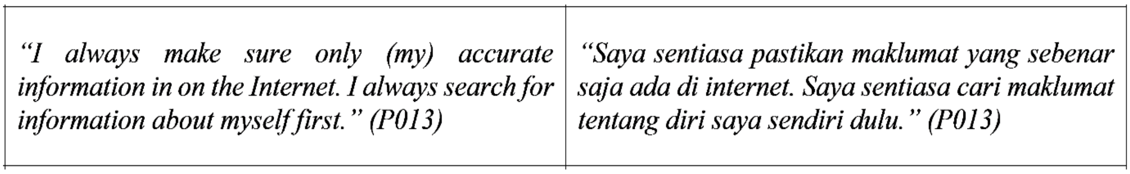
Despite one participant claiming to do it for fun, most participants' primary reason for conducting a self-search was concern over the availability of their personal information on the Internet. It can be seen that participants viewed their information on the Internet seriously. By implementing self-searching, they aimed to uncover their digital footprints and this implies concern to protect their personal information. While some participants were quick to assert that this was a seldom-done action, some were conducting this strategy regularly.



"So I check myself. Once in two, three months I'll check..." (P005)	*"So I check sendirilah. Dua, tiga bulan sekali I check..." (P005)*

Box 6-39: Theme 2-P005

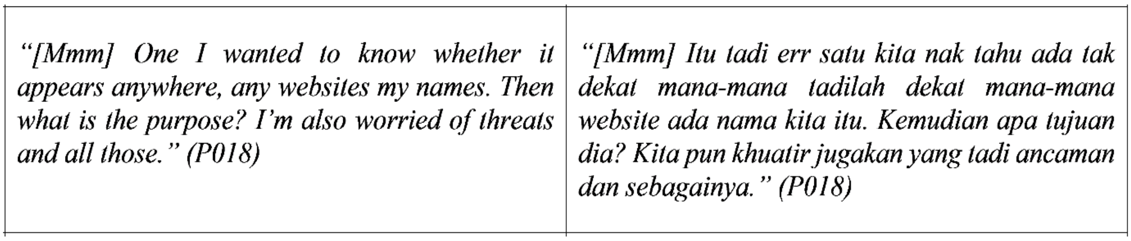
One participant stated 'curiosity' as the reason for their self-searching, while others were more straightforward:



"I always make sure only (my) accurate information in on the Internet. I always search for information about myself first." (P013)	*"Saya sentiasa pastikan maklumat yang sebenar saja ada di internet. Saya sentiasa cari maklumat tentang diri saya sendiri dulu." (P013)*

Box 6-40: Theme 2-P013

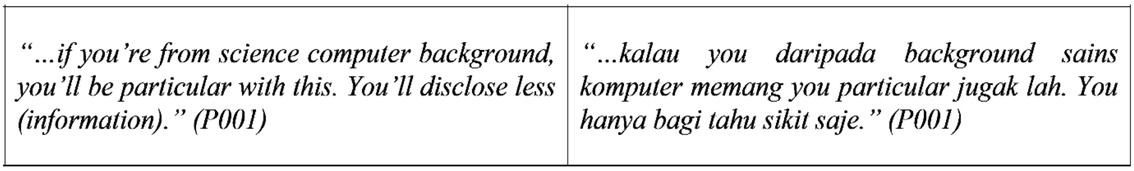
Participants were using a self-search to check on the availability of their personal information online. They were very concerned about the accuracy of their information. In addition, they also expressed the possibility of a 3rd party misusing their personal informationand highlighted threats as their concern:



"[Mmm] One I wanted to know whether it appears anywhere, any websites my names. Then what is the purpose? I'm also worried of threats and all those." (P018)	*"[Mmm] Itu tadi err satu kita nak tahu ada tak dekat mana-mana tadilah dekat mana-mana website ada nama kita itu. Kemudian apa tujuan dia? Kita pun khuatir jugakan yang tadi ancaman dan sebagainya." (P018)*

Box 6-41: Theme 2-P018

Some participants resorted to disclosing less information online to protect their privacy. One participant for example, suggests that there is very limited information about them available online:



"...if you're from science computer background, you'll be particular with this. You'll disclose less (information)." (P001)	*"...kalau you daripada background sains komputer memang you particular jugak lah. You hanya bagi tahu sikit saje." (P001)*

Box 6-42: Theme 2-P001

For participants that do not have a Facebook account, they tried to avoid friends that regularly upload information online (Appendix H – Box 6-43: Theme 2-P016).

However they admit that there is a difficulty in controlling others when seeking not to have information about them published on the Internet. Thus, this is one way to minimise publication about themselves on the Internet, which might cause privacy implications for them.

The participants' behaviour clearly indicates that they are aware of online privacy risks and threats. Participants showed their concern with the availability of personal information on the Internet. This searching for information on themselves points out the privacy awareness of participants (Madden et al., 2007). They are uncertain about the availability and accuracy of their personal information.

Theme conclusion

The findings above suggested that participants were highly concerned with their personal information on their social media account i.e. Facebook. Their privacy behaviour implies that they are aware of privacy issues when participating in social media. In addition, the reason for their concern is because of their understanding on the perceived risk associated with the disclosure.

In this research however, it was clear that participants' purpose of using social media was found to have no professional intentions, such as a formal organisation tool or a platform for self-promotion (Mangold & Faulds, 2009) but more towards maintaining friendships and family relationships. Research suggests that employees' desire to separate both segments were to avoid any conflicts caused by the collision of identities (Rothbard & Ramarajan, 2009). Employees were found to perform boundary regulation in relation to their privacy concerns. Self-censorship and controlling access (Skeels & Grudin, 2009) were strategies used by employees in the management of their personal information related to boundary regulation. The ability to control the means through which individuals manage their social interaction has developed a sense of ownership.

Similar privacy concern and privacy behaviour were expressed when participants were discussing their personal information on the Internet. Participants' behaviour when self-searching suggests that they were concerned with the disclosure of their personal information (Madden et al., 2007). The action of regularly conducting a self-search presented the value of their personal information to them. Most of the participants were using self-search as a way of managing their online presence and identity, to identify unwanted information that might have been disclosed (Marshall & Lindley, 2014) while one participant mentioned that this search was *'for fun'* (P002). Similarly, the entertainment purpose of self-searching was listed as the least motivational reason found in their study (Marshall & Lindley, 2014).

Participants used their name as a mean to assess their exposure on the Internet. This action was also known as 'ego search' or 'vanity search' in some research (Jones et al., 2008). This implies how participants sees the role of a 'full name' as personal identification on the Internet. Participants, expressed relief when discovered that their self-search result did not disclose their personal information.

"I feel relieved because if it can be found on the Internet, it means that it's easy for people (to do something bad)...there are potentials for threats." (P011)	*"Saya rasa lega sikit sebab kalau ada dekat Internet maksudnya senang sikit orang nak (buat benda tak baik)...potensi dia nak buat jahat dekat kita tu ada." (P011)*

Box 6-44: Theme 2-P011

As government employees, when conducting a self-search, found not only information about social activities but also their employment. Findings show that participants were uncomfortable when information about them can be linked to their professional and social activities.

The data analysis shows that participants have different privacy perceptions and privacy concerns when their personal information is disclosed on the social media or Internet (in general) when compared with their disclosure on their official websites. Participants were fairly careful in restricting their personal Facebook profile information to make it disappear from the public eye. Further, by conducting a self-search, participants were concerned with the availability of their personal information on the Internet. This behaviour suggests a high privacy concern from participants over their personal information.

In contrast to obligatory disclosure, participants did not show similar concerns and behaviour as above. Although their personal information can be viewed by anyone and the same attributes were also being disclosed on their official websites, the level of concern with this type of disclosure is not the same. This was shown on section 6.2.1 above, where most participants expressed the belief that obligatory disclosure is safe and low risk.

The conflicts between privacy perception and privacy concerns in different situations corresponds with the idea of privacy as 'contextual integrity' (Nissenbaum, 2004). Nissenbaum argues that the degree of privacy expectations of individuals differs according to context.

6.2.3 Obligatory disclosure impacts employees' privacy and productivity.

Information privacy concern is the extent to which an individual is concerned about organisational practices related to the collection and use of his or her personal information (Smith et al., 1996). In line with Xu et al. (2011) in defining privacy concerns contextually based on situations, this research defines privacy concerns as: 'employee's concerns about possible loss of privacy as a result of obligatory disclosure'.

Feelings with disclosure

With respect to a participant's feelings over obligatory disclosure, it was also observed that the feelings expressed when participants first experienced the nature of their obligatory disclosure were generally positive. Participants were quick to express their feelings when they first noticed or became aware that information about them is available on their organisation's website:

"Haa [laugh] oh very proud, [laugh] suddenly my name was there. It was never there before" (P004)	*"Haa [ketawa] rasa macam oh bangganya, [ketawa] tiba-tiba nama ada kan. Tak pernah-pernah ada kan haa." (P004)*

Box 6-45: Theme 3-P004

This similar response was echoed by another participant (Appendix H – Box 6-46: Theme 3-P002). It can be seen that most participants were excited and proud upon discovering their personal information had been published on their organisation's website. However, participants had generally experienced different feelings over the disclosure when they first noticed that their information was on the website. Feeling proud and excited were the most positive responses expressed. However, after a certain period of time had passed, with similar experiences of obligatory disclosure shown from one organisation to another, most participants felt differently. For example:

"Not like what it used to be [laugh]." (P004)	*"Dah tak macam dulu dah [ketawa]." (P004)*

Box 6-47: Theme 3-P004

Other participants hinted that they had got used to it and were feeling normal.

"The feeling? Now the feeling is that I'm used to it, it's already three times, seeing this, oh still the same [Laugh]." (P007)	*"Perasaan itu? Perasaan ini sekarang dah biasa dah, dah 3 kali dah ni, tengok oh sama saja [ketawa]." (P007)*

Box 6-48: Theme 3-P007

This feeling may result from the common government website practices that participants experienced as an employee. It suggests that most organisation websites were practising obligatory disclosure, and this feature was commonly found in public organisation websites similar to those found by Badrul et al. (2014). As a result, feelings of pride and excitement diminished over time.

"Ok look at it, it seems ok but let's say like there's no more excitement, no more, normal [laugh]." (P006)	*"Ok tengok itu ok juga tapi let say like kita tak adalah excitement itu dah tak adalah, normal [ketawa]." (P006)*

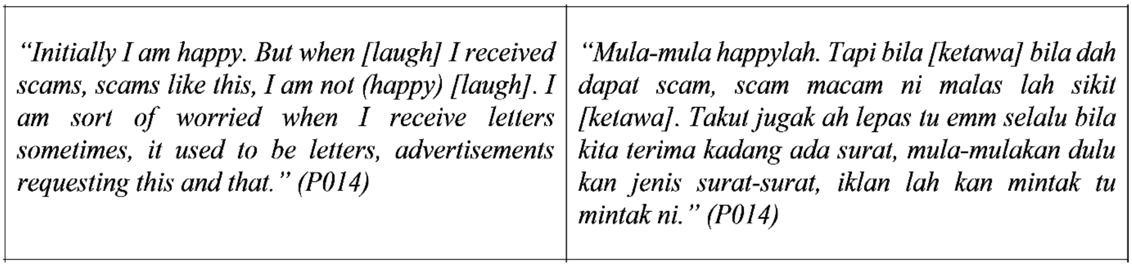
Box 6-49: Theme 3-P006

Apart from the feelings that this was normal, and expressions of pride and excitement, other feelings mentioned were: 'appreciated'; 'as a challenge'; 'safe'; 'sense of belonging'; 'embarrassed'; and 'happy'. As observed, none of the feelings were negative. However, when compared to current feelings, participants revealed three negative feelings towards their own disclosure. Among the feelings identified were: 'worry', 'vulnerable', and 'reluctant'. Five participants revealed these feelings while another three participants set their positive feeling as 'normal'. They were very clear about their obligatory disclosure:

"I feel like, (my) personal details are exposed to outsiders." (P003)	*"Asalnya macam (saya) rasa, personal detail tu macam telah didedah ke luar." (P003)*

Box 6-50: Theme 3-P003

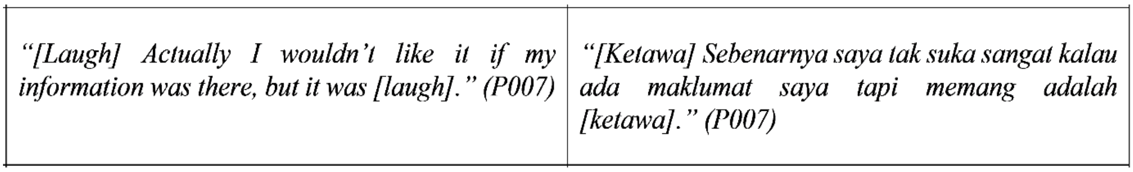
Prior to this current position, this participant could accept the disclosure as it was for an official purpose, however in this current posting the participant was feeling vulnerable. The same feeling from a long serving employee was discovered:



"Initially I am happy. But when [laugh] I received scams, scams like this, I am not (happy) [laugh]. I am sort of worried when I receive letters sometimes, it used to be letters, advertisements requesting this and that." (P014)	*"Mula-mula happylah. Tapi bila [ketawa] bila dah dapat scam, scam macam ni malas lah sikit [ketawa]. Takut jugak ah lepas tu emm selalu bila kita terima kadang ada surat, mula-mulakan dulu kan jenis surat-surat, iklan lah kan mintak tu mintak ni." (P014)*

Box 6-51: Theme 3-P014

It was clear that some participants tried to hide their feelings by saying that they had got used to it and did not feel anything. Initially they stated they were feeling normal, but later admitted to having reservations with the disclosure:



"[Laugh] Actually I wouldn't like it if my information was there, but it was [laugh]." (P007)	*"[Ketawa] Sebenarnya saya tak suka sangat kalau ada maklumat saya tapi memang adalah [ketawa]." (P007)*

Box 6-52: Theme 3-P007

By analysing participants' feelings when they first experienced obligatory disclosure and their current feelings, this study was able to uncover if there were any shifts of feeling that was brought by this phenomenon. Hence, it was possible to discover the influence of obligatory disclosure towards employees and any resulting privacy concerns without participants mentioning it.

From the participants' responses, negative feelings were demonstrated when participants had experienced obligatory disclosure for some time. All of the participants that shared these feelings had spent between 6 and 30 years in public service. These feelings indicate that there are privacy concerns with obligatory disclosure, but surprisingly most participants did not explicitly mention this. However, this could suggest that individuals that have experienced obligatory disclosure for a certain amount of time may come across privacy violations, which may influence their privacy concerns and behaviours.

However, as stated in section 5.2.6.1, at the beginning, all but a few participants showed little privacy concern over obligatory disclosure. Two participants - who were from the top management category - expressed high privacy concerns around the disclosure of an employee's information. These two participants were very clear from the beginning of interview that obligatory disclosure affected their privacy:

"That is why sometimes I'm worried of this privacy thing..." (P017)	*"Itu yang kadang-kadang yang I worried of this privacy thing..." (P017)*

Box 6-53: Theme 3-P017

Similarly, another participant, expressed their feelings without hesitation:

> *"Number one, I feel less privacy." (P005)*

Box 6-54: Theme 3-P005

The evaluation of participants' feelings demonstrated the inconveniences that can arise due to obligatory disclosure. Shifts in participants' feelings could be explained by the impact they had after experiencing obligatory disclosure. This was further supported by two participants who strongly believed that their privacy is affected by obligatory disclosure. This research suggests that obligatory disclosure may violate employees' privacy.

Privacy concern

It can be observed that most participants were inclined towards discussing privacy issues after questions on the concept of privacy and personal information were addressed. It was during the latter stage of the interview that privacy issues came to the fore. Their views on privacy were apparent when information about them on social media and the Internet was brought up. To investigate further influences on the nature of privacy, the researcher revisited questions regarding obligatory disclosure to gauge their views on privacy and contribute to a better understanding of the situation-specific context.

Participants exhibited uneasiness when their information was made available on a government website. An experienced middle level manager, concurred:

"Yes to me sometimes not all employees are comfortable when employees' information is displayed to the public, for public knowledge." (P009)	*"Iyalah betullah pada saya maklumat kakitangan kadang-kadang tak semua kakitangan itu dia selesa untuk dimaklumkan kepada public, untuk public tahu." (P009)*

Box 6-55: Theme 3-P009

There were concerns when information about them was made available to outside parties, specifically to those unintended third parties. Participants sincerely expressed their concern about this:

"I feel like, (my) personal details are exposed to outsiders." (P003)	*"Asalnya macam (saya) rasa, personal detail tu macam telah didedah ke luar." (P003)*

Box 6-56: Theme 3-P003

This statement clearly presents the participant's disappointment with the disclosure and implies the participant's understanding of the perceived risk that he may be susceptible to. They gave an insight into why the concern emerged:

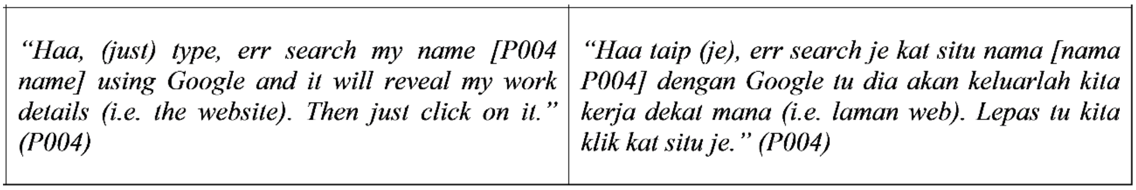
"Yes, people knew who we are, right?" (P005)	*"Ye lah people tau kita ni siapa kan?" (P005)*

Box 6-57: Theme 3-P005

This participant, from the top management category, strongly believed that the disclosure of employee information on official websites raises privacy implications for those employees. According to the participant, this disclosure allowed others to receive subjective information about an individual. This remark could indicate that there was an element of privacy invasion when personal details were exposed publicly.

For example, individuals who preferred not to be identified alongside their professional career because of extenuating personal reasons can easily be identified. During a participant's self-search on the Internet, a total of 10 participants revealed that their search engine result query page presented information that was linked to their official website. Furthermore, participants found that their details were disclosed online by newspapers, social media, private sector organisations' website and public records. This large amount of information from various sites can be used to link to individuals whose details have been disclosed by obligatory disclosure. Hence a richer profile of individuals can be constructed. Due to the high credibility of obligatory disclosure, those pieces of information from a variety of different websites could be seen as high quality and credible.

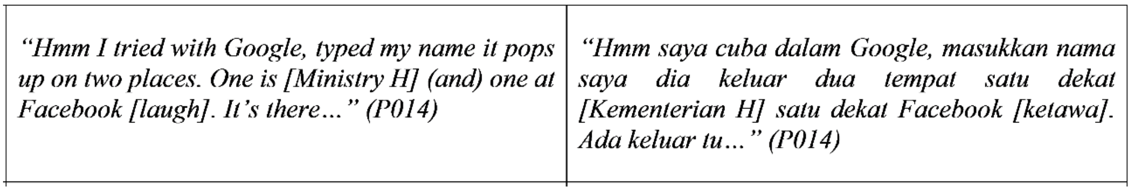
For some participants, the government website was the only source of information about them on the Internet. This could suggest that obligatory disclosure has been a source of an individual's online exposure.



"Haa, (just) type, err search my name [P004 name] using Google and it will reveal my work details (i.e. the website). Then just click on it." (P004)	*"Haa taip (je), err search je kat situ nama [nama P004] dengan Google tu dia akan keluarlah kita kerja dekat mana (i.e. laman web). Lepas tu kita klik kat situ je." (P004)*

Box 6-58: Theme 3-P004

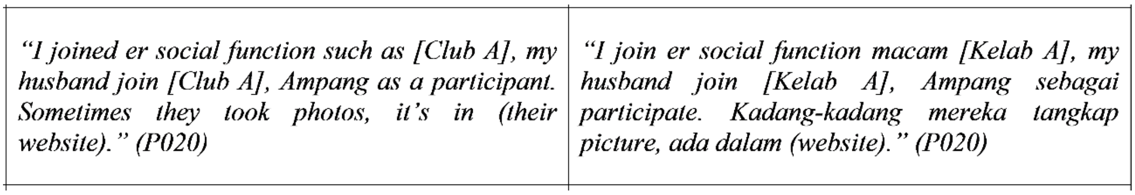
Another group of participants attributed their exposure on the Internet to information that had been generated by official websites and Facebook.



"Hmm I tried with Google, typed my name it pops up on two places. One is [Ministry H] (and) one at Facebook [laugh]. It's there…" (P014)	*"Hmm saya cuba dalam Google, masukkan nama saya dia keluar dua tempat satu dekat [Kementerian H] satu dekat Facebook [ketawa]. Ada keluar tu…" (P014)*

Box 6-59: Theme 3-P014

In addition, some participants viewed third party disclosure by another organisation's website (private) or an online news portal as their main source of disclosure. Most of this group were involved with their department's functions within the private sector. Participants claimed that - besides personal information from official websites - information pertaining to their social activities was also presented.



"I joined er social function such as [Club A], my husband join [Club A], Ampang as a participant. Sometimes they took photos, it's in (their website)." (P020)	*"I join er social function macam [Kelab A], my husband join [Kelab A], Ampang sebagai participate. Kadang-kadang mereka tangkap picture, ada dalam (website)." (P020)*

Box 6-60: Theme 3-P020

They were not happy with how Internet users are able to gather their information. Both their professional and social life were disclosed. Participants explained that due to their role in their department, they attended official functions as the department representative. Because of this, their activities normally appeared on the websites of either government or private organisations as news information. However, the employees feels uncomfortable when their social activities are known to the public.

"Yes, yes for example, I am also active in a shooting club. Sometimes they published our name and everything on it (their website), sometimes (I) feel uncomfortable." (P009)	*"Ya, ya contoh, saya inilah agaknya err saya pun antara yang aktif dalam Kelab Menembak jugalah. Kadang-kadang dia buat pun dia keluar juga nama-nama kita apa semua dalam itu, pun tak sedap juga kadang-kadang." (P009)*

Box 6-61: Theme 3-P009

Although most participants stated that information disclosed by obligatory disclosure was 'basic' and 'not detailed', P017 remarks somehow suggest that, that amount of information was indeed enough to get to know a targeted individual. Despite the 'basicness' of information, it is adequate to identify, contact and locate an individual which would assist in distinguishing or tracing an individual's identity (Krishnamurthy & Wills, 2009). The availability of his information to strangers heightened participant's P017 concerns.

"Er people recognise you! People recognise you right and people that you don't know, (and) don't know you, could know who you are. Do you feel comfortable?" (P017)	*"Er people recognise you! People recognise you kan and people yang you tak tau, (dan) yang tak kenal you boleh tau siapa you, who, who you are kan. Do you feel comfortable?" (P017)*

Box 6-62: Theme 3-P017

Photographs that were made available on official websites made it easy for public officials to be recognised. Because this information can be collected by anyone, they draws attention to the potential risk of privacy invasion. They further explained details of the threat that could happen to public employees:

"...let say for some reason, for some reason you happened to be at some place for example in a demonstration protest, you happened to pass by there. And then you do not know there are people who have seen your face. Then they took photographs haa TKP also (there). Haa you know it can create a lot of problems." (P017)	*"...let say la for some reason la, for some reason, err you happened to be at some place for example dalam apa tu dalam rusuhan-rusuhan protest apa ni kan, you happen to past by there kan. And then you do not know there are people who, who (have) seen your face. Nanti dia tangkap gambar haa TKP pun ada dekat (situ). Haa you know it can create a lot of problem, a lot of problems." (P017)*

Box 6-63: Theme 3-P017

Knowing anyone could get hold of their information and had the ability to recognise them made them uncomfortable. This was a good example of how disclosure of personal information to outsiders can influence an individual's concerns about privacy. Another participant explicitly voiced his concern:

"...its not too secure (laugh). It can be said as not secure (and) that is why I check (my information)." (P005)	*"... tak berapa secure la kan [ketawa]. Boleh kata tak berapa secure because, saya tu saya check (maklumat tentang saya)." (P005)*

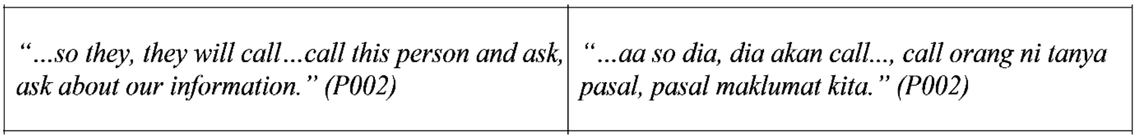
Box 6-64: Theme 3-P005

Nonetheless, the participant was also concerned about publishing direct contact information of employees, such as email addresses, which would allow outsiders to contact people directly.

"I must say, I must put, I (am) against this policy, the expose in, in individual email to, to public." (P005)

Box 6-65: Theme 3-P005

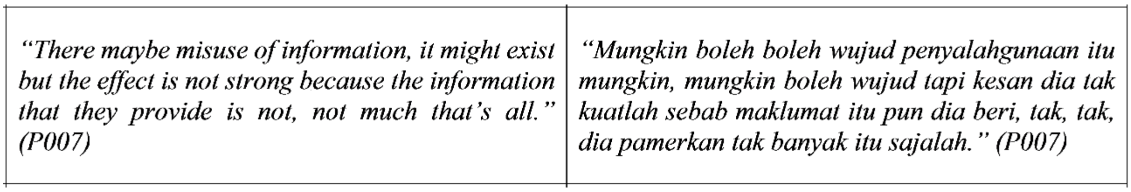
What the participant is referring to is the specific official email address that is dedicated to an employee, rather than having a general email for the public. Furthermore, email addresses have been identified as a starting point for phishing attacks (Halevi et al., 2013). Another participant believed that outsiders may resort to contacting other employees within the same office to gather information on targeted employees.



"...so they, they will call...call this person and ask, ask about our information." (P002)	*"...aa so dia, dia akan call..., call orang ni tanya pasal, pasal maklumat kita." (P002)*

Box 6-66: Theme 3-P002

Despite mentioning that a public organisation's websites disclosed 'basic' information, the same participant admitted the nature of privacy implications that may arise.



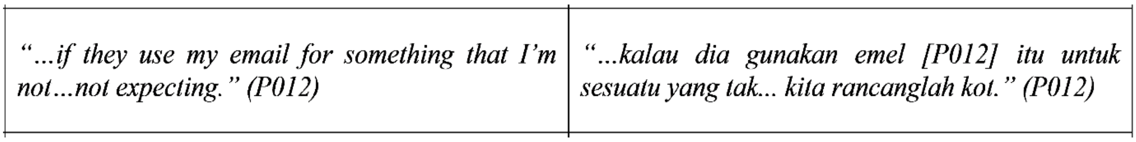
"There maybe misuse of information, it might exist but the effect is not strong because the information that they provide is not, not much that's all." (P007)	*"Mungkin boleh boleh wujud penyalahgunaan itu mungkin, mungkin boleh wujud tapi kesan dia tak kuatlah sebab maklumat itu pun dia beri, tak, tak, dia pamerkan tak banyak itu sajalah." (P007)*

Box 6-67: Theme 3-P007

Although this participant gave this view after being prompted by the interviewer, it showed an understanding of possible information misuse due to the disclosure of personal information. The availability of personal information on the Internet influences an individual's privacy concerns, due to the possibility of information abuse (Dinev & Hart, 2004a).

These concerns escalated in line with the advancement of technology, where information can be easily copied, distributed, collected and reused. Findings revealed that employees demonstrated concern around these risks. Similarly, one participant presented the idea of improper use of their personal information for marketing purposes (Appendix H – Box 6-68: Theme 3-P007).

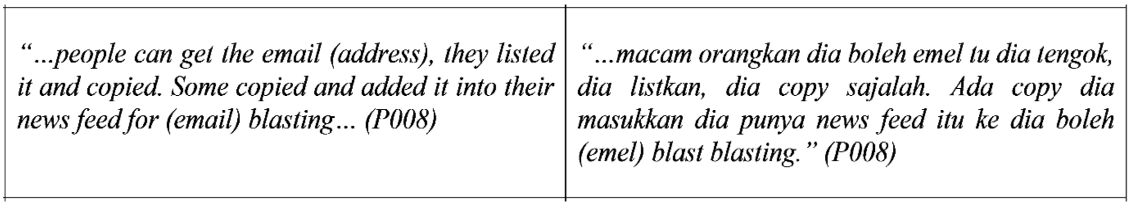
Another participant, who was less IT literate, was also aware of the risks.



"...if they use my email for something that I'm not...not expecting." (P012)	*"...kalau dia gunakan emel [P012] itu untuk sesuatu yang tak... kita rancanglah kot." (P012)*

Box 6-69: Theme 3-P012

This is probably due to their familiarity with using email in their daily work - they might come across unexpected emails in their inbox. An email address was among the participants' most cited types of information disclosed by an organisation's website. As it is publicly available, it can be exploited by any interested parties. As another participant described:

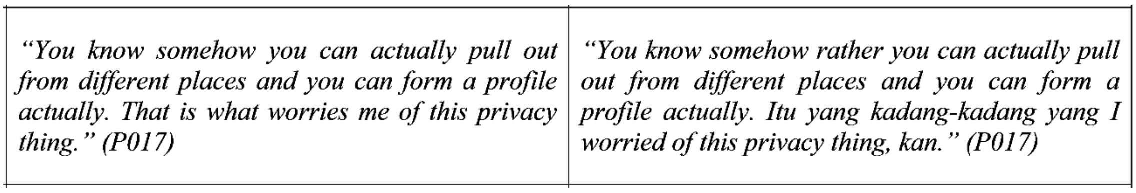


"...people can get the email (address), they listed it and copied. Some copied and added it into their news feed for (email) blasting... (P008)	*"...macam orangkan dia boleh emel tu dia tengok, dia listkan, dia copy sajalah. Ada copy dia masukkan dia punya news feed itu ke dia boleh (emel) blast blasting." (P008)*

Box 6-70: Theme 3-P008

Some interested parties may harvest and use the email addresses for the benefit of themselves. It can be seen that email addresses were misused by members of the public to send unrelated emails to government employees for their own benefit.

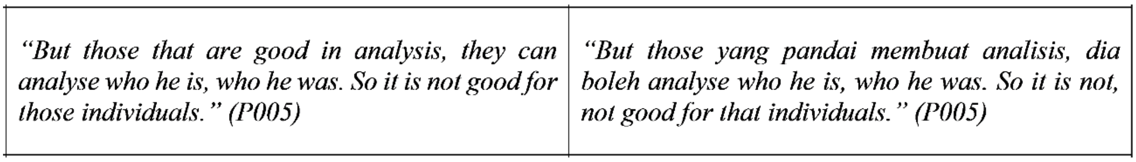
Two participants who had shown a high degree of privacy concerns responded in a more profound direction. The information that was published, albeit 'basic', can pose serious privacy consequences to employees. This information can be used to deduce richer information about an individual from different web resources. As the thoughts of the participant were expressed:



"You know somehow you can actually pull out from different places and you can form a profile actually. That is what worries me of this privacy thing." (P017)	*"You know somehow rather you can actually pull out from different places and you can form a profile actually. Itu yang kadang-kadang yang I worried of this privacy thing, kan." (P017)*

Box 6-71: Theme 3-P017

This concern was not unfounded, because researchers have proven that only by using basic information of individuals found on the Internet, it is possible to infer additional sensitive information about them e.g. social security numbers, identity (Acquisti & Gross, 2009; Aimeur et al., 2012). Some participants went further, arguing that it has a negative impact on employees:



"But those that are good in analysis, they can analyse who he is, who he was. So it is not good for those individuals." (P005)	*"But those yang pandai membuat analisis, dia boleh analyse who he is, who he was. So it is not, not good for that individuals." (P005)*

Box 6-72: Theme 3-P005

The interpretation of their responses suggested that they are aware of the privacy risks that have resulted from the disclosure of their information on an organisation’s website. Even if the information was deemed ‘basic’, the value and significance of the information is tremendous - due to the high degree of identification. More so when the information published is more detailed than was expected.

Participants were concerned that the personal attributes disclosed could be beyond what they expected to be revealed. They listed personal attributes such as name, email address (office), (work) unit, position, and telephone number (office) as acceptable personal attributes for disclosure. Participants felt that other personal attributes (if disclosed) may have undesirable consequences for government employees. Such information could be exploited by interested parties.

Another dimension of privacy concern was the secondary use of personal information without their knowledge or consent (Culnan & Armstrong, 1999; Smith et al., 1996). This concern refers to information that was published for one purpose but is used for another purpose without consent from the individuals. Participants’ concerns around unauthorised secondary use of personal information were illustrated nicely by a participant. This is due to their experience with an unexpected situation. They discovered their personal information, similar to that which had been disclosed on their organisation’s website, appeared on an ambiguous website.

“There is a website, it is like a website, not a website, it’s a website but it has information such as profiles only, they collected information such as this only.” (P018)	*“Dia buat website dia, dia ada tempat, dia macam ada satu website, bukan website, dia website dia tapi dia hanya untuk macam lebih kepada profil saja, dia kumpul-kumpulkan maklumat yang macam ini saja.” (P018)*

Box 6-73: Theme 3-P018

This participant is unsure of the status of the web page that published their information. The website was only publishing limited profiles about them, including their employment information. However, they are almost certain that this information was collected from their organisation’s website:

"When I see my full name, kind of information that was disclosed, but there is a high possibility that it came from our own website." (P018)	*"Dia mungkin bila kita tengok nama penuh macam mana, apa maklumat yang dia dapat itu tapi bila saya tengok itu kemungkinan besar mungkin daripada website kita sendiri." (P018)*

Box 6-74: Theme 3-P018

Participants strongly believed that this information was a by-product of obligatory disclosure based on the disclosure of their full name and working position. They explicitly expressed their privacy concern:

"...to me it violates my privacy because I will be contacted..." (P018)	*"...bagi saya benda itu dah tak jadi privasi untuk sayalah sebab kita akan dihubungi..." (P018)*

Box 6-75: Theme 3-P018

This information was probably collected by data broker companies who scraped information from the Internet due to the widespread accessibility of personal information moreover from government websites. This could lead employees into difficult situations. Another participant encountered private organisations misusing government employees' information, such as names, position or photographs in their promotional documentation (Appendix H – Box 6-76: Theme 3-P009).

This could suggests that information that had been published was collected and later used for different purposes. In this case, a private commercial organisation was seeking the opportunity to manipulate government employees' information for their own commercial benefits.

Generally, participants' hold the belief that obligatory disclosure publishes correct and accurate information of employees most of the time. Despite one participant describing the success rate at finding other employees on government websites as *"found 95% of the time"*, participants raise concerns around the efficiency of the obligatory disclosure management that they experienced. Most of them expressed their disappointment that incorrect information that was published, due to a failure to regularly update information. Nine participants criticise information that was not updated. As explained in section

5.2.4.2, participants viewed obligatory disclosure largely as disclosure through the staff directory. Thus they encountered information that has not been updated from the staff directory:

"The publication should be regularly updated, because sometimes on the websites there are outdated information and even staff was already transferred." (P016)	*"Penyiaran tu sepatutnya di update selalulah, dikemaskinilah sebab kadang-kadang dalam web ini ada maklumat yang lama itu dan pegawai pun dah bertukar." (P016)*

Box 6-77: Theme 3-P016

Another reason that could possibly be related to this is negligence. They highlighted the incorrect telephone number that appear on their websites and assumed that this may be caused by 'carelessness' (Appendix H – Box 6-78: Theme 3-P011).

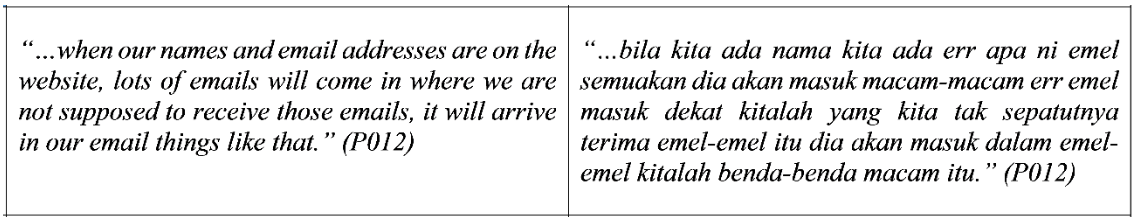
However, participants were quick to add that this situation did not always happen and was occasional. It can be suggested that participants were concerned with the inaccuracy of information, which may result in mistaken identities and misreporting of information (Smith, 1993). Additionally, this will affect their ability to be contacted and also in their efforts to contact other employees. Another consequence of this is loss of confidence in the employee. Since obligatory disclosure was perceived as a verifying tool, absence on the website would cast doubt on the status of employment.

It is interesting to note that because organisational websites were perceived as a reference point in identifying employees (refer to section 6.2.4.1), any errors in publication of employees' information will have privacy consequences. Inaccurate personal information portrayed on organisational websites will result in false identity and a skewed reputation of employees. This is consistent with Smith et al.'s (1996) findings that identify that errors in personal information were one of the factors of privacy concerns with organisations' practice among consumers.

Findings suggest that participants have concerns with the availability of their personal information on the Internet (Dinev & Hart, 2004), since they don't know who the viewers are. As such, they might believe that their information is open to information abuse (Dinev & Hart, 2004) and personal safety (Nosko et al., 2010).

Privacy invasion

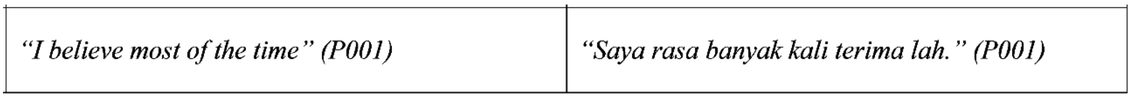
Data from the participants revealed that there are different channels of privacy invasion that could impact upon employees. Participants mentioned four types of communication channels that invaded their privacy: emails, telephone numbers, faxes and letters. Most of the participants reported of receiving spam emails and unsolicited telephone calls rather than paper-based spam (letters and fax):



"...when our names and email addresses are on the website, lots of emails will come in where we are not supposed to receive those emails, it will arrive in our email things like that." (P012)	*"...bila kita ada nama kita ada err apa ni emel semuakan dia akan masuk macam-macam err emel masuk dekat kitalah yang kita tak sepatutnya terima emel-emel itu dia akan masuk dalam emel-emel kitalah benda-benda macam itu." (P012)*

Box 6-79: Theme 3-P012

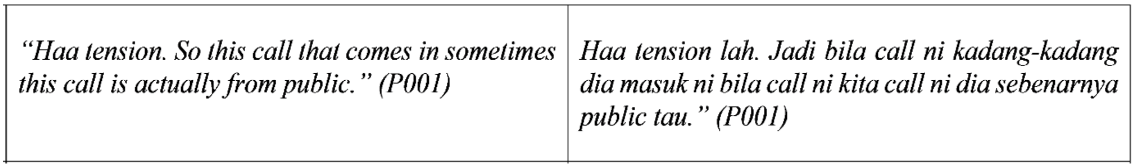
Another participant referred to another invasion that of telephone calls promoting products or marketing services e.g. personal loan (Appendix H – Box 6-80: Theme 3-P001). When prompted on the frequency of telephone calls, they mentioned:



"I believe most of the time" (P001)	*"Saya rasa banyak kali terima lah." (P001)*

Box 6-81: Theme 3-P001

Participants recounted receiving numerous telephone calls from the public. A participant , who is a technical employee, expressed the feeling of receiving such a call:



"Haa tension. So this call that comes in sometimes this call is actually from public." (P001)	*Haa tension lah. Jadi bila call ni kadang-kadang dia masuk ni bila call ni kita call ni dia sebenarnya public tau." (P001)*

Box 6-82: Theme 3-P001

Similar to spam emails, participants saw these telephone calls as an endless situation. They received them every day, as explained:

"It's a must. Even today there are four. But not about loans. Today is about courses." (P014)	*"Mesti ada. Hari ni pun ada empat. Tapi pinjaman takde lah. Hari ni kursus." (P014)*

Box 6-83: Theme 3-P014

As a result of relentless spam and unsolicited communication, most participants expressed feeling uneasiness, disturbed and stressed about with the situation:

"...disturbing actually, may bothers me to read because we have other things to do, right?" (P012)	*"... mengganggu kita juga sebenarnya mungkin mengganggu kita untuk membaca juga kadang-kadang sebab benda yang lain ada lagikan?" (P012)*

Box 6-84: Theme 3-P012

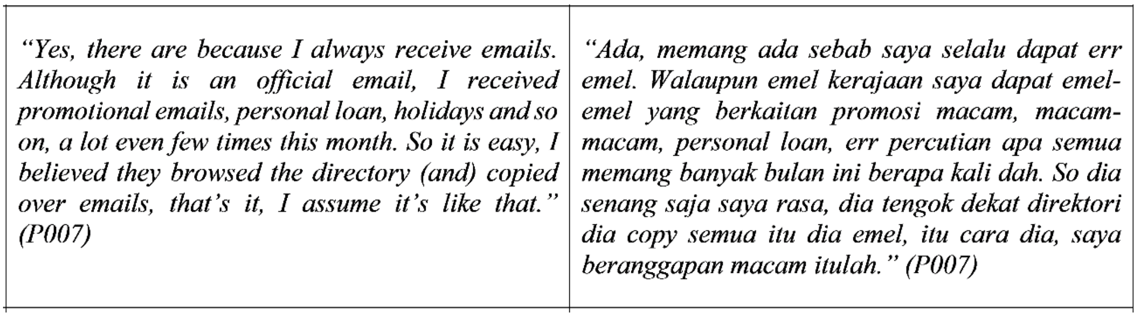
The emotions that participants expressed indicated that obligatory disclosure has invaded their privacy, although most of the participants did not realise it. However, as the interview progressed the participants started to relate their privacy experiences. For example, participants captured the concept of privacy invasion, in line with the situation and context:

"Ish! This is official email so what is this? So I got negatively affected by it. Therefore, I am not keen with this. That's why I think my privacy is violated a bit." (P008)	*"Ish! Ini emel rasmi so apa ini? So kita terganggu dari segi itulah. Itulah kadang kita tak, tak tak berkenanlah dengan benda itu. Itulah saya rasa privasi terganggu sikitlah." (P008)*

Box 6-85: Theme 3-P008

As observed in the interview, the most stated privacy violation experienced by participants is receiving unsolicited emails. Receiving spam emails can be considered as an infringement to individual's privacy (Sipior et al., 2004; Fallows, 2003). This is because it defeats the concept of the right to be let alone, as suggested by Warren and Brandeis (1890), where Internet users cannot choose for themselves when, how and to what extent information about them is used.

Employees' official mailboxes were inundated with unsolicited emails, such as advertisement of training courses and spam emails. The employees' email addresses could possibly be harvested manually or bought from data brokers. As contact information is available publicly on government websites, as presented in the result of web content analysis, it is not surprising for their contact information may fall into the wrong hands. Spam emails were the result of contact information disclosure on the website as confidently stated by one participant:

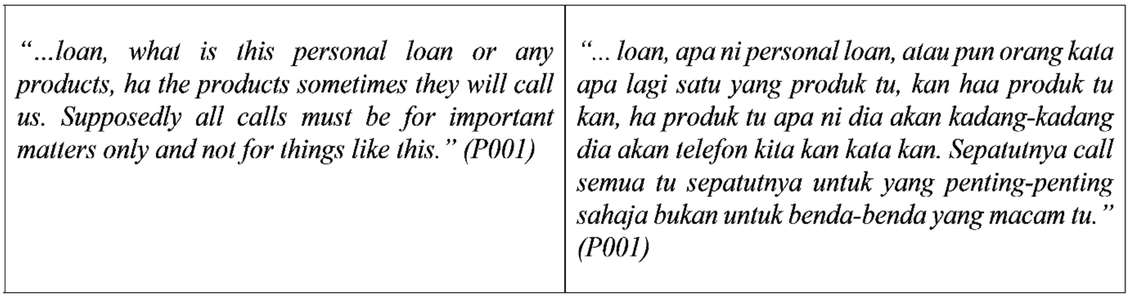


"Yes, there are because I always receive emails. Although it is an official email, I received promotional emails, personal loan, holidays and so on, a lot even few times this month. So it is easy, I believed they browsed the directory (and) copied over emails, that's it, I assume it's like that." (P007)	*"Ada, memang ada sebab saya selalu dapat err emel. Walaupun emel kerajaan saya dapat emel-emel yang berkaitan promosi macam, macam-macam, personal loan, err percutian apa semua memang banyak bulan ini berapa kali dah. So dia senang saja saya rasa, dia tengok dekat direktori dia copy semua itu dia emel, itu cara dia, saya beranggapan macam itulah." (P007)*

Box 6-86: Theme 3-P007

Lower productivity

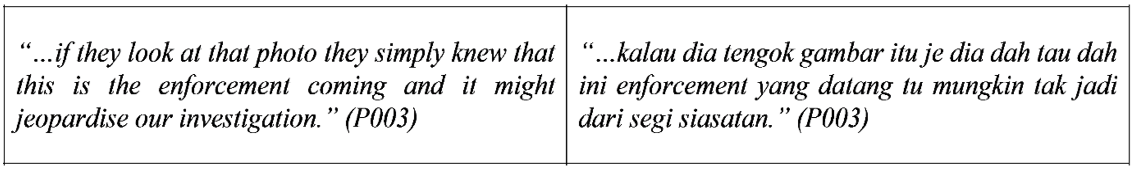
The participants related that receiving telephone calls and emails not related to their work has implications on their working performance. As shown above, telephone calls and emails were the most used mode of communication. Because contact information is publicly available, workers received telephone calls and spam emails during office hours. While all phone calls at work are supposed to be related to official duties, the majority are not.



"...loan, what is this personal loan or any products, ha the products sometimes they will call us. Supposedly all calls must be for important matters only and not for things like this." (P001)	*"... loan, apa ni personal loan, atau pun orang kata apa lagi satu yang produk tu, kan haa produk tu kan, ha produk tu apa ni dia akan kadang-kadang dia akan telefon kita kan kata kan. Sepatutnya call semua tu sepatutnya untuk yang penting-penting sahaja bukan untuk benda-benda yang macam tu." (P001)*

Box 6-87: Theme 3-P001

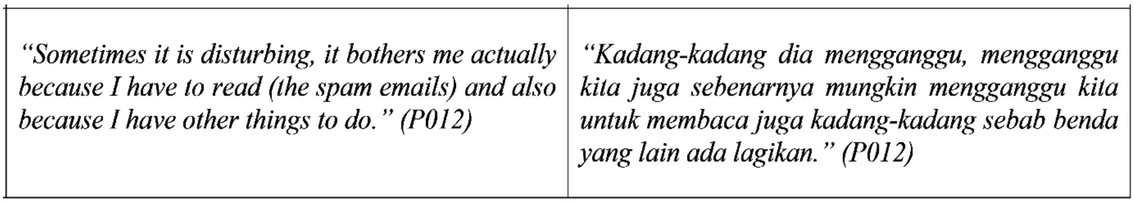
Another participant explains that because they always answer telephone calls, they had ended up doing other people's work in order to attend to the caller's request. In addition, they expressed concerns over completing work efficiently. As an enforcer, they found it difficult to do the job if their identity is widely known and recognisable.



"...if they look at that photo they simply knew that this is the enforcement coming and it might jeopardise our investigation." (P003)	*"...kalau dia tengok gambar itu je dia dah tau dah ini enforcement yang datang tu mungkin tak jadi dari segi siasatan." (P003)*

Box 6-88: Theme 3-P003

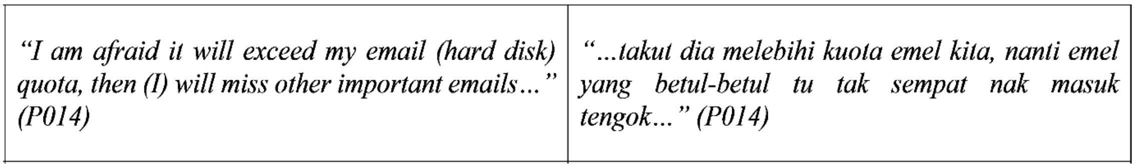
Instead of improving efficiency and productivity of employees, obligatory disclosure was found to waste working time and reduce the productivity of employees:



"Sometimes it is disturbing, it bothers me actually because I have to read (the spam emails) and also because I have other things to do." (P012)	*"Kadang-kadang dia mengganggu, mengganggu kita juga sebenarnya mungkin mengganggu kita untuk membaca juga kadang-kadang sebab benda yang lain ada lagikan." (P012)*

Box 6-89: Theme 3-P012

They explained that the time it took to manage and delete unwanted emails is diverting their focus on work. Another issue arises when the capacity of email inbox exceeds the allocated hard disk quota. Each employee has been allocated a certain amount of hard disk space:



"I am afraid it will exceed my email (hard disk) quota, then (I) will miss other important emails..." (P014)	*"...takut dia melebihi kuota emel kita, nanti emel yang betul-betul tu tak sempat nak masuk tengok..." (P014)*

Box 6-90: Theme 3-P014

Findings from these interviews in this area were similar to those as reported in Moustakas et al. (2005). In addition, up to 1,200 minutes per employee per year were wasted identifying and deleting spam emails in a German university environment (Caliendo et al., 2008).

Unnecessary disclosure

Employees perceived that obligatory disclosure at the same time also disclosed unnecessary information. For them, they felt that there should be a justifiable reason for disclosure. Six of the participants felt that personal information of employees was disclosed unnecessarily. Four participants viewed obligatory disclosure as disclosing more than necessary information to the public. They mentioned that the publication of passport photographs belong to employees was unnecessary (Appendix H – Box 6-91: Theme 3-P006).

To them, the publication of employees' photographs is more than that which required for the public to engage with government employees.

"But if it's just for publication to others, public, there is no need for profile photo, just name is sufficient." (P006)	*"Tapi like sekadar nak paparkan kepada orang lain, public, tak perlu kot gambar profile just setakat nama pun dah cukup." (P006)*

Box 6-92: Theme 3-P006

In support of this statement, participants pointed that the purpose of government is to provide services to the public.

> *"People are looking for services. So why, why, do you need to know who's who?" (P017)*

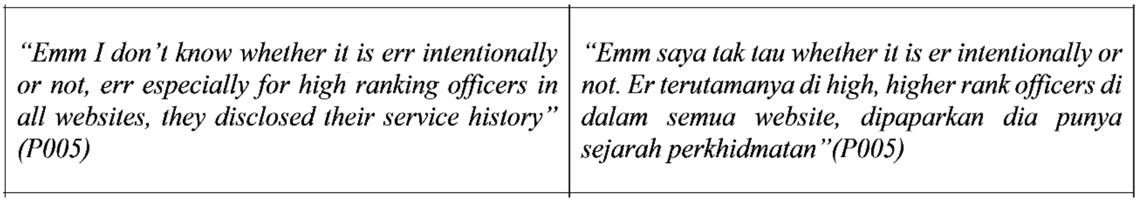
Box 6-93: Theme 3-P017

They strongly believed that official websites revealed lots of information about employees. Further, they also stated that unnecessary information was published alongside other relevant details.

> *"They used to divulge a lot of information sometimes things err that as not necessary also they go, go and tell. You know." (P017)*

Box 6-94: Theme 3-P017

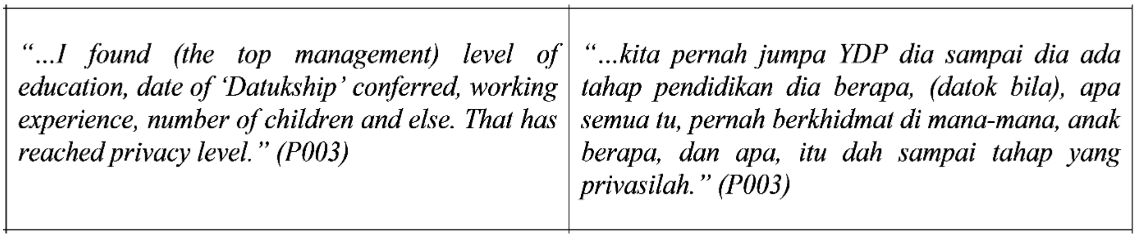
Similarly, some participants were not comfortable with information that they thought was irrelevant:



"Emm I don't know whether it is err intentionally or not, err especially for high ranking officers in all websites, they disclosed their service history" (P005)	*"Emm saya tak tau whether it is er intentionally or not. Er terutamanya di high, higher rank officers di dalam semua website, dipaparkan dia punya sejarah perkhidmatan"(P005)*

Box 6-95: Theme 3-P005

The remarks by participants suggested that participants are worried, and wary with the information that has been disclosed. According to them, personal information should be disclosed just to serve the purpose of delivering services to the public. However, certain information that was deemed unsuitable and unnecessary was found to have been published on government websites. Furthermore, one participant discovered that too much detailed information was available online:



"...I found (the top management) level of education, date of 'Datukship' conferred, working experience, number of children and else. That has reached privacy level." (P003)	*"...kita pernah jumpa YDP dia sampai dia ada tahap pendidikan dia berapa, (datok bila), apa semua tu, pernah berkhidmat di mana-mana, anak berapa, dan apa, itu dah sampai tahap yang privasilah." (P003)*

Box 6-96: Theme 3-P003

In accordance with the web content analysis findings, 23 different types of personal information were found on government websites. Some of the personal information that was stated above by participants was indeed extracted during web content analysis, such as level of education, photograph and working information. Although information about family members was not discovered in web content analysis, this information was mentioned by two participants. Information about family members was seen as unnecessary for inclusion in obligatory disclosure. Moreover, information about an individual's family was perceived by many participants as personal information in section 5.2.5.2, which may result in higher sensitiveness.

Most of the participants that shared this view were more concerned with the consequences of this disclosure. The precondition of disclosure implies that more of an employee's information was revealed than it should be. These findings indicate that while 'basic' information was found to have privacy implications, excessive disclosure could pose a higher privacy risk.

Relevancy

Apart from disclosing unnecessary pieces of information, another issue that was brought up regards the relevancy of disclosing the details of certain personnel. The participants largely agreed that not all employees should be disclosed on official websites. Although the participants were familiar with searching of government employees through official websites, they still believed that disclosing the details of staff is not appropriate across the board. They were concerned about what they perceived to be excessive disclosure of individuals belonging to an organisation. Their responses suggested that obligatory disclosure is disclosing a higher number of individuals than it should. This could invite potential privacy risks to supposedly uninvolved individuals.

"...only specific employees should be published on the web, not all..." (P009)	*"...pada saya untuk jaga keharmonian dari segi semua kakitangan yang ada mungkin hanya orang-orang tertentu saja nak diletak di web, tidak semua..." (P009)*

Box 6-97: Theme 3-P009

This statement supports the idea of limiting the number of employees on websites. This participant signals that there are some issues with current disclosure settings. There is a possibility that the current practice is disclosing the details of all employees within the organisation on the website. This could be achieved by publishing the information of all employees through the staff directory function, making it available for public view. Although data from the first phase of study discovered a high number of employees listed on government websites (in section 5.1.4.2), as stated before this study did not attempt to validate the publication of all employees through obligatory disclosure. Similarly, participants believed that the government should limit disclosure of employees:

"But for average staff like me, I think it is not needed." (P001)	*"Tapi bagi orang yang kebanyakan macam kita ni saya rasa tak perlu." (P001)*

Box 6-98: Theme 3-P001

However, some participants make contrasting comments regarding this. They suggest that all employees should be listed on the website (staff directory). Besides viewing it as facilitating the delivery of services, they explained it as one possible way to instil the sense of belonging within the organisation. Despite this, a strong category that emerged is the relevancy of disclosure. Many participants believed that disclosure has to be associated with the nature of employees' work. Participants mentioned that employees' scope of work should be considered when obligatory disclosure is implemented. Different organisations have different missions and objectives in this area. Different employees, with different positions and different scopes of work have specific roles in their organisation. The participants highlighted that the publication of details belonging to employees with a sensitive scope of work should be reconsidered:

"...but if it involves sensitive area then I think it must be hidden, for example those involved in procurement." (P008)	*"...tapi kalau bidang yang melibatkan sensitif ini saya rasa kena hide jugalah macam contoh terlibat dengan memproses perolehan." (P008)*

Box 6-99: Theme 3-P008

Another participant provided more examples of sensitive work positions:

"Investigation officer no need, prosecutor no need" (P013)	*"Pegawai siasatan tak perlu, pegawai pendakwaan tak perlu." (P013)*

Box 6-100: Theme 3-P013

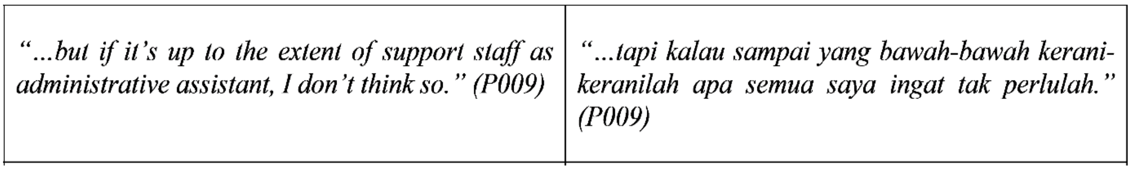
This implies that there are certain employees, appointed to sensitive positions, where it is better to hide their details from public view. Exposing an individual's information, if it is related to this sensitive position, will have an impact on employees due to the nature of this job. One participant explained the concern, in relation to working position sensitivity:

"If dealings with public without any financial or confidential information, then it can to facilitate users, but if there are implications or organisation's security or officer's safety then it may be kept hidden." (P014)	*"Macam kalau macam dealing dengan public yang tak ada membawa implikasi kewangan ke implikasi rahsia macam tak rahsia ke boleh lah untuk menyenangkan pengguna, tetapi kalau ada implikasi atau pun keselamatan mungkin perlu keselamatan pejabat atau pun keselamatan pegawai tu mungkin kena rahsiakan." (P014)*

Box 6-101: Theme 3-P014

The explanation given by this participant indicates threats that might surface from an employee’s role in the organisation.

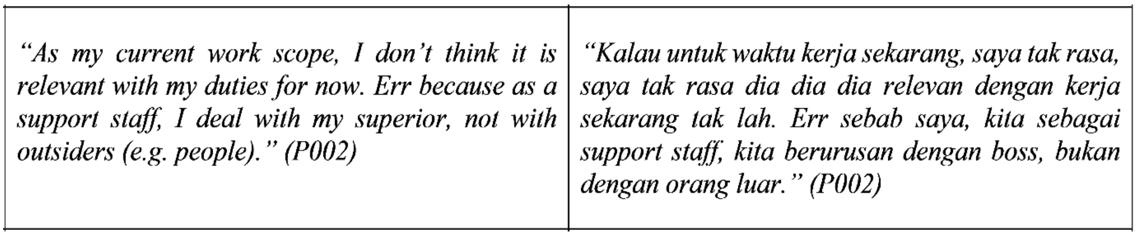
Another concern demonstrated by participants is the publication of information on employees in the lower rungs of the organisation. Participants suggested that this category of staff may be better off not published on the website. A participant, who is in the professional and management category suggests:



“...but if it’s up to the extent of support staff as administrative assistant, I don’t think so.” (P009)	*“...tapi kalau sampai yang bawah-bawah kerani-keranilah apa semua saya ingat tak perlulah.” (P009)*

Box 6-102: Theme 3-P009

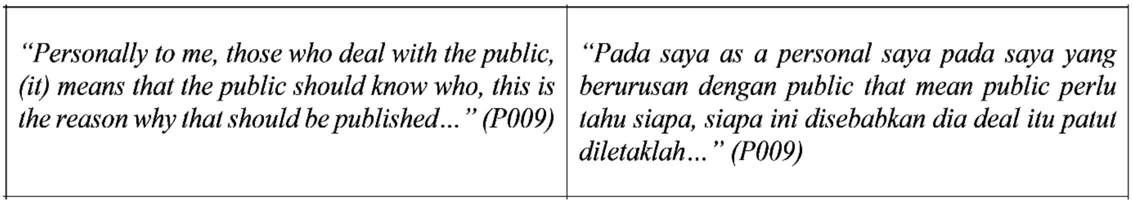
Another participant, who is from the support staff category, concurred:



“As my current work scope, I don’t think it is relevant with my duties for now. Err because as a support staff, I deal with my superior, not with outsiders (e.g. people).” (P002)	*“Kalau untuk waktu kerja sekarang, saya tak rasa, saya tak rasa dia dia dia relevan dengan kerja sekarang tak lah. Err sebab saya, kita sebagai support staff, kita berurusan dengan boss, bukan dengan orang luar.” (P002)*

Box 6-103: Theme 3-P002

The participant mentioned the factor of relevancy for obligatory disclosure. Participants seem to be suggesting that obligatory disclosure should be relevant to the purpose. They saw that employees who are involved directly with the public should be disclosed to the public.

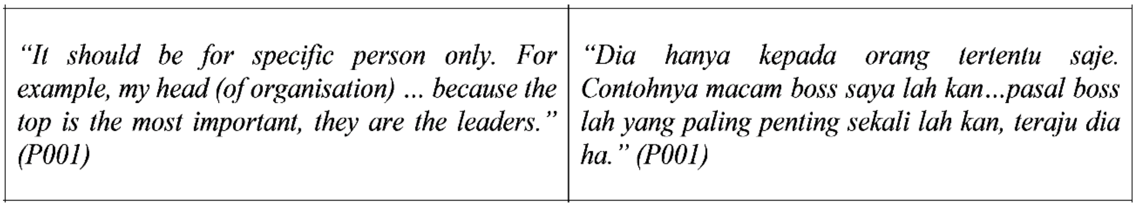


“Personally to me, those who deal with the public, (it) means that the public should know who, this is the reason why that should be published...” (P009)	*“Pada saya as a personal saya pada saya yang berurusan dengan public that mean public perlu tahu siapa, siapa ini disebabkan dia deal itu patut diletaklah...” (P009)*

Box 6-104: Theme 3-P009

Employees that are involved with the public were seen as potential individuals to have their details published on government websites. This could suggest that participants saw that the purpose of having employees’ information on official websites is to increase the delivery of public services. However, participants also cited top management as an example of the type of staff that should have their details disclosed (Appendix H – Box 6-105: Theme 3-P018).

This is due to their position as the leader of their organisation, thus projecting notions of organisational identity and an outward impression of their organisation.



"It should be for specific person only. For example, my head (of organisation) ... because the top is the most important, they are the leaders." (P001)	*"Dia hanya kepada orang tertentu saje. Contohnya macam boss saya lah kan...pasal boss lah yang paling penting sekali lah kan, teraju dia ha." (P001)*

Box 6-106: Theme 3-P001

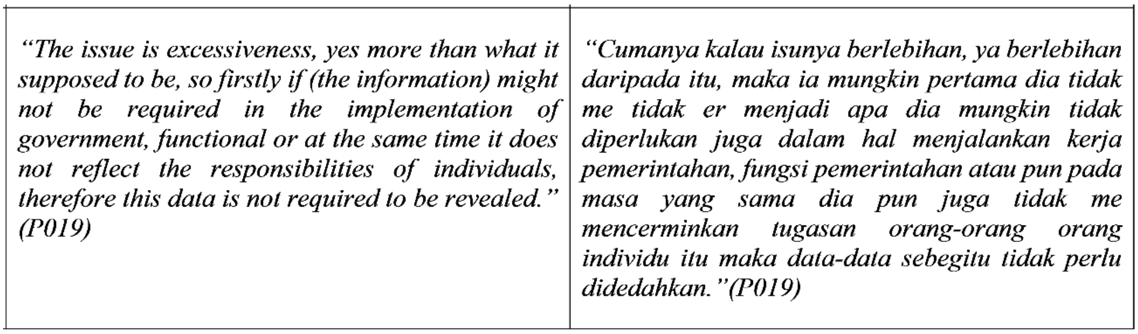
Based on the participants' data, it can be suggested that most participants emphasised the relevancy of the publication of personal information. This means that employees' website publication must be based on the scope of their work and not solely based on their status as employees. It was suggested that employees who were in sensitive types of work and the lower rungs of working categories, i.e. a support group, should be exempted from obligatory disclosure. This type of truncated publication will, of course, assist citizens by maintaining efficient delivery services but at the same time minimise the number of employees (i.e. individuals) exposed on the Internet. Hence, consequently minimising privacy invasion to employees.

Theme conclusion

After the issue of personal information and privacy were brought up during interviews, participants demonstrated concerns around privacy based on obligatory disclosure. In particular, this was related to the disclosure of personal information to outsiders, errors regarding their personal information, and unauthorised secondary used of personal information. In fact, participants have already experienced privacy invasion without realising that it is affecting their privacy. Participants unearthed the current situation of disclosure, which showed that unnecessary and irrelevant personal information of employees had been disclosed. In addition, instead of improving service delivery and efficiency, participants have revealed that obligatory disclosure serves lower their productivity at work.

Commentators

Excessive disclosure was identified as a factor for privacy violation in obligatory disclosure. The commentator was careful in discussing issues around employees' privacy by obligatory disclosure. In trying to balance between the day to day needs of governments and an individual's right to privacy, one commentator stated:



"The issue is excessiveness, yes more than what it supposed to be, so firstly if (the information) might not be required in the implementation of government, functional or at the same time it does not reflect the responsibilities of individuals, therefore this data is not required to be revealed." (P019)	*"Cumanya kalau isunya berlebihan, ya berlebihan daripada itu, maka ia mungkin pertama dia tidak me tidak er menjadi apa dia mungkin tidak diperlukan juga dalam hal menjalankan kerja pemerintahan, fungsi pemerintahan atau pun pada masa yang sama dia pun juga tidak me mencerminkan tugasan orang-orang orang individu itu maka data-data sebegitu tidak perlu didedahkan."(P019)*

Box 6-107: Theme 3-P019-commentator

If the information disclosed is beyond the appropriate level of relevancy (of employees) to perform their duties, then it might be considered as privacy-invasive. Commentator's comments were similar with this research finding that participants saw obligatory disclosure as revealing unnecessary personal information of employees (including themselves) on official websites. This struck many participants' privacy concerns. Participants also cited the relevancy of disclosing employees' information on the websites, as shown above. The participants' opinions on the issues of relevancy and unnecessary disclosure reflected their evaluation that obligatory disclosure caused violations of employees' privacy. Specific pieces of information that were considered sensitive were found available and this made participants feel uneasy. In addition, the current practice of disclosing a high number of employees also caused concern for employees.

6.2.4 Obligatory disclosure leads to higher privacy vulnerabilities for employees

The participants showed that obligatory disclosure introduced privacy risks that went beyond information privacy violations. As shown in section 5.2.6.4, five privacy risks were discussed by participants. One of the risk is misinterpretation of information that may occurred when information such as photographs taken at certain social functions that were attended by government officials and were posted on the government's website (Appendix H – Box 6-108: Theme 4-P009).

The photographs may give an indication of 'endorsement' from the respective government's department via the presence of its employees at the social function. However, they stresses that this may not be the case. This information can be manipulated and abused to trick government employees. Another approach is articulated by another participant:

"To [P012], information on the website can be manipulated, he can by asking, 'Oh that day I ask that officer he said can?'. 'Ha who is the officer?', 'so, so and so.'" (P012)	*Bagi [P012], maklumat maklumat dekat website itu dia boleh (salah)guna, dia boleh misal tanya"Oh hari itu saya tanya pegawai itu dia kata boleh?", "Haaa siapa pegawai itu?", "Sekian, sekian, sekian." (P012)*

Box 6-109: Theme 4-P012

Any individuals may refer to an employee's name on the website, and use this particular name to influence another employee for their benefit. In order to do this, information such as employees' employment and hierarchical information (e.g. organisation chart) may assist in identifying the employee as a potential victim. As shown in section 5.1.2, this type of information was widely disclosed. Employees that were tricked into this may face embarrassment or, worse still, action by their organisation that results from their unauthorised actions or having revealed confidential information. Hence, participants manage to foresee the risks to the organisation. Since this research sample is from a public sector organisation, the risk is much higher considering that the public sector holds a lot of confidential and classified information. As one participant put it:

"There are! Because you see people tend to get this information, you know if somebody wants to get a project or something, they know who to look for." (P017)	*"Ada!! Because you see people tend to get this information, you know kalau if somebody wants to get a project or something kan. They know who to look for." (P017)*

Box 6-110: Theme 4-P017

Another participant shared the same concern, because employees possess confidential government information, which might be released accidently:

"...sometimes they insist to get (the information), if they have our contact number, they insist to know more than that for example when will it be allocated? Is it enough? How much is the allocation? Then that information will indirectly reveal confidential information such as price of tender and so on." (P018)	*"...kadang-kadang dia mendesak sehinggakan dia nak mendapatkan, kalau dapat kontak kita, dia mendesak supaya nak tahu lebih daripada itu contohnya peruntukkan ini bila? Cukup ke peruntukkan ini? Berapa agaknya? Nanti secara tak langsung maklumat itu akan menyebabkan maklumat-maklumat itu rahsia yang menyebabkan harga satu-satu tender dan sebagainya itu menyebabkan dia akan dapat." (P018)*

Box 6-111: Theme 4-P018

This concern was supported by another participant:

"...public can call and ask everything because I have experienced it before 'oh how much is this tender's price, that tender's price' because they assume they can call since there are telephone numbers displayed..." (P006)	*"...public boleh call and tanya macam-macamlah sebab saya sendiri pun pernah dapat panggilan 'Oh berapa harga tender ini, berapa harga tender itu' sebab dia orang beranggapan ok dah ada phone number terus call jelah..." (P006)*

Box 6-112: Theme 4-P006

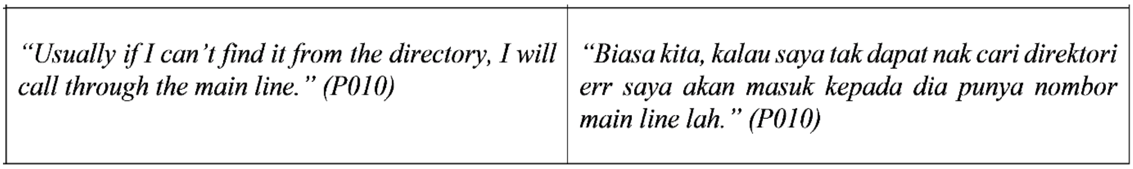
Participants explained the risks of doing their work in the context of receiving telephone calls:

"When (information is) public, it is difficult to authorise whether it is a real authorised phone call from bank or fraud..." (P001)	*"Bila (maklumat kita) public, dia kita macam.. tu la kan kalau kita tak boleh authorise sama ada, orang kalau bank telefon kan kita tak tau samada panggilan tu daripada authorisation bank atau pun orang fraud kan..." (P001)*

Box 6-113: Theme 4-P001

Since public information is accessible by anyone, including unintended recipients, they uncovered a risk that may be caused by manipulating obligatory disclosure. Employees must be more alert and careful when receiving communication from the public. Additional precaution when dealing with the public, such as verifying callers, rests on the employees. However, this is not an easy task as the caller may be well prepared with convincing answers.

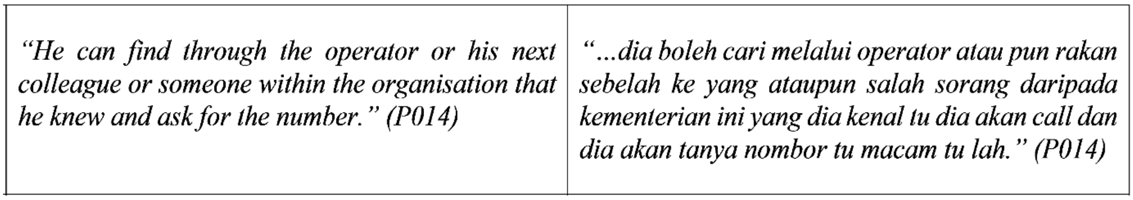
Participants also revealed that they were able to gather information about other employees with assistance from within the organisation itself. Most of them will call either the mainline and speak to the operator or call the relevant division/unit if it was listed on their websites. Under normal circumstances, participants admitted that they were able to get the specific employees' information that was required.



"Usually if I can't find it from the directory, I will call through the main line." (P010)	*"Biasa kita, kalau saya tak dapat nak cari direktori err saya akan masuk kepada dia punya nombor main line lah." (P010)*

Box 6-114: Theme 4-P010

Employees were then able to get information about the current location, current and future programme, and whereabouts of an employee. Indirectly, more information can be obtained about a particular employee:

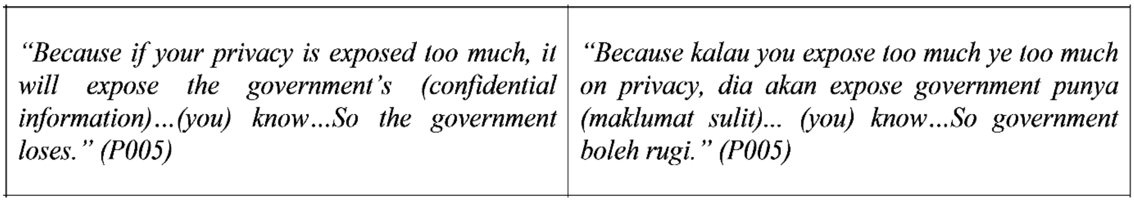


"He can find through the operator or his next colleague or someone within the organisation that he knew and ask for the number." (P014)	*"...dia boleh cari melalui operator atau pun rakan sebelah ke yang ataupun salah sorang daripada kementerian ini yang dia kenal tu dia akan call dan dia akan tanya nombor tu macam tu lah." (P014)*

Box 6-115: Theme 4-P014

While this could be seen as one of the advantages of obligatory disclosure, which is to support government efficiency, this could lead to another potential risk to employees. It reveals how anyone can get additional information about an employee easily by contacting the workplace of an individual. Any unaware colleague will provide the information requested in good faith. Unknown to them, this information - ranging from personal contact information to whereabouts and office activities - can be wrongly used to attack an employee.

This suggests that obligatory disclosure could be a starting point for a flow of personal information from various resources. As shown above, obligatory disclosure can cause more information disclosure with ‘disclosure by colleague’. Publication of presumably harmless information has the potential to lead to huge consequences. Besides the direct effect on the employees, the government might be at the receiving end. While the examples above were in the context of procurement and project management, another wider context is regarding official secrecy in terms of national security. This is especially pertinent if the information was more than what was expected:



“Because if your privacy is exposed too much, it will expose the government’s (confidential information)…(you) know…So the government loses.” (P005)	*“Because kalau you expose too much ye too much on privacy, dia akan expose government punya (maklumat sulit)... (you) know…So government boleh rugi.” (P005)*

Box 6-116: Theme 4-P005

What this participant means is that if the government’s revealing too much of employees’ personal information on its website, it will eventually expose the government’s confidential and classified information. By using the weakest link in the security chain, i.e. the ‘human factor’ (Furnell & Papadaki, 2008), and coupled with high quality information of employees, the employee and the government may be at risk of compromising national security.

Privacy attack

As disclosure of personal information, as shown above, raises privacy concerns and privacy risks, employees mentioned the idea of privacy attacks that may have occurred to them. Malicious Internet users may launch a cyber-attack based on personal information found on organisational website.

The social engineering (SE) technique is among the threats that could be used to manipulate employees (Brody et al., 2012). They illustrate this in the context of a procurement officer where interested parties may approach public employees holding this position for their commercial benefit (Appendix H – Box 6-117: Theme 4-P006)

A high ranking employee in a department, concurred:

"...you know, if somebody wants to get a project or something, they know who to look for. Who are the people, who are the people making the key decision making process." (P017)	*"...you know, kalau if somebody wants to get a project or something kan, they know who to look for. Who are the people, who are the people making the key decision making process kan." (P017)*

Box 6-118: Theme 4-P017

Pretexting is an SE attack where a scenario is created to persuade a potential victim to disclose information (Luo et al., 2011). This technique was reported to be used to manipulate employees into leaking information about organisations (Brody et al., 2012), but these findings also presented the possibility of using pretexting to gather other individuals' personal information. This is achievable by exploiting "the cognitive biases of humans and corporate policies" (p. 7) to satisfy a customer or important users of the organisation (Luo et al., 2011). 'Disclosure by colleague' is one of the examples of a SE attack.

Another example of SE attack is by 'using a superior name'. Since a specific unit or division's information was disclosed - which includes all employees within it - it is not difficult to guess at a complete hierarchical picture of a unit or division. This information can later be manipulated to influence another employee into making decisions or revealing confidential information to that person.

"To me, information on the website can be manipulated, he can obtain it by asking, 'Oh that day I ask that officer he said can?'. 'Haa who is the officer?', 'so, so and so.'" (P012)	*"Bagi [P012], maklumat maklumat dekat website itu dia boleh guna, dia boleh misal tanya 'Oh hari itu saya tanya pegawai itu dia kata boleh?', 'Haaa siapa pegawai itu?', 'Sekian, sekian, sekian'" (P012)*

Box 6-119: Theme 4-P012

Employees that were subjected to this persuasion might accidently relent to the request if they believe that it has been given permission by their superior. In fact, it is also possible to use their colleagues name in the pretext of gaining the employee's trust.

On the other hand, several participants raised concerns over the ability to be contacted directly. They expressed their concerns after receiving letters and faxes from companies which were not related to their official duties. Most of these were promotional materials, including quotations for services. The employees certainly believed that those companies collected their contact information from the organisation's website.

"It was so detail. Where did they get this? Haa later I knew it was from the website, from the directory." (P014)	*"Kata detail sangat. Mana dia dapat ni? Haa baru tau ada dalam website, dalam direktori." (P014)*

Box 6-120: Theme 4-P014

Spam emails were often cited by employees. They received promotional and marketing emails as well as lots of unrelated emails. Because of the relentless flow of spam emails, they were concerned with the threat that they might pose. Participants elaborated on the threats:

"I think this is also dangerous because sometimes it's like a personal loan advertisement but when we click on it, it can be a virus or Trojan or whatever I'm not sure!" (P007)	*"Saya rasa benda ini bahaya jugalah sebab kadang-kadang kita nampak contoh benda itu macam dia iklan personal loan tapi tiba-tiba kalau kita klik benda itu tiba-tiba virus, ataupun inilah Trojan ke apa kita pun tak pastilah!" (P007)*

Box 6-121: Theme 4-P007

The type of attack that was highlighted is known as phishing. While Internet users are exposed to conventional phishing, individuals in organisations were targeted with a more advance phishing technique known as spear phishing. Spear phishing technique targets individuals within an organisation in which their information is easily available e.g. in the public domain (Trend Micro, 2012). Employees will receive emails that appear to be trustworthy and are tricked into clicking a web link or attachment that contains malware or takes them to an exploit-laden site. One participant elaborated on phishing attacks:

"...because sometimes they ask for account number, address, numbers this and that. If we disclose, they will do something right. Withdraw money from my account or something else." (P014)	*"...kadang sebab dia mintak nombor akaun, alamat nombor ni ni kan. Bila kita bagi dia do something kan. Dia keluarkan duit akaun ke tak pasti lah." (P014)*

Box 6-122: Theme 4-P014

These privacy risks and threats present how contact information that was published on a government website for public usage was misused by malicious people to commit a privacy breach to employees. In fact, a high ranking government employee made a significant comment:

> *"I must say, I must put, I (am) against this policy, the expose in in individual email to, to public." (P005)*

Box 6-123: Theme 4-P005

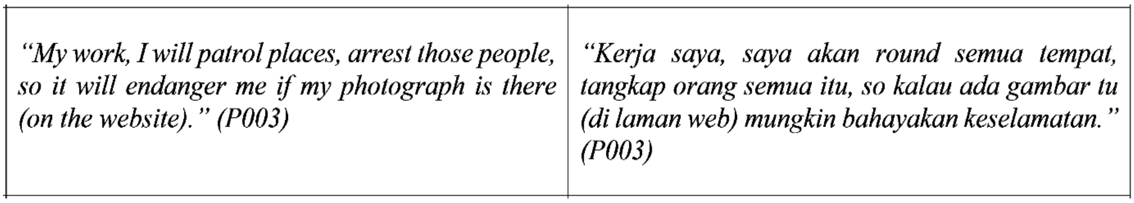
This statement shows how risky it is to disclose an individual's email on government websites. What this participant means by 'individual email address' is a mailbox that is dedicated specifically to an employee, although it is created by the organisation. Two participants highlighted fake accounts that can be created using their names or other information that is available on organisation's website.

"Worried they can use it to create fake accounts, right?" (P008)	*"Takut orang boleh menggunakanlah untuk buat create akaun palsu, ke kan?" (P008)*

Box 6-124: Theme 4-P018

Since this attack is personal and persistent (Smith, 2013) it requires both employees and organisation to play their part in reducing and subsequently combating the spear-phishing attack.

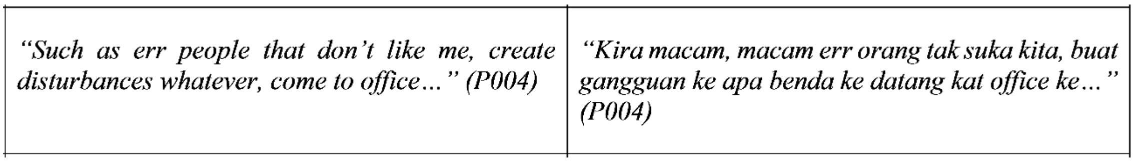
Besides concerns over informational privacy, there is also an indication that participants' concerns involved potential threats to their personal safety. Many participants related their information on the website to the risk of physical attack:



"My work, I will patrol places, arrest those people, so it will endanger me if my photograph is there (on the website)." (P003)	*"Kerja saya, saya akan round semua tempat, tangkap orang semua itu, so kalau ada gambar tu (di laman web) mungkin bahayakan keselamatan." (P003)*

Box 6-125: Theme 4-P003

This concern relates specifically to a specific piece of information that is disclosed. This remark provides insight into participant's concern with the link between the online environment and their whereabouts in the real world. Furthermore, information on official websites can assist a potential adversary in determining the likelihood of physical location of an employee during the day. They highlighted this possibility:

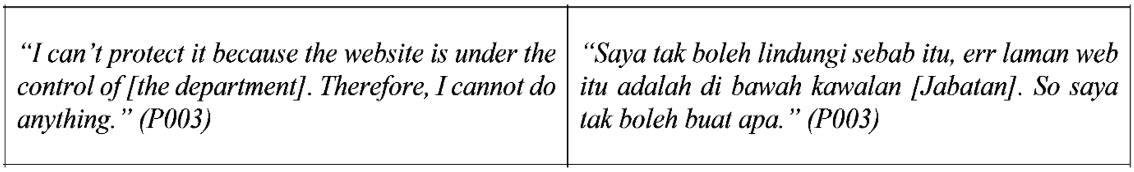


"Such as err people that don't like me, create disturbances whatever, come to office..." (P004)	*"Kira macam, macam err orang tak suka kita, buat gangguan ke apa benda ke datang kat office ke..." (P004)*

Box 6-126: Theme 4-P004

As an employee, their professional life will be mostly centred on their organisation's office. Thus during working hours, it is highly likely that employees can be found at their office. Hence, the location of individuals can be predicted most of the time. Therefore, it can be suggested that individuals are prone to privacy threats such as stalking.

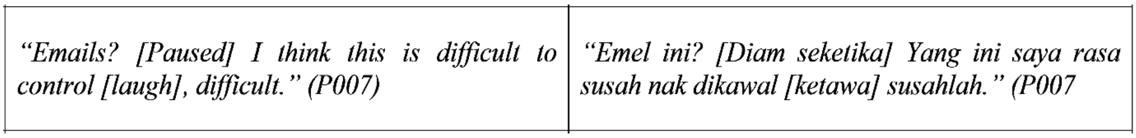
The characteristics of obligatory disclosure which increase higher vulnerabilities for employees' privacy was specified as a sub-theme for this section. These characteristics, when combined with a trusted online platform i.e. an organisation's website, will indeed pose higher values for any individual's personal information found in it. Information was thought to be of a high quality because it is accurate, verified and identifiable. Furthermore, individuals involved in obligatory disclosure were locatable, easily contacted, and importantly existed. This type of personal information is indeed valuable to data brokers or interested parties. While individuals were found to have falsified information (Fox et al., 2000) or have been providing inaccurate information (Lwin & Williams, 2003) when conducting self-disclosure, the same opportunities did not arise with obligatory disclosure. They expressed their frustration because they cannot engage in protective privacy behaviour by defending their details online. Specifically, one participant when referring to their photograph having been published, expressed disappointment:



"I can't protect it because the website is under the control of [the department]. Therefore, I cannot do anything." (P003)	*"Saya tak boleh lindungi sebab itu, err laman web itu adalah di bawah kawalan [Jabatan]. So saya tak boleh buat apa." (P003)*

Box 6-127: Theme 4-P003

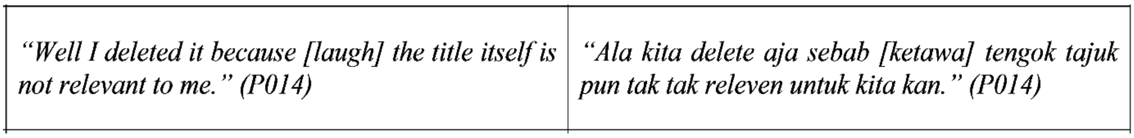
A similar situation was found when employees were faced with continuous spam emails:



"Emails? [Paused] I think this is difficult to control [laugh], difficult." (P007)	*"Emel ini? [Diam seketika] Yang ini saya rasa susah nak dikawal [ketawa] susahlah." (P007*

Box 6-128: Theme 4-P007

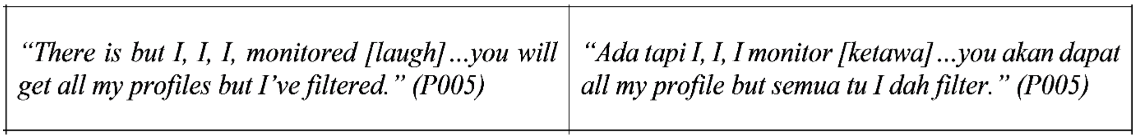
Therefore, employees were left with limited defence mechanism strategies, and these were felt to be less effective.



"Well I deleted it because [laugh] the title itself is not relevant to me." (P014)	*"Ala kita delete aja sebab [ketawa] tengok tajuk pun tak tak releven untuk kita kan." (P014)*

Box 6-129: Theme 4-P014

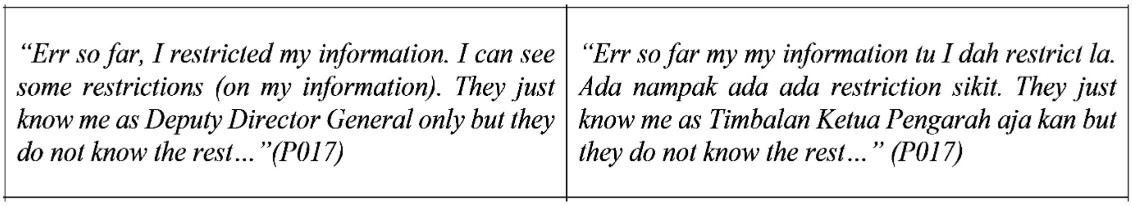
Findings revealed that participants possess limited strategies to protect their privacy due to obligatory disclosure. Some of them were unsure about how to approach any situations that might arise. For others, with indirect threats such as spam emails, some were satisfied by deleting the emails and redirecting it to their spam mailbox. It can be inferred from participants' responses to the issue that many employees have no control over their obligatory disclosure. Participants have no say of what can or cannot be disclosed about them. In addition, they were left with limited and less effective privacy protection practices to ensure that their personal information is protected. In contrast, when employees had the chance to control their disclosure, they took proactive measures in protecting their privacy:



"There is but I, I, I, monitored [laugh]...you will get all my profiles but I've filtered." (P005)	*"Ada tapi I, I, I monitor [ketawa]...you akan dapat all my profile but semua tu I dah filter." (P005)*

Box 6-130: Theme 4-P005

Another participant echoed similar privacy behaviour:

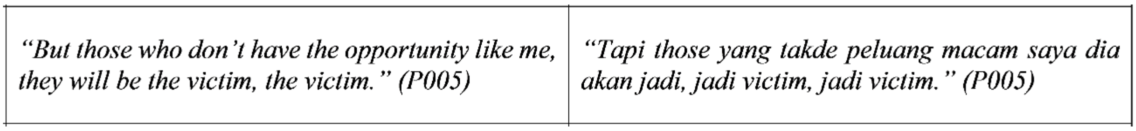


"Err so far, I restricted my information. I can see some restrictions (on my information). They just know me as Deputy Director General only but they do not know the rest..."(P017)	*"Err so far my my information tu I dah restrict la. Ada nampak ada ada restriction sikit. They just know me as Timbalan Ketua Pengarah aja kan but they do not know the rest..." (P017)*

Box 6-131: Theme 4-P017

Both participants actively monitored their personal information in order to ensure that only relevant information was published. Interestingly, both participants were top level employees in their respective departments. Hence, both had acquired a high amount of power and influence within their departments. For that reason, they were able to point out their unhappiness with the disclosure and take action to satisfy their concerns. However, both admitted that they were only doing it towards their own personal information, and not interfering with the information of other employees.

Based on this revelations, it could be suggested that obligatory disclosure posed higher implications to an individual's privacy. Sympathetically, one of them expressed:



"But those who don't have the opportunity like me, they will be the victim, the victim." (P005)	*"Tapi those yang takde peluang macam saya dia akan jadi, jadi victim, jadi victim." (P005)*

Box 6-132: Theme 4-P005

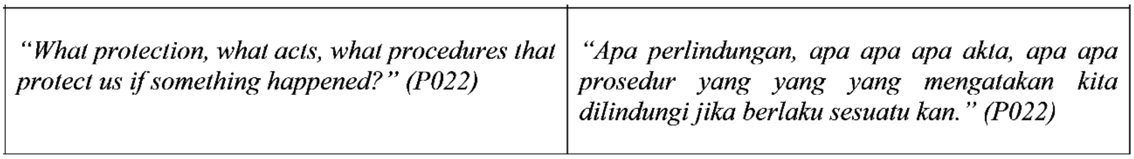
This honest and insightful remark on the consequences of disclosure to other employees should be not be taken lightly.

Theme conclusion

The main finding of this theme is that employees were exposed to privacy attacks either online or in the real world with obligatory disclosure. Risks from an invisible audience, misinterpretation of information, and misuse of information, to even their working colleagues were stated by employees. Further, on a macro level, risk towards the organisation was also considered due to the exposure of employees' information. Due to the high risks posed by obligatory disclosure, some employees that had the (informal) opportunity to control their disclosure were taking measures to limit information about themselves on the website. The fact that 23 different types of personal information can be extracted from a specific type of organisational website should be given high attention. In conclusion, obligatory disclosure prepared a conducive environment for the attacker to deploy a privacy attack on employees.

Commentators

Employees' information that was disclosed by government websites was found to fall outside the reach of data protection regulation. Although there was a privacy policy stated on each government website, it generally refers to website users – who are not the employees. Commentators agreed that this is another issue to be addressed:



"What protection, what acts, what procedures that protect us if something happened?" (P022)	*"Apa perlindungan, apa apa apa akta, apa apa prosedur yang yang yang mengatakan kita dilindungi jika berlaku sesuatu kan." (P022)*

Box 6-133: Theme 4-P022-commentator

They stated that while Malaysia has enforced Personal Data Protection Act (PDPA) 2010 in late 2013, it was the commercial sector that was regulated. Personal information that belongs to the government was excluded from PDPA. As a result, personal information of employees or any personal information that originated from a government entity is not covered under this act.

Due to lack of regulatory protection of data from government websites, the risks of intrusion, manipulation, misuse, unauthorised collection or leakage escalates since the government is the largest data collector of personal information. On a micro level, personal information can be processed and analysed by interested parties to form a fuller profile of individuals.

"Because with information technology, data can be exaggerated, personal data can be repackaged...if the data is added to databases (then) repackaged, then data is being exaggerated. It means that the data will become specific profiles (of individuals)." (P019)	*"Sebab data dengan adanya teknologi maklumat ni data boleh di exaggerate ye, data peribadi di buat oleh orang untuk di di repackage lah...kalau benda tu dah masuk dalam database dia repakaging of the data, then the data is being exaggerated. Maksudnya dia akan di jadi profil-profil (individu) yang lebih spesifik..." (P019)*

Box 6-134: Theme 4-P019-commentator

As information was easily available on the website, commentators highlighted the vulnerability of knowing an individual's name:

"...the 'name' has relationship with other (information), I see it this way...When they know your name, location, then they can still get your information." (P022)	*"...nama tu kalau er ini ini ini ada ada ada relation antara satu (sama lain), I nampak macam ni...Dia dah tahu nama, kat mana then dia still can get your information." (P022)*

Box 6-135: Theme 4-P022-commentator

In combination with other available information, accurate and rich profiles describing individuals can be constructed. As found in this research, obligatory disclosure characteristics (as presented below) contribute to the substantial value of the individual's information.

While in commercial settings, the target for consumer information is the consumer profile instead of the real individual (Zwick & Dholakia, 2004). Consumers have the option to implement privacy strategies in order to conceal their true identity e.g. anonymity. Nevertheless, obligatory disclosure offers little protection against revealing the identity of a real person because of characteristics that lead to the high trustworthiness of its information.

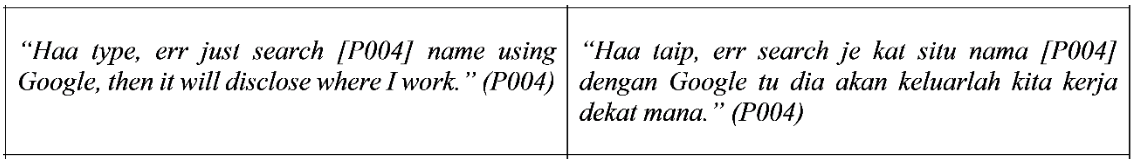
Undoubtedly, the government through its website - has an interest to serve the public in an efficient manner and increased delivery of public services. This was the main reason used to support obligatory disclosure. While this approach facilitates the organisation in serving the public, it inadvertently reveals individuals to the online environment. Disclosure of employees' personal information raises higher vulnerabilities for individuals' privacy.

6.2.4.1 Characteristics of obligatory disclosure

Data from participants suggests that obligatory disclosure has certain characteristics. While these characteristics assisted employees and consequently the government in fulfilling their responsibilities, at the same time it also contributes to a conducive hunting ground for 'authentic' personal information. Seven characteristics of obligatory disclosure were identified. These characteristics amplify potential privacy risk and increase the vulnerabilities of an individual.

Searchable

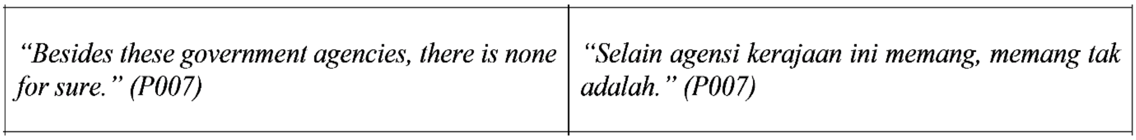
Because information presented on the Internet is searchable, information from obligatory disclosure also has similar properties (Madden et al., 2007). 'Searchable' is the ability to search for an individual. Participants admitted that their information was easily searchable on the web as a result of obligatory disclosure. Most participants mentioned 'name' as the primary information used for searching of individuals online. Ten participants referred literally to an individual's name while explaining the method of searching:



"Haa type, err just search [P004] name using Google, then it will disclose where I work." (P004)	*"Haa taip, err search je kat situ nama [P004] dengan Google tu dia akan keluarlah kita kerja dekat mana." (P004)*

Box 6-136: Sub-theme 4-P004

Most participants concurred and revealed the website's section which the search engine pinpoints their information. Information about employees can easily be searched for in just a matter of keystrokes. Publication on the organisation website broadcasts information, and this can be indexed by commercial search engines. To some participants, obligatory disclosure is the only medium by which their personal information is disclosed on the Internet.

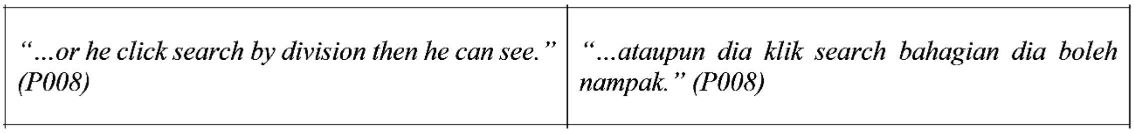


"Besides these government agencies, there is none for sure." (P007)	*"Selain agensi kerajaan ini memang, memang tak adalah." (P007)*

Box 6-137: Sub-theme 4-P007

They further explained that they believed no information about them can be found on the Internet except from government websites (i.e. obligatory disclosure) based on their Google self-search results.

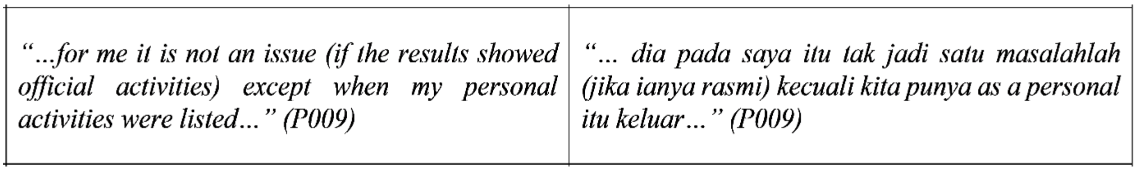
Thus, in the online environment, users must have some initial information about a person to conduct a search for an individual. But at the same time there is another way of searching for public employees without having to know their names. This technique was made possible by integrating an internal search feature into the website. Participants acknowledged the availability of this feature:



"...or he click search by division then he can see." (P008)	*"...ataupun dia klik search bahagian dia boleh nampak." (P008)*

Box 6-138: Sub-theme 4-P008

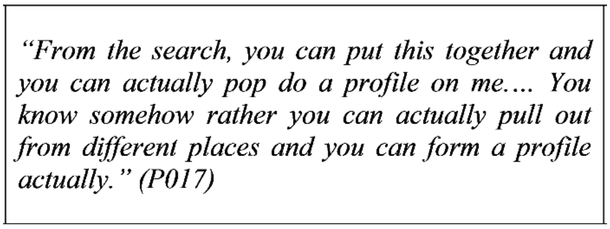
Therefore, employees are searchable either by using personal attributes - such as names - or employment information. The searchable capabilities of employees' information made participants feel uneasy. They described it as 'worrying' when their information was searchable and could be used to gather additional information about them. They were concerned when the search engine results indirectly pointed to their personal activities outside their official duties.



"...for me it is not an issue (if the results showed official activities) except when my personal activities were listed..." (P009)	*"... dia pada saya itu tak jadi satu masalahlah (jika ianya rasmi) kecuali kita punya as a personal itu keluar..." (P009)*

Box 6-139: Sub-theme 4-P009

This might have exposed employees' personal activities to others that might use this information and link to them as a government employee. This information can further be combined and analysed to get a better picture of an individual.



"From the search, you can put this together and you can actually pop do a profile on me.... You know somehow rather you can actually pull out from different places and you can form a profile actually." (P017)

Box 6-140: Sub-theme 4-P017

This information could be used against employees in influencing them to make decisions. A high ranking government official cautioned that as a government employee it is advisable to limit disclosure of personal information online.

In the case of obligatory disclosure, employees do not have the opportunity to either customise or control the searchability of their information. In contrast, on social media users were offered customisation of their profiles and can limit the searchability of their personal profiles by configuring the privacy settings. Furthermore, findings from the web content analysis discovered that all of the websites analysed incorporated an internal search engine for searching employees. The ability to search for employees demonstrates a higher risk for an individual as presented above. In addition, employees that may not have any online presence elsewhere had their personal information exposed to the online world.

Discoverable

'Discoverable' refers to the ability to find an individual. It is important to distinguish between 'discoverable' and 'searchable' since both might offer similar meanings. In searchable, some personal information must be known beforehand in order to search for an individual. In this research context, the most commonly stated personal information attributes by participants when searching for an individual (i.e. government employees) are *name* and *employment information*.

On the other hand, discoverable refers to an act where someone does not necessarily know anything about an individual, but was able to get that information because it is freely and publicly available. For example, anyone could browse a public organisation's website and will be presented with information about employees. Information about employees is listed and readily available:

"...so they can't say 'I don't know your office number' because by right they can look for it on the website." (P006)	*"...so is like dia orang tak boleh kata "Saya tak tahu nombor office you" because they by right boleh cari saja dekat website." (P006)*

Box 6-141: Sub-theme 4-P006

In the context of e-Government, discoverable information assists the public in finding the right person to answer queries or present with feedback. For example, if a person does not have someone in mind (any government employee) but knows which agency is responsible for his problems, then he/she can browse the agency's website and find the person in charge of addressing the issues. This could also benefit the public when they are not sure or have misspelled an employee's name, but with an employee's employment information the specific employees can be discovered. They mentioned the technique:

"...but if we don't have (names) or we just want to search within a division, we click that division and it will appear..." (P016)	*"...tapi kalau kita rasa kita tak tahu (nama), kita just nak cari bahagian itu, kita akan klik bahagian, dia akan keluar..." (P016)*

Box 6-142: Sub-theme 4-P016

Participants expressed that they felt it is good for the public to be able to find them when issues arise.

"... if from work perspective, I feel I like it there because when the public wanted to deal (with the government), it's easy, it means that they can find us, find us there (the website)..." (P008)	*"... kalau dari segi kerjanya kita rasa sukalah benda itu ada so nanti orang bila nak berurusan senanglah maksudnya orang boleh carilah, cari dekat situ..." (P008)*

Box 6-143: Sub-theme 4-P008

They reiterated it as one of their responsibilities to the public:

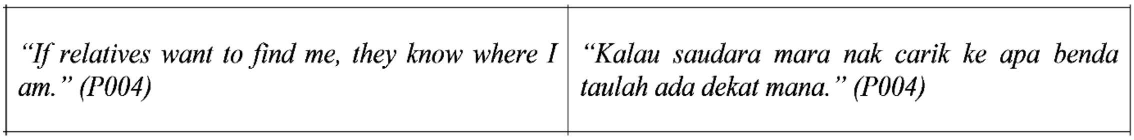
"... public can find us when they have problems, yes we want to entertain the public, it is one of our responsibilities." (P009)	*"...orang boleh cari kita andai kita ada masalah, memang pun kita nak entertain orang pun, itu salah satu tugas kita." (P009)*

Box 6-144: Sub-theme 4-P009

However, information can also be discovered by data brokers or any malicious individuals. The employees' personal information can consequently be harvested from government websites either for commercial or illegitimate purposes.

Locatable

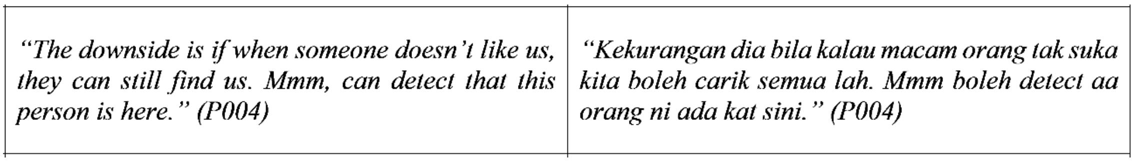
Some participants reported that they were able to discover other employees' (organisation) postage addresses from their organisation's official website, and used this information to send official letters to them. This suggests that employees' locations were exposed alongside obligatory disclosure. Thus 'locatable' refers to the capability of being physically located. After all, an organisation's website can tell what an individual's job is, and where they are working. It is also easy, from this, for their relatives and friends to get an idea of their working place and location:



"If relatives want to find me, they know where I am." (P004)	*"Kalau saudara mara nak carik ke apa benda taulah ada dekat mana." (P004)*

Box 6-145: Sub-theme 4-P004

Nevertheless, when asked about any downsides of being locatable, they said without hesitation:



"The downside is if when someone doesn't like us, they can still find us. Mmm, can detect that this person is here." (P004)	*"Kekurangan dia bila kalau macam orang tak suka kita boleh carik semua lah. Mmm boleh detect aa orang ni ada kat sini." (P004)*

Box 6-146: Sub-theme 4-P004

Disclosing an individual's location could invite a privacy risk to users (Schilit et al., 2003; Schrammel et al., 2009). As a member of enforcement staff, they experienced unwanted individuals arriving in their office. They further explained that this could be because of dissatisfaction with decisions from their field visit:

"Got the names (from the website), then came to the office and look at (our) car's number plate so they will follow and things like that." (P010)	*"Tengok nama, tau, tau rupanya datang ke office tengok pulak plat keretanya so dia akan follow apa semuanya dan sebagainya." (P010)*

Box 6-147: Sub-theme 4-P010

Based on obligatory disclosure characteristics, the physical location of individuals can easily be figured out. A potential adversary can wait near the organisation's compound or even go straight to the building or particular office level. In fact, web content analysis reveals a high disclosure of location information, up to building block or level accuracy. In addition, 94% of the websites surveyed disclosed their location information.

Contactable

Obligatory disclosure allows the public to contact government employees. 'Contactable' means the ability to be contacted. All participants mentioned that they were contactable by the public or by individuals from outside their organisation. The mode of contact ranges from telephone calls and emails to letters and faxes. Similarly, contact information was found in all of the websites surveyed. Most of the participants alluded to telephone calls and emails when describing how they are contacted:

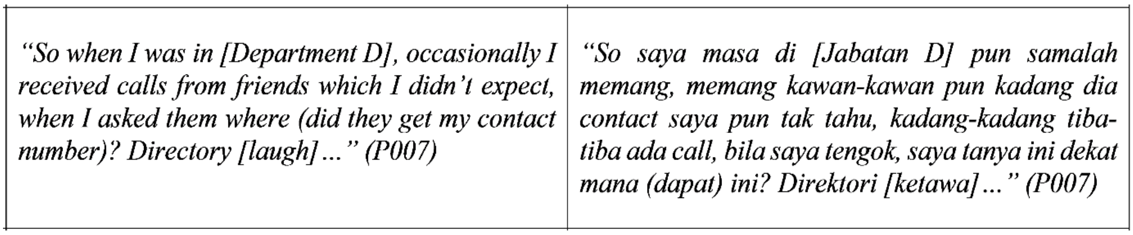
"When my name is on the website, so people can easily call me....they can contact me easily." (P002)	*"Ki, kira macam ah nama sendiri dekat website so er orang senang nak call. ...orang senang nak berhubung dengan kita." (P002)*

Box 6-148: Sub-theme 4-P002

"Email is ok, actually email can be considered as black or white, right? So I prefer email." (P006)	*"Emel ok actually emel is sesuatu yang very dah black and white, kan? So I prefer email." (P006)*

Box 6-149: Sub-theme 4-P006

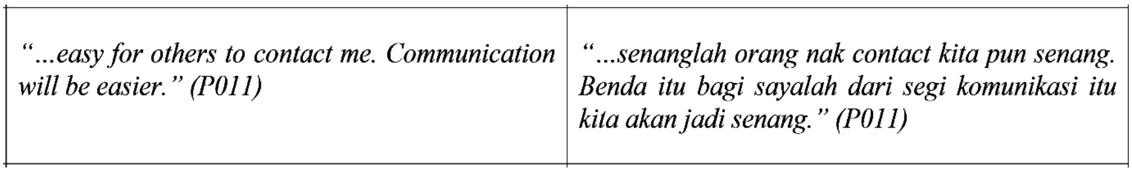
Sometimes, receiving a telephone call may come as a surprise for the employee. They highlighted their experience:



"So when I was in [Department D], occasionally I received calls from friends which I didn't expect, when I asked them where (did they get my contact number)? Directory [laugh] ..." (P007)	*"So saya masa di [Jabatan D] pun samalah memang, memang kawan-kawan pun kadang dia contact saya pun tak tahu, kadang-kadang tiba-tiba ada call, bila saya tengok, saya tanya ini dekat mana (dapat) ini? Direktori [ketawa] ..." (P007)*

Box 6-150: Sub-theme 4-P007

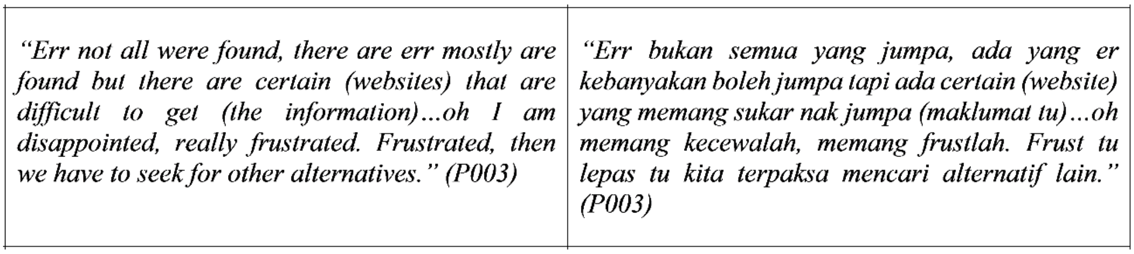
This is because the employees can be contacted directly based on published contact information. Participants indicated that they prefer to be contacted when there are issues regarding their official work. Hence, they could provide a faster response and better services to the public:



"...easy for others to contact me. Communication will be easier." (P011)	*"...senanglah orang nak contact kita pun senang. Benda itu bagi sayalah dari segi komunikasi itu kita akan jadi senang." (P011)*

Box 6-151: Sub-theme 4-P011

Nevertheless, contact information was occasionally difficult to get from the websites. The consequence of not finding a specific employee on the official website was frustration:



"Err not all were found, there are err mostly are found but there are certain (websites) that are difficult to get (the information)...oh I am disappointed, really frustrated. Frustrated, then we have to seek for other alternatives." (P003)	*"Err bukan semua yang jumpa, ada yang er kebanyakan boleh jumpa tapi ada certain (website) yang memang sukar nak jumpa (maklumat tu)...oh memang kecewalah, memang frustlah. Frust tu lepas tu kita terpaksa mencari alternatif lain." (P003)*

Box 6-152: Sub-theme 4-P003

The frustration expressed by some participants strengthened the contactable characteristic of obligatory disclosure. Employees were not expecting this information to be absent from the organisation website. Therefore, participants revealed their strategy to find the employee's information. As stated in section 6.2.4, information about other employees - including their current whereabouts, current and future activity or work programme - can be disclosed by their colleagues or someone within their organisation.

"If I don't know, then when I contact their officer or anyone that is in that division, I will ask whether this particular officer is around. That is the only way." (P008)	*"Kalau kita dah tak tahu sangat and then bila kita akan contact lah dia punya pegawai, sesiapa yang dekat dalam bahagian itu and then kita tanyalah ada tak sekian, sekian pegawai nama ini. Itu sajalah cara dia." (P008)*

Box 6-153: Sub-theme 4-P008

By using information from websites, an individual's personal information can be collected unknowingly.

Identifiable

'Identifiable' can be defined as the ability of others to identify an individual. Employees expressed that obligatory disclosure assists others in identifying them. For example, participants stated that obligatory disclosure made them easily recognisable. This was neatly expressed by several participants, in particular towards the disclosure of photographic images of them.

"...if they just see the photo, they will know that this is the enforcement (staff) that came..." (P003)	*"...kalau dia tengok gambar itu je dia dah tau dah ini enforcement yang datang tu..." (P003)*

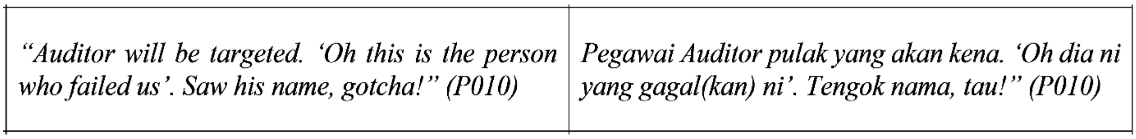
Box 6-154: Sub-theme 4-P003

The consequences of this will have an effect on their work productivity. As a member of enforcement staff, it is difficult for them to conduct an investigation and operation if too much detail is known about them. Aside from this, the risks related to being identified were also mentioned by them and were discussed earlier. They also expressed their uneasiness if the public recognise them.

"Because felt like ah, they knew our face, better don't [laugh] later they will able to recognise (me) anywhere..." (P006)	*"Sebab rasa macam ah ni orang dah kenal melalui muka itu ah baik tak payah [ketawa] kan nanti orang boleh cam dekat mana-mana..." (P006)*

Box 6-155: Sub-theme 4-P006

Besides this specific type of information (facial recognition), they also perceived that this disclosure (in general) made them uncomfortable as they can be identified:

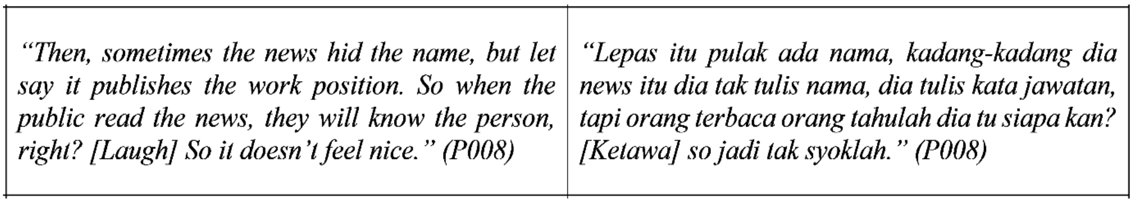


"Auditor will be targeted. 'Oh this is the person who failed us'. Saw his name, gotcha!" (P010)	*Pegawai Auditor pulak yang akan kena. 'Oh dia ni yang gagal(kan) ni'. Tengok nama, tau!" (P010)*

Box 6-156: Sub-theme 4-P010

For example, when an auditor performs audits and discovers incompliances, the auditor will make certain recommendations and decisions. When the result is not expected by the respective company or organisation, the company may undertake action in retaliation. Thus the employee who is appointed as auditor can be identified from obligatory disclosure.

One participant offered an example of identifiability characteristics that may be faced by employees. When newspapers or media report any misconduct or an accusation of a public employee, it will normally conceal the name of the employee pending investigation. For this reason, only certain information was disclosed in the news, such as the organisation and working position.



"Then, sometimes the news hid the name, but let say it publishes the work position. So when the public read the news, they will know the person, right? [Laugh] So it doesn't feel nice." (P008)	*"Lepas itu pulak ada nama, kadang-kadang dia news itu dia tak tulis nama, dia tulis kata jawatan, tapi orang terbaca orang tahulah dia tu siapa kan? [Ketawa] so jadi tak syoklah." (P008)*

Box 6-157: Sub-theme 4-P008

The information that had been published could be used to find additional information in order to create a more complete profile of an individual. Finally, a rich profile of an individual could possibly be compiled based on that information (Appendix H - Box 6-158: Sub-theme 4-P005).

As presented in the web content analysis, the potential for identifying employees is high considering that 23 different types of personal information can be found via obligatory disclosure.

Accurate

Information about employees that was published was considered correct and accurate by participants. They revealed that the public were able to contact them correctly using that information:

"They just look at the website and they were able to contact us correctly." (P012)	*"Dia tengok laman web saja dia boleh hubungi kita dengan tepat." (P012)*

Box 6-159: Sub-theme 4-P012

Because of the accuracy of an employee's information, any misspelled or wrong information will not lead to finding the targeted employee:

"There is a search box but it is not so helpful because sometimes if you misspelled, then you can't find that person" (P006)	*"Ada juga dia punya carian punya box itu tapi is not so helpful lah sebab kadang-kadang kalau kita silap eja itu memang lari habislah." (P006)*

Box 6-160: Sub-theme 4-P006

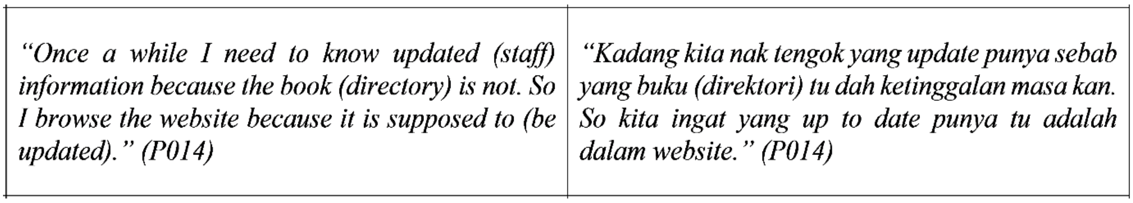
The same reason was echoed by other participants. They admitted that sometimes they can't find the specific person from the website. They further explained that this might have happened because of a misspelling of the person's full name.

However, to several participants inaccuracy on employees' information does happen occasionally. While they pointed out some administrative issues that could have contributed to this, they agreed that most of the time an employee's information is accurate. They shared one of the steps for reviewing the accuracy of employees' information by the organisation. The organisation instructed all employees to conduct a self-check on their own information for publication on the official website. Employees were instructed (via email) to reconfirm their personal information:

"…e-mail from system administrator to all staffs to check our names, are we still at the same division, and then our job description. We have to update again, (because) they are afraid if the same person at the same division but having a different responsibility, or changes unit, confirming job description, yes they did, they did it." (P008)	*"…emel daripada system administrator kepada semua supaya semua cek balik nama kita, adakah kita masih lagi dekat bahagian itulah, bahagian itu, and then dia punya job description. Kitakan kan dia nak update baliklah job description dia takut orang itu kadang dulu satu bahagian tapi buat kerja lain, tukar unit ke kan job description itu dia minta confirm balik itu memang adalah, dia ada buat." (P008)*

Box 6-161: Sub-theme 4-P008

This indicates the considered importance of publishing accurate and correct information on the organisation's website. Organisations were also seen as having a review mechanism in place to ensure disclosed information is up-to-date. Up-to-date information will enhance the quality of information on the website and thus obtain a higher trust from web users (Escobar-Rodríguez & Carvajal-Trujillo, 2014).



"Once a while I need to know updated (staff) information because the book (directory) is not. So I browse the website because it is supposed to (be updated)." (P014)	*"Kadang kita nak tengok yang update punya sebab yang buku (direktori) tu dah ketinggalan masa kan. So kita ingat yang up to date punya tu adalah dalam website." (P014)*

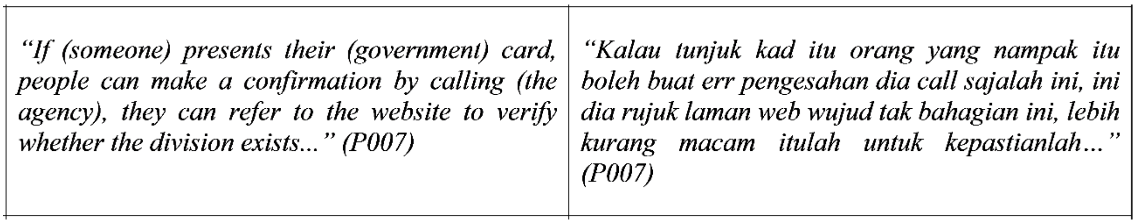
Box 6-162: Sub-theme 4-P014

Therefore, this could suggest that employees' information on the website was accurate and reliable.

Verifiable

Participants mentioned that an organisation's website served as an official communication tool from the government to citizens. Another characteristic that emerged from participants' data is that the 'organisation website is considered a verification tool'. It is regarded as a point of reference for the public and the employees itself. One example was when trying to get the employee's full name. Information on the websites was seen as a reference point for employees to get this information (Appendix H – Box 6-163: Sub-theme 4-P012).

It is also served as a verification tool for the public to ensure that any individuals claiming to be a government employee can be verified by browsing their organisation's official website. Information from the official website in this case, e.g. the staff directory, was then compared to information that was conveyed to them.



"If (someone) presents their (government) card, people can make a confirmation by calling (the agency), they can refer to the website to verify whether the division exists..." (P007)	*"Kalau tunjuk kad itu orang yang nampak itu boleh buat err pengesahan dia call sajalah ini, ini dia rujuk laman web wujud tak bahagian ini, lebih kurang macam itulah untuk kepastianlah..." (P007)*

Box 6-164: Sub-theme 4-P007

Further, it was also noticed that information on websites is used to establish authenticity (Appendix H – Box 6-165: Sub-theme 4-P007).

The public may refer to details on government websites for clarification or to cross-check information. This clearly shows how an organisation's website is regarded as a verification tool to the public.

Theme conclusion

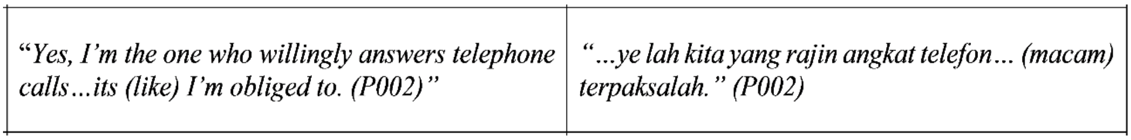
All seven characteristics of obligatory disclosure were presented above. These characteristics, in combination with the publically available personal information, increased the risk and vulnerabilities faced by the public employees.

6.2.5 Civil servants' organisational commitments reduce employees' privacy concerns

This is a major theme that was identified as an opposing factor that can reduce an employee's privacy concerns. Participants, as employees, saw the publication of their personal information as required in order to meet the organisation's objectives. Therefore, it was seen as normal for their information to be disclosed on the organisation's website, and as adhering to organisational policy. There are three categories within this theme: *civil servant professionalism*, *e-Government initiatives*, *improve efficiency*.

Civil servant professionalism

Findings showed that receiving frequent telephone calls made participants uncomfortable, especially when these were not related to their work. However, participants noted that due to their position as government employees they tended to accept it as 'part and parcel' of their responsibilities:



"*Yes, I'm the one who willingly answers telephone calls…its (like) I'm obliged to. (P002)"*	*"…ye lah kita yang rajin angkat telefon… (macam) terpaksalah." (P002)*

Box 6-166: Theme 5-P002

Some participants expressed it as a strategy to ensure that public employees became more responsible:

"Maybe actually I think maybe they want their staff to be more responsible, maybe." (P006)	*"Mungkin agar actually ya saya rasa mungkin dia nak pegawai dia lebih bertanggungjawab kot." (P006)*

Box 6-167: Theme 5-P006

Findings revealed that participants were willing to surrender some of their privacy with obligatory disclosure, because they understood it as part of their responsibility as government employees (Appendix H **-** Box 6-168: Theme 5-P011).

This suggests the willingness of employees to allow obligatory disclosure in order to be able to perform an effective service to the citizens. It is evident that participants put citizens first when elaborating on the publication of employees' information on government websites. A senior level employee, gave interesting responses highlighting connections between privacy risk and civil servant professionalism:

"With how many calls coming in…if it's specific for us then it is good, although it affects our work, where calls kept coming in but it is not an issue because it is our job to give the best to the public." (P009)	*"Banyak mana call masuk pun kalau spesifik untuk kita is good walaupun itu menjejaskan dari segi kerja itulah sekejap masuk, sekejap masuk call itukan tapi tak ada masalah sebab memang tugas kita nak bagi terbaik untuk public." (P009)*

Box 6-169: Theme 5-P009

For the participant, disturbances caused by this were considered minor and could be tolerated as long as he was able to offer the best service to the public. While focusing on receiving calls related to his work was a priority, his willingness to attend to unrelated telephone calls suggested the importance of delivering service to the public. When justifying the disclosure of their information on the website, many participants focused on the benefit to the public:

"If it relates to, relates to our work that needs to be contacted, I prefer it to be in the portal in order to facilitate (the public)." (P008)	*"Kalau melibatkan benda, bidang kerja kita itu kalau memang perlu dihubungi, saya suka benda itu adalah dalam portal supaya memudahkan orang (awam) nak itu." (P008)*

Box 6-170: Theme 5-P008

Another participant believed that it was easier for the public to interact with employees when they knew the employee they were contacting:

"...the public should know who he/she actually is because when they want to communicate, it's easier." (P009)	*"...yang public perlu tahu siapa dia sebenarnya sebab bila public nak berhubung tadi dia mudah." (P009)*

Box 6-171: Theme 5-P009

These responses suggested that participants understood their role as government employees in delivering public service. This was mentioned by a participant who has a senior management role in an organisation:

"Because the Malaysian Government is people friendly." (P013)	*"Sebab Kerajaan Malaysia dia mesra rakyat." (P013)*

Box 6-172: Theme 5-P013

Here, the assumption deduced from participants' data is that participants are willing to surrender their privacy for the sake of providing an efficient public service. Employees were trying to meet the expectations of the public. Another participant added a further reason for accepting obligatory disclosure. He touched on adhering to orders as a reason for disclosure:

"...because we follow the policy, right. They, request to publish every err the employees, right. So I think it is ok. We are just following orders." (P001)	*"... pasal kita pun ikut polisi situ kan. Dia, dia mintak terterakan err setiap, sorry setiap apa ni kakitangan tu kan. Jadi saya rasa ok je lah. Kita just follow orders je lah." (P001)*

Box 6-173: Theme 5-P001

It can be seen that there is a relationship between this category and the employees' feelings. This statement by the participant revealed a connection between the *normal* feelings with *following orders*. Participants who mentioned feeling *normal* with obligatory disclosure might suggest that they are just adhering to their organisation's policy. From their response, there is reluctance from employees to have their information made available on the website, but as a dedicated public servant, employees are expected to adhere to rules and regulation within the public service. They gave an interesting insight on why sensitive information, such as working grade, might be disclosed:

"But those who do that (disclosing information), they want to please their top management. That's why they publish the ranking of their top management." (P005)	*"Tapi orang yang buat tu kita faham dia nak please dia punya boss. Nak please boss dia ah letaklah ranking boss dia." (P005)*

Box 6-174: Theme 5-P005

It seems to suggest that low privacy awareness among government employees contributed to the disclosure of sensitive employee information on the government website. Likewise, the tendency to satisfy their superiors resulted in people publishing unnecessary information related to an employee.

e-Government initiatives

Participants argued that the public has the right to information. For them, obligatory disclosure is one of the channels used to fulfil the citizen's right to information. The public require this information in order to interact with the government for any service required.

"The public need to be told," (P013)	*"Rakyat perlu diberitahu." (P013)*

Box 6-175: Theme 5-P013

They stressing the importance of disclosing employee information to the public. While agreeing with this idea, another participant focused on the purpose of information use by the public:

"...ok this person (needs it) for official purposes, he needs it." (P015)	*"...ok memang orang ini urusan rasmi, dia perlukan itu." (P015)*

Box 6-176: Theme 5-P015

Other participants disagreed with withholding information from the public:

"So if even names, email addresses, telephone numbers cannot be known, it's unfair to me..." (P010)	*"Jadi kalau itu pun nama, emel, nombor telefon pun tak boleh tahu, unfairlah..." (P010)*

Box 6-177: Theme 5-P010

They stated that the public has the right to know governmental information. This right was clearly stated:

"...they have the right to know about certain information of ours, so that we are accessible [laugh]." (P006)	*"...they have the rights to tahulah pasal certain information so we are accessible [ketawa]." (P006)*

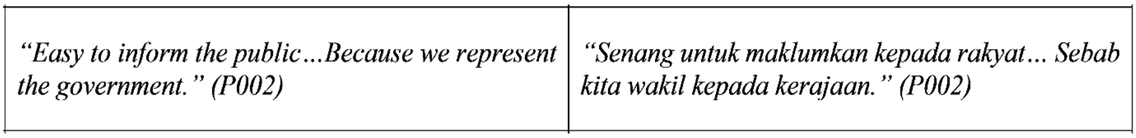
Box 6-178: Theme 5-P006

Another justification raised by participants was that they viewed government employees as 'belonging to the public'. This is due to their salary coming from the government payroll, which in turn is funded by public tax collection. Government employees thus perceived a sense of ownership:

"Although it's like 'oh they know lots of information', as a public servant, it's understandable that we are like in a way public property..." (P006)	*"Walaupun dia rasa macam like 'oh banyaknya information dia tau' tapikan bila kita dah jadi public servant then it's understandable that we are like in a way public property..." (P006)*

Box 6-179: Theme 5-P006

Another view regarded public employees as the government's representative. As such, information on employees is justifiably being disclosed for the benefit of the public.

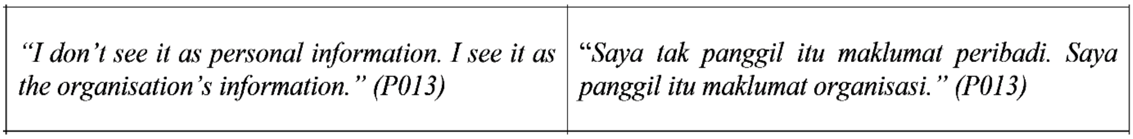


"Easy to inform the public…Because we represent the government." (P002)	*"Senang untuk maklumkan kepada rakyat… Sebab kita wakil kepada kerajaan." (P002)*

Box 6-180: Theme 5-P002

While admitting that a lot of information (including their personal information) was disclosed to the public, participants seemed to lower their concerns in respect of being 'public property'.

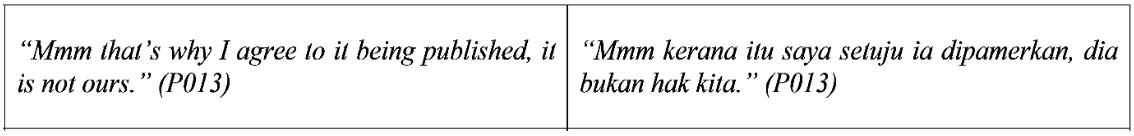
This belief is supported by another participant:



"I don't see it as personal information. I see it as the organisation's information." (P013)	"*Saya tak panggil itu maklumat peribadi. Saya panggil itu maklumat organisasi." (P013)*

Box 6-181: Theme 5-P013

When employees cease to see it as their personal information, this shifts the ownership. Hence, the management of this information now lies with the organisation, and the decision over whether or not to publish it lies with the organisation. Participants are consequently less concerned with the disclosure. It was clear with this participant's remark:

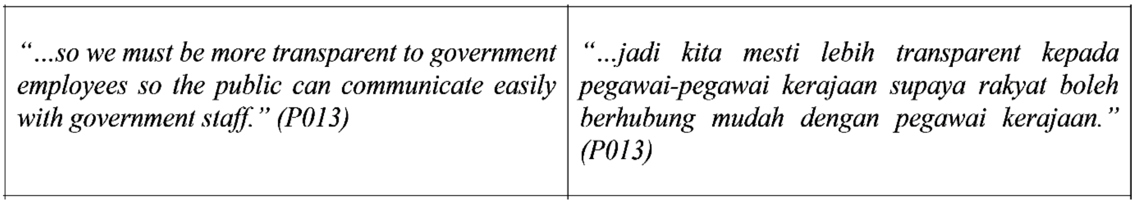


"Mmm that's why I agree to it being published, it is not ours." (P013)	*"Mmm kerana itu saya setuju ia dipamerkan, dia bukan hak kita." (P013)*

Box 6-182: Theme 5-P013

The sense of ownership of personal information could lead to a participants' behavioural intention to protect things that they own. Therefore, when the sense of ownership is lost, less privacy concerns were shown. The findings are consistent with Sharma and Crossler (2014), when they investigated disclosure behaviour in social commerce. Perceived ownership towards information was found to influence a higher privacy risk.

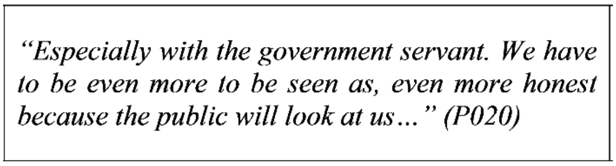
Participants relate obligatory disclosure to government transparency. In fact, access to information has been described as a core component of governmental transparency (Redford, 1969). The public has access to government information and the organisation's activities, which gives them the ability to closely observe government agencies. Findings suggest that the participants viewed access to employees as a means of transparency:



"...so we must be more transparent to government employees so the public can communicate easily with government staff." (P013)	*"...jadi kita mesti lebih transparent kepada pegawai-pegawai kerajaan supaya rakyat boleh berhubung mudah dengan pegawai kerajaan." (P013)*

Box 6-183: Theme 5-P013

Since transparency is regarded as a strategy for combating corruption (Cuillier & Piotrowski, 2009) publishing information about government employees may make them more cautious in doing their work. One participant, a high-ranking officer, cautioned civil servants on the consequences of this disclosure:



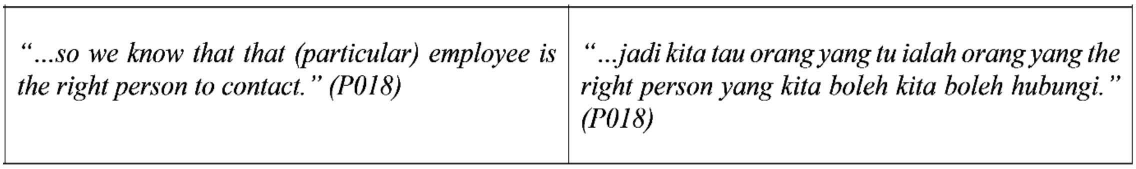
"Especially with the government servant. We have to be even more to be seen as, even more honest because the public will look at us..." (P020)

Box 6-184: Theme 5-P020

This response indicates that transparency may influence government employees when performing their job, since they assume that they are being watched by the public. One factor that this participant did not mention is that they are also being watched by people other than the public.

Almost all participants emphasised one benefit of obligatory disclosure as facilitating access to the government. The public may view the list of employees, allowing them to know who to address the issue to (Appendix H – Box 6-185: Theme 5-P010).

In short, obligatory disclosure assists the public in finding the right employee, which in turn translates to a more efficient and faster delivery of services:



"...so we know that that (particular) employee is the right person to contact." (P018)	*"...jadi kita tau orang yang tu ialah orang yang the right person yang kita boleh kita boleh hubungi." (P018)*

Box 6-186: Theme 5-P018

Knowing the right person to approach with queries and feedback saves the public a lot of time and energy. In particular, participants focused on 'direct access' to relevant employees as the main advantage for the public:

"One is, of course, easier direct access to employees for the public." (P006)	*"One is memang easier for public to access direct kepada dia." (P006)*

Box 6-187: Theme 5-P006

Participants who deals more with other government employees, explained that this assisted them if they have queries:

"...so we can say that access to me is easy, meaning that it's the main function to attend queries or questions." (P016)	*"...jadi kita boleh maklumkan capaian mudah kepada saya ini macam mana so maksudnya itu fungsi dialah yang paling utamalah supaya kalau ada pertanyaan ataupun soalan senang." (P016)*

Box 6-188: Theme 5-P016

Based on their experience as subjects and users of obligatory disclosure, participants were more inclined towards the positive aspects of this practice:

"Not disturbing I think...it's good that at least they (the public) can easily contact us, know who we are, to whom, it's easier." (P011)	*"Tak mengganggulah saya rasa... sebab bagus juga at least orang, siapa nak contact kita senang, tahu siapa kita, nak direct dengan siapa, memudahkanlah." (P011)*

Box 6-189: Theme 5-P011

Another participant, while agreeing that it is convenient for the public, stated a caveat regarding the extent to which this information does not interfere with his privacy:

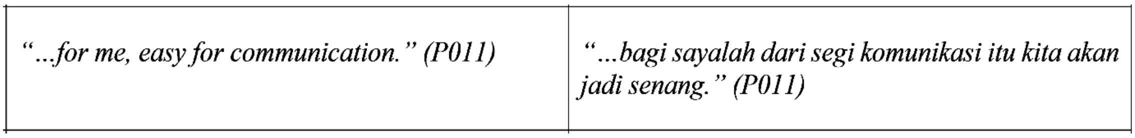
"I don't think it interferes (with privacy), actually it speeds up and facilitates delivery service to the public, only sometimes there are abuses..." (P007)	*"Saya rasa tak tak mengganggu (privasi), sebenarnya dia mempercepat dan mempermudahkan orang berurusanlah cuma kadang-kadang ada benda-benda yang disalahguna..." (P007)*

Box 6-190: Theme 5-P007

Therefore, we can see that in the eyes of the employees, although obligatory disclosure has the potential risk of being misused, they were willing accept it for the benefit to the public. However, this could suggest that it could result in an invasion of privacy if the perceived risk of information disclosure exceeded the benefits expected from the disclosure.

Improve efficiency

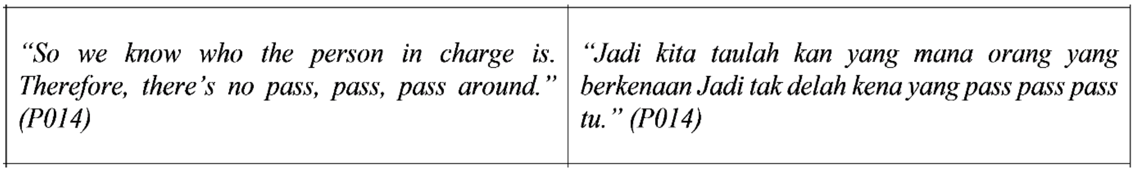
Another benefit that was captured by participants is the increase of service delivery. Faster services, easy communication and direct contact contributed to the advantages of obligatory disclosure. They saw it as:



"...for me, easy for communication." (P011)	*"...bagi sayalah dari segi komunikasi itu kita akan jadi senang." (P011)*

Box 6-191: Theme 5-P011

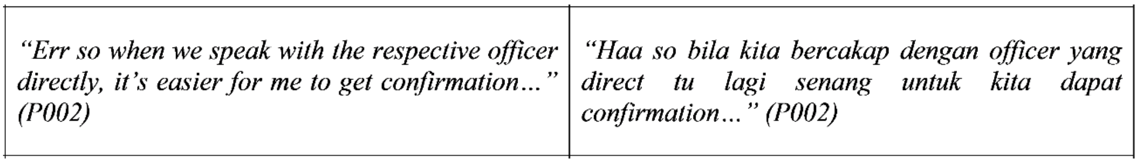
This is due to the ability of the public to contact employees directly. Participants shared a belief that by identifying which employees they wanted to communicate with, they could evade the so called 'passing around' syndrome:



"So we know who the person in charge is. Therefore, there's no pass, pass, pass around." (P014)	*"Jadi kita taulah kan yang mana orang yang berkenaan Jadi tak delah kena yang pass pass pass tu." (P014)*

Box 6-192: Theme 5-P014

Henceforth, faster services can be provided to the public:



"Err so when we speak with the respective officer directly, it's easier for me to get confirmation..." (P002)	*"Haa so bila kita bercakap dengan officer yang direct tu lagi senang untuk kita dapat confirmation..." (P002)*

Box 6-193: Theme 5-P002

One possible explanation for why participants held the view that direct access outweighed privacy concerns was that they also used this information themselves - either when conducting official duties or as a member of the general public seeking services from respective government agencies. Aside from benefitting the public, undoubtedly obligatory disclosure benefitted them as well as an employee. Participants were also asked about the benefits of obligatory disclosure to them as employee.

As they were directly experiencing this situation daily, it is appropriate to understand how obligatory disclosure could assist them in their daily work. It was evident that the participants themselves were using this disclosure regularly.

Participants associated the benefit of disclosure with the easier ability to find another employee, either for official or personal purposes. Armed with this information, they would then make contact with the employees - either by telephone number or email:

"I browse (the website) there are names, I can contact directly that's all." (P009)	*"Kita terus browse (laman web) dekat situ ada nama dia boleh hubungi terus, itu sajalah." (P009)*

Box 6-194: Theme 5-P009

Participants pointed to communicating directly with the specific person as the main reason that disclosure could benefit them. It assisted them in identifying the right person for specific queries, hence saving time and increasing public service delivery.

As such, obligatory disclosure will improve their work and their tasks:

"Mmm will speed up our work, our job…that is good. We are also able to go straight to the individual." (P012)	*"Mmm mempercepatkanlah kita punya kerja, ...itu baguslah. Kita pun akan terus kepada individu tersebut." (P012)*

Box 6-195: Theme 5-P012

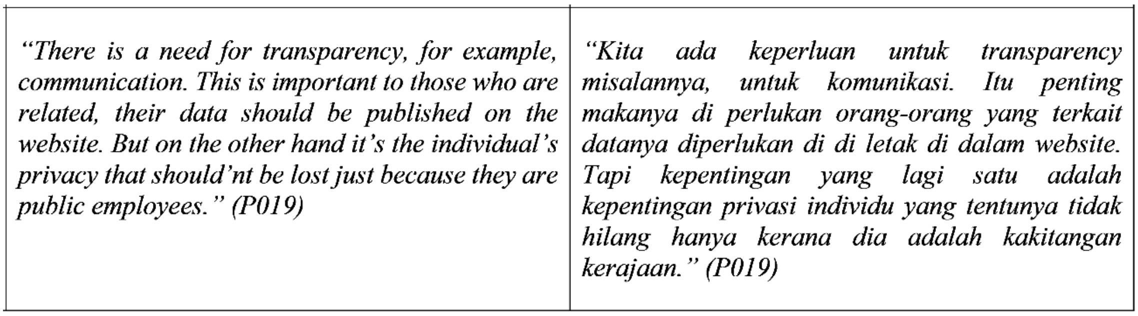
Another reason that could have an influence on participants' decisions regarding obligatory disclosure was because it could generate a positive impression of themselves. Two participants explicitly used the word 'proud' to describe their current feelings upon seeing their information available on their organisation's website. One possible reason for this is the idea of being associated with a reputable and trustworthy entity. Furthermore, it is considered an honour to serve one's country and its people. As such, positions come with a lot of competition and are difficult to secure, and they are generally well respected. Online image and reputation could possibly become one of the benefits that could be associated with obligatory disclosure.

Theme conclusion

Based on the findings, the fact that these experiences were shared by many participants indicates that they were focused on the benefits of the disclosure either to the public or themselves as employees. The relationship with the organisation that conducted obligatory disclosure was seen as having a strong influence on participants. Although some participants highlighted privacy implications with the disclosure, they are willing to sacrifice their personal privacy for much needed public services. In addition, personal benefits - such as positive reputation - might have an influence on their feelings around disclosure. This could be another reason why participants were less concerned by this disclosure. Employees weigh the risk-benefit calculation in deciding their privacy decisions (Dinev & Hart, 2006; Culnan & Armstrong, 1999). Individuals are influenced by a specific set of preferences during the decision process. According to Acquisti and Grossklags (2005), individuals are expected to make decisions based on incomplete information about possible consequences after their personal information is released. In addition, people also tend to make simplified decisions and rely on what they know (Smith et al., 2011; Acquisti & Grossklags, 2005).

Commentators

Commentators acknowledged the consequences of employees' privacy with obligatory disclosure. However, they adds that the government is promoting transparency to the public by publishing employees' information. They articulated the challenge clearly, in addressing the balance between the privacy interests of employees and the competing interests of e-Government:



"There is a need for transparency, for example, communication. This is important to those who are related, their data should be published on the website. But on the other hand it's the individual's privacy that should'nt be lost just because they are public employees." (P019)	*"Kita ada keperluan untuk transparency misalannya, untuk komunikasi. Itu penting makanya di perlukan orang-orang yang terkait datanya diperlukan di di letak di dalam website. Tapi kepentingan yang lagi satu adalah kepentingan privasi individu yang tentunya tidak hilang hanya kerana dia adalah kakitangan kerajaan." (P019)*

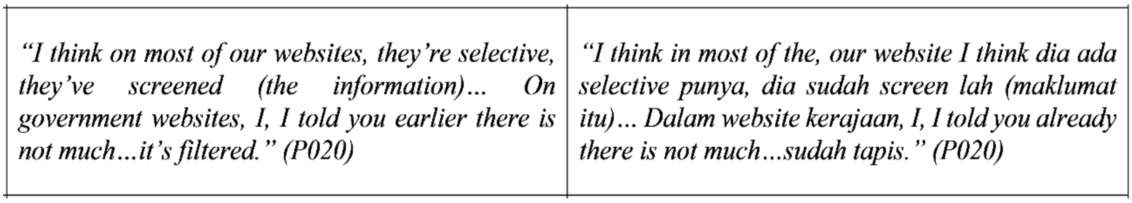
Box 6-196: Theme 5-P019-commentator

This remark signifies the importance of obligatory disclosure to the employees, which supported the data collected from interviews. Nevertheless, the balance between a government's interest in enhancing service delivery and an individual's privacy must be considered in order to achieve the goals of e-Government and at the same time protect an employee's privacy.

6.2.5.1 Trust in the organisation to alleviate employees' privacy concerns

This theme focuses on the trust in an organisation, which is considered as a sub-theme for theme 5. Participants demonstrated a high level of trust towards their organisation and this was noticeable during the interviews.

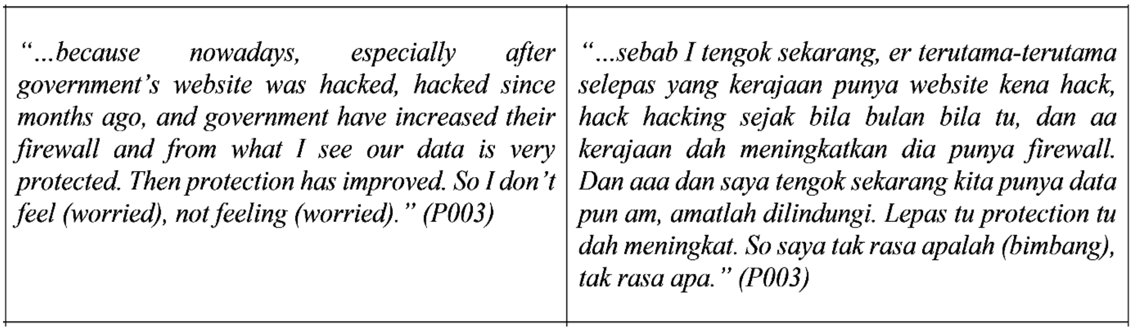
As the official website was under their organisation's IT division/unit jurisdiction (depending on organisation), participants believed reasonable safety and security steps had been taken before information about them was published online. They described their confidence over security measures employed by their organisation's IT division:



"I think on most of our websites, they're selective, they've screened (the information)... On government websites, I, I told you earlier there is not much...it's filtered." (P020)	*"I think in most of the, our website I think dia ada selective punya, dia sudah screen lah (maklumat itu)... Dalam website kerajaan, I, I told you already there is not much...sudah tapis." (P020)*

Box 6-197: Sub-theme 5-P020

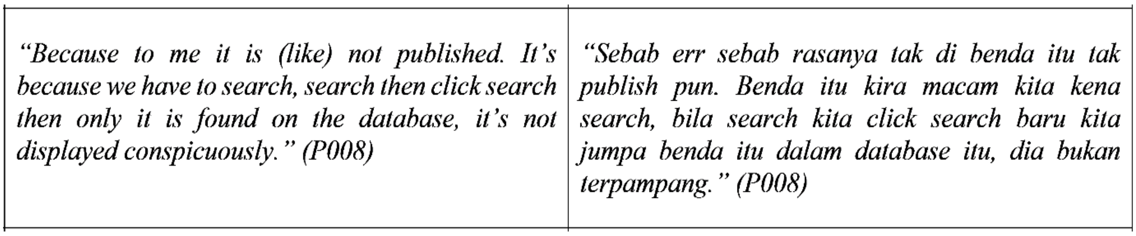
Similarly, another participant shares the same level of confidence in their organisation's safety and security measures:



"...because nowadays, especially after government's website was hacked, hacked since months ago, and government have increased their firewall and from what I see our data is very protected. Then protection has improved. So I don't feel (worried), not feeling (worried)." (P003)	*"...sebab I tengok sekarang, er terutama-terutama selepas yang kerajaan punya website kena hack, hack hacking sejak bila bulan bila tu, dan aa kerajaan dah meningkatkan dia punya firewall. Dan aaa dan saya tengok sekarang kita punya data pun am, amatlah dilindungi. Lepas tu protection tu dah meningkat. So saya tak rasa apalah (bimbang), tak rasa apa." (P003)*

Box 6-198: Sub-theme 5-P003

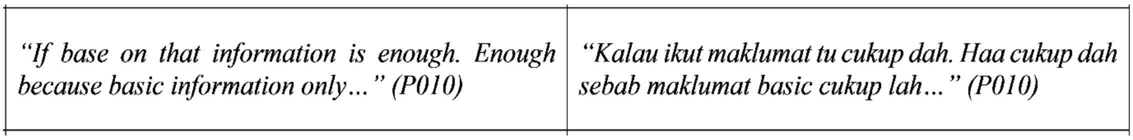
Participants also describe the disclosure as not 'openly' done. To them, their information was not directly displayed but instead was quite hidden from public view. This means that employees' information could not directly be viewed on the website's homepage, but instead users have to click a few times before arriving at the staff directory area. Layers of pages that 'buried' employees' information added to the assumption of safety from participants.



"Because to me it is (like) not published. It's because we have to search, search then click search then only it is found on the database, it's not displayed conspicuously." (P008)	*"Sebab err sebab rasanya tak di benda itu tak publish pun. Benda itu kira macam kita kena search, bila search kita click search baru kita jumpa benda itu dalam database itu, dia bukan terpampang." (P008)*

Box 6-199: Sub-theme 5-P008

Participants also perceived that the organisation disclosed limited information about an employee. This response was evident from many participants:



"If base on that information is enough. Enough because basic information only..." (P010)	*"Kalau ikut maklumat tu cukup dah. Haa cukup dah sebab maklumat basic cukup lah..." (P010)*

Box 6-200: Sub-theme 5-P010

They suggested that their information disclosure is not detailed and only certain information was revealed by their organisation.

Interview data suggested that the employees had a high level of trust in their organisations. Many participants expressed confidence that appropriate measures were carried out to protect employees' information.

Theme conclusion

From the above responses, it can be suggested that participants perceived the disclosure of their information on their organisation's website was non-threatening, because of their confidence in their organisation. This assertion can be attributed to the high trust that the employees had towards their organisation. This perception influenced how participants viewed their privacy implications with regard to this disclosure. Higher trust in institutions was found to influence individuals' belief that adequate measures were undertaken by the institution to treat personal information sensitively (Devos et al., 2002). As the organisation is the individual's employer, and also the Government, participants seem to indicate a higher perception of trust towards them. This perception was then translated to the online environment, where similar perceptions transpired. Asian countries were found to have a higher degree of trust in government websites compared to western countries. As Malaysia is an Asian country, these findings are in line with what Hsu (2006) reported.

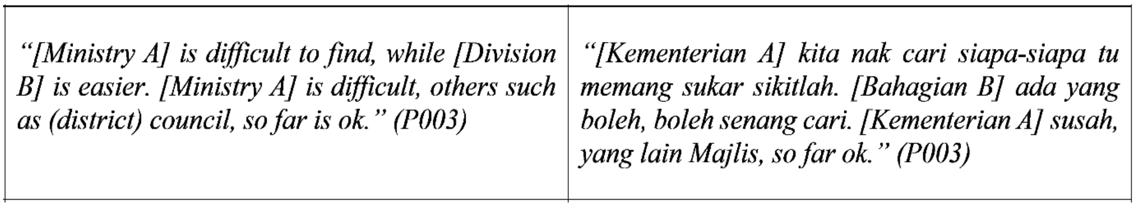
6.2.6 Lack of emphasis on employees' privacy in public organisations result in unreasonable amounts of personal information disclosure

Organisation's policy

The results from the participants indicated mixed answers about why employees' information disclosure was practiced by their organisations through their official websites. In general, participants claimed that obligatory disclosure on the Malaysian Government's website happened for regulatory reasons, which ranged from government policy across all agencies, to the agency's own decision, to no policy at all.

Two participants mentioned that it was department policy; some said it was from top management instruction, whilst others believed it was the government's policy that covered all departments and ministries.

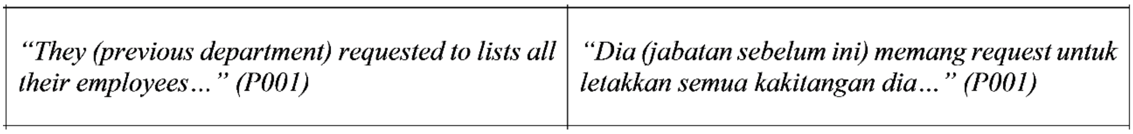
Conversely, one participant clearly stated that there was no policy regarding publishing employees' information on the organisation's website. This corresponded to another participant's responses, who described several different versions of obligatory disclosure. On some websites, information on employees' is easy to find whilst on others it is difficult.



"[Ministry A] is difficult to find, while [Division B] is easier. [Ministry A] is difficult, others such as (district) council, so far is ok." (P003)	*"[Kementerian A] kita nak cari siapa-siapa tu memang sukar sikitlah. [Bahagian B] ada yang boleh, boleh senang cari. [Kementerian A] susah, yang lain Majlis, so far ok." (P003)*

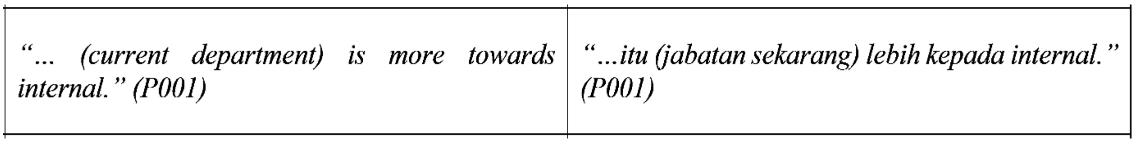
Box 6-201: Theme 6-P003

For instance, one participant experienced two different policies on obligatory disclosure when it was posted by two different organisations. While both organisations disclose employees' information via a staff directory on their websites, the revelation of individuals differed between the organisations. Prior to this, the participant's personal information was published on the website for public viewing and could be accessed by anyone. In the current organisation, the publication of employees on the staff directory page was limited to selected employees only. However, a full staff list was available to other employees but it was only for internal viewing. For his previous department:



"They (previous department) requested to lists all their employees…" (P001)	*"Dia (jabatan sebelum ini) memang request untuk letakkan semua kakitangan dia…" (P001)*

Box 6-202: Theme 6-P001



"… (current department) is more towards internal." (P001)	*"…itu (jabatan sekarang) lebih kepada internal." (P001)*

Box 6-203: Theme 6-P001

Hence different departments have different policies regarding the disclosure of their employees' details on the websites. Some participants mentioned that all employees were disclosed, while others mentioned that only selected employees were disclosed (for example Appendix H – Box 6-204: Theme 6-P014).

When discussing IT policy within the Malaysian Government system, a central agency named Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) was brought forward by five participants. This is a unit under the Prime Minister's department which is responsible for IT development in the public sector. Participants identified MAMPU as the agency that developed policies for Malaysian Government websites including 'obligatory disclosure policy'. However, participants were not sure whether there is actually a policy or a set of guidelines which touch on obligatory disclosure.

"I believed MAMPU came up with what they say similar like a service circular." (P016)	*"Saya rasa ada dalam MAMPU dia ada keluarkan dia panggil apa lebih kurang macam pekeliling perkhidmatan jugalah." (P016)*

Box 6-205: Theme 6-P016

In contrast, some participants strongly believed there are no circulars regarding obligatory disclosure:

"No, there is no circulars." (P009)	*"Tak ada, tak ada satu pekeliling pun." (P009)*

Box 6-206: Theme 6-P009

Additionally, other participant mentioned that it seemed like a standard practice for Malaysian Government's websites to have a staff directory available for public viewing:

"If according to Malaysian Government standard, it is a must, must have." (P013)	*"Kalau ikut standard website Kerajaan Malaysia, perlu ada, kena ada." (P013)*

Box 6-207: Theme 6-P013

This statement was not referring to a standard practice on obligatory disclosure but instead to the standard inclusion of a staff directory feature on government websites. According to the participant, information about employees was seen a standard practice for Malaysian Government websites, based on MAMPU directives. MAMPU, which is the agency that conducted the annual MGPWA, together with another agency (MDEC) published their assessment methodology details. Another participant elaborated in more detail - among the content that was required was employment information, which was assumed as compulsory:

"...must have, most importantly is the organisation information, organisation chart, vision, mission, objective, function from top to bottom, directory, announcement, or circulars, circular letters. Anything related to general function or specific function (of the agency) must be included, that is the basic information on the web, photographs, location, map, telephone number for queries, which is basic." (P016)	*"... mesti ada yang paling pentinglah maklumat organisasi, carta organisasi, visi dan misi, objektif, fungsi daripada atas sampai ke bawah, direktori, pengumuman, ataupun pekeliling, surat edaran. Apa yang berkaitan dengan fungsi-fungsi umum atau khusus mesti ada dalam, itu yang basic mesti ada dalam laman web; gambar, kedudukan, peta lokasi, nombor telefon kalau ada pertanyaan itu basic." (P016)*

Box 6-208: Theme 6-P016

Another participant who had experienced this assessment believed that employees' information must be included:

"I didn't notice, but err staffs information must be included" (P018)	*"Saya tak perasan tak tapi tapi err kaki, kakitangan memang perlu ada." (P018)*

Box 6-209: Theme 6-P018

Findings from participants suggest that, significantly, participants' responses clearly showed that they were not sure about any policies regarding obligatory disclosure. Employees relied on criteria and guidelines from the MGPWA regarding obligatory disclosure. This could indicate that the criteria and guidelines for this assessment were assumed by the participants to be a directive for standards in government websites.

MGPWA report

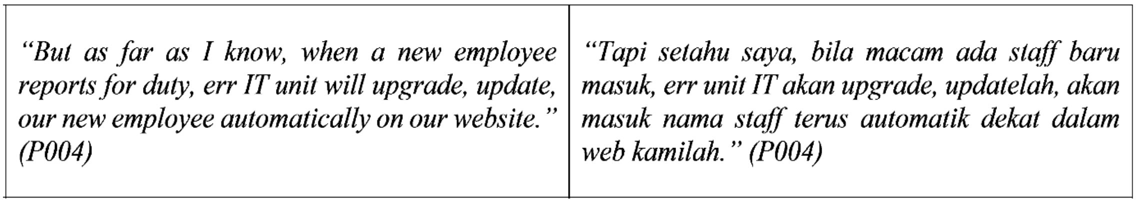
The MGPWA 2012 report did not state that it is compulsory for government websites to include a staff directory. However, it mentioned a staff directory as an example for *searchable database* criteria. This could imply that government employees, including the IT staff responsible for websites, misinterpreted the example as a requirement for MPGWA. The report also listed four criteria that are relevant to this study. Under the *content* pillar, *phone contact, address, email* and *about us* were listed as the criteria of assessment. Personal information of employees could be disclosed when government websites tried to comply with the criteria. Upon further examination, only *email* was found to suggest the disclosure of employees' personal information while the other criteria do not. What was stated in the criteria of assessment is: *"... that allows citizens to contact the respective government unit."* (Multimedia Development Corporation, 2012 p. 58).

Obligatory disclosure process

This category refers to the examination of participants' knowledge on the process of publishing their personal information on the organisation's website. Although participants gave mixed answers regarding the policy or guidelines concerning obligatory disclosure, it is beneficial to assess their knowledge regarding the process of obligatory disclosure of their information.

The participants' knowledge of the process may indicate how well the employees were informed on the usage of their personal information by their organisation. Equally important would be to gather how curious participants are around the process of the publication of their personal information on the organisation's website. By understanding the process behind the publication, employees would know how their personal information would be treated, and what to do if certain privacy issues arose.

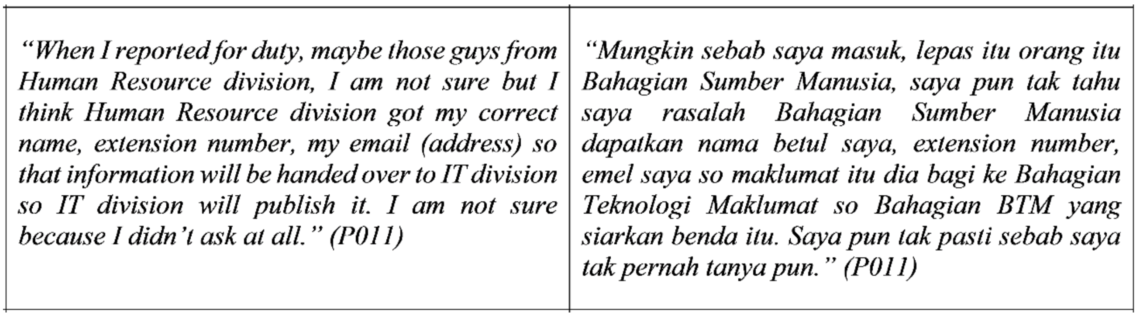
Interview data showed that most participants were not informed on the process of obligatory disclosure. Participants, without hesitation, answered "don't know" when asked how their information came to be published on the website but tried to explain. Interestingly, two participants believed that this was automatically done to all employees. Whilst this doesn't mean that it is 'automatically' updated, it could mean that obligatory disclosure is in fact mandatory. Therefore, there is no need for them to know and understand the process.



"But as far as I know, when a new employee reports for duty, err IT unit will upgrade, update, our new employee automatically on our website." (P004)	*"Tapi setahu saya, bila macam ada staff baru masuk, err unit IT akan upgrade, updatelah, akan masuk nama staff terus automatik dekat dalam web kamilah." (P004)*

Box 6-210: Theme 6-P004

Some of the participants made assumptions about the process. Most of them pointed to the Information Technology (IT) division/unit as the main unit responsible for publishing information on the website. This is not surprising, since the IT unit was being tasked with handling all the IT-related facilities and infrastructures within the organisation, including the website. Human Resources departments were also mentioned by participants as handling employee-related information.

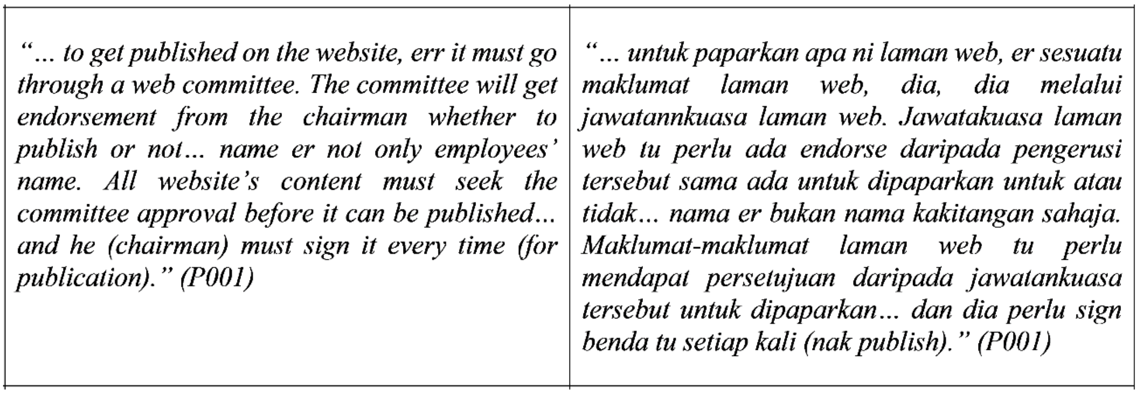


"When I reported for duty, maybe those guys from Human Resource division, I am not sure but I think Human Resource division got my correct name, extension number, my email (address) so that information will be handed over to IT division so IT division will publish it. I am not sure because I didn't ask at all." (P011)	*"Mungkin sebab saya masuk, lepas itu orang itu Bahagian Sumber Manusia, saya pun tak tahu saya rasalah Bahagian Sumber Manusia dapatkan nama betul saya, extension number, emel saya so maklumat itu dia bagi ke Bahagian Teknologi Maklumat so Bahagian BTM yang siarkan benda itu. Saya pun tak pasti sebab saya tak pernah tanya pun." (P011)*

Box 6-211: Theme 6-P011

It can also be observed that they didn't know about the process, and was not concerned about how their information was disclosed on the organisation's website.

Although the participants were not informed of the process, some of them claimed that they knew the process, and admitted to knowing it without being told. They claimed that they found out about it informally due to their experience within the government. Another, as an IT staff member, had a better explanation on the process. The participant mentioned about a website committee that was responsible for anything published on the website, which all the other participants didn't.

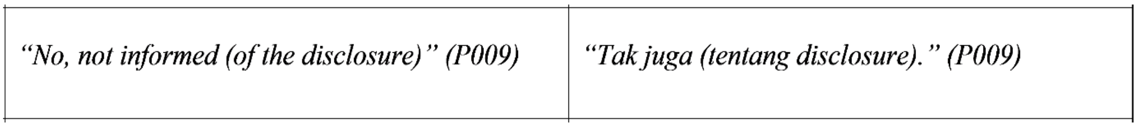


"... to get published on the website, err it must go through a web committee. The committee will get endorsement from the chairman whether to publish or not... name er not only employees' name. All website's content must seek the committee approval before it can be published... and he (chairman) must sign it every time (for publication)." (P001)	*"... untuk paparkan apa ni laman web, er sesuatu maklumat laman web, dia, dia melalui jawatannkuasa laman web. Jawatakuasa laman web tu perlu ada endorse daripada pengerusi tersebut sama ada untuk dipaparkan untuk atau tidak... nama er bukan nama kakitangan sahaja. Maklumat-maklumat laman web tu perlu mendapat persetujuan daripada jawatankuasa tersebut untuk dipaparkan... dan dia perlu sign benda tu setiap kali (nak publish)." (P001)*

Box 6-212: Theme 6-P001

Low employees' participation

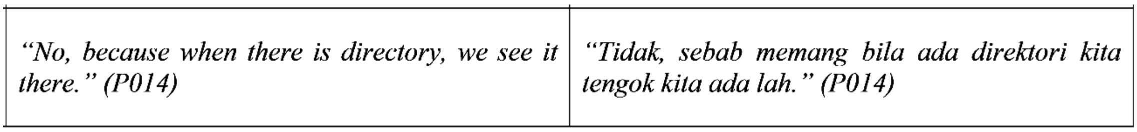
Currently, participants were not referred to when their organisation intended to publish their information on its website. Participants only knew of the publication when they browsed the website and discovered themselves. When asked directly whether they were informed about the publication, nine participants assuredly mentioned they didn't. They said:



"No, not informed (of the disclosure)" (P009)	*"Tak juga (tentang disclosure)." (P009)*

Box 6-213: Theme 6-P009

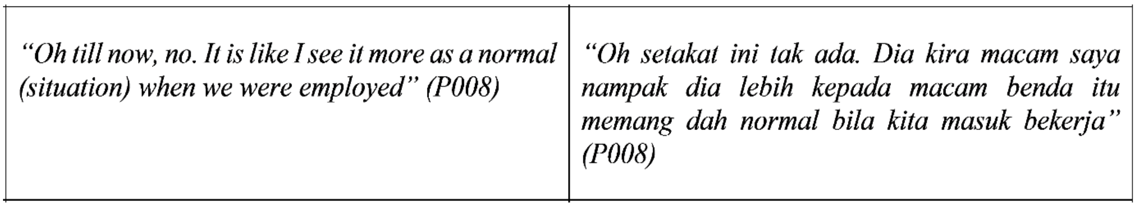
Similarly, others was also not informed and only knew of the disclosure by browsing the directory:



"No, because when there is directory, we see it there." (P014)	*"Tidak, sebab memang bila ada direktori kita tengok kita ada lah." (P014)*

Box 6-214: Theme 6-P014

Another participant concurred and explained why:

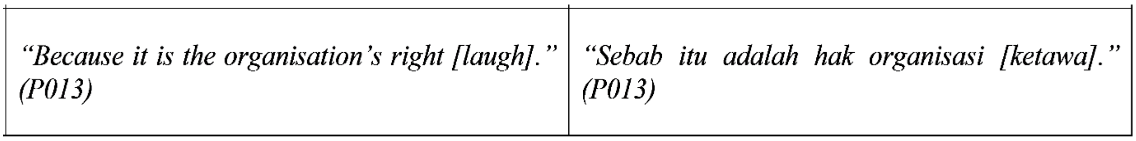


"Oh till now, no. It is like I see it more as a normal (situation) when we were employed" (P008)	*"Oh setakat ini tak ada. Dia kira macam saya nampak dia lebih kepada macam benda itu memang dah normal bila kita masuk bekerja" (P008)*

Box 6-215: Theme 6-P008

The responses supported the organisational culture findings which led to employees believing that the publication of personal information is a requirement for every employee. As stated earlier, although participants were clueless around how their personal information was being treated for publication, less effort was seen from the participants to gather information about this treatment.

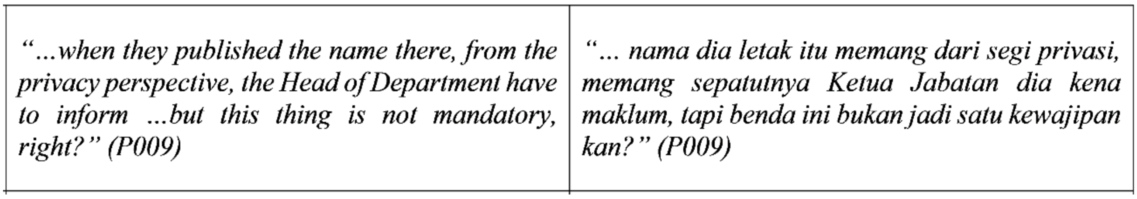
One participant believed that this information did not belong to the employees but to the organisation. Therefore, if it does not belong to the employees then there would be no need for the organisation to inform the employees or request consent when publishing information about them



"Because it is the organisation's right [laugh]." (P013)	*"Sebab itu adalah hak organisasi [ketawa]." (P013)*

Box 6-216: Theme 6-P013

Some participants perceived that it is the right of the organisation to publish any information that belongs to them. Another participant, although agreeing that the publication of employees' information may lead to a breach of employees' privacy, however believed that would not be an obligation for the organisation to refer to the employees before publishing it:



"...when they published the name there, from the privacy perspective, the Head of Department have to inform ...but this thing is not mandatory, right?" (P009)	*"... nama dia letak itu memang dari segi privasi, memang sepatutnya Ketua Jabatan dia kena maklum, tapi benda ini bukan jadi satu kewajipan kan?" (P009)*

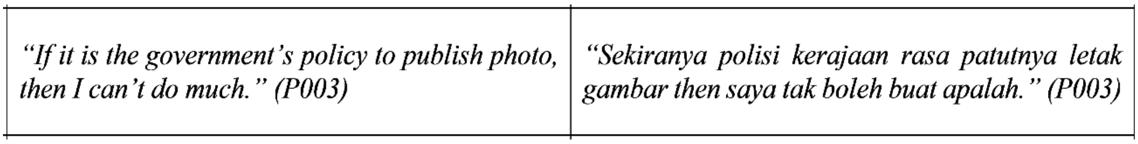
Box 6-217: Theme 6-P009

This remark hinted that obtaining consent from employees is unusual in this context. The argument that it is not mandatory to inform employees shows the influence of the organisation's perceived ownership of the information. Most of the participants believed that it was their organisation's responsibility to disclose information on the official website.

Privacy was strongly connected with the element of control, by referring to Westin's (1967) view of privacy. According to him, the ability to control an individual's information about themselves underlined the concept of privacy.

If users were to be given the power to control their disclosure, they themselves would have to accept responsibility for the disclosure of their personal information. It is postulated that users with higher levels of control would be more willing to disclose information about themselves because of the perception of having lower privacy risks. Users with a lower level of control seem to disclose less information because they perceived privacy risks as higher.

Furthermore, employees expressed their inability to control the disclosure of their personal information on government websites. They expressed disappointment at their inability to decide on the degree of how much of their personal information should be disclosed. They stated that they have no choice but to accept it, if it's the policy of the government:

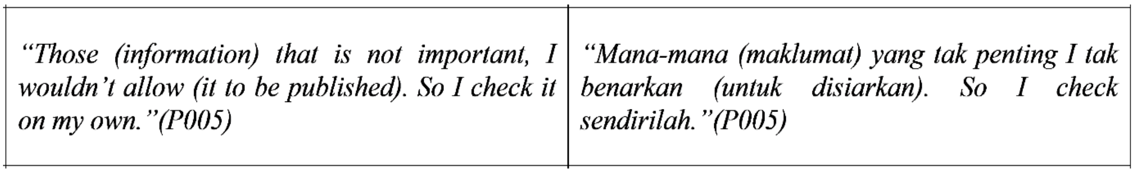


"If it is the government's policy to publish photo, then I can't do much." (P003)	*"Sekiranya polisi kerajaan rasa patutnya letak gambar then saya tak boleh buat apalah." (P003)*

Box 6-218: Theme 6-P003

They expressed a wish to have their photograph removed from the website. They further explained that it was difficult for them to protect their information because it was beyond their control, and it is the department's decision to decide the degree of disclosure.

In contrast, some participants explained that they personally inspected their information and instructed their organisation to remove any information about them that was not important or relevant:



"Those (information) that is not important, I wouldn't allow (it to be published). So I check it on my own."(P005)	*"Mana-mana (maklumat) yang tak penting I tak benarkan (untuk disiarkan). So I check sendirilah."(P005)*

Box 6-219: Theme 6-P005

Since some participants have the capacity to influence their organisation directly, they had the opportunity to prevent any disclosure about them that was deemed inappropriate. Their confession that they filter their information implies the mounting privacy invasion contributed to by government websites towards their employees. Hence, when employees have the ability to control their disclosure, protective steps were taken in order to minimise the loss of their privacy.

Data from the study indicated that participants do not have a clear understanding of the process of obligatory disclosure. Understanding the process allowed employees to voice their concerns, (if any), related to published information on the website to responsible parties. Employees knew where to go and how to direct their complaints, and did not waste time searching for the responsible person. Subsequently, the error would be addressed in a shorter period of time because the responsible person was contacted and the correct procedure was followed for correction.

Knowledge on the flow of information, starting from the owner (i.e. employee) to eventually being published on the website, would assist employees in lodging complaints when they identified errors on information about themselves. The issue of errors was one of the concerns raised about information privacy. Employees did not feel comfortable if information about them was inaccurately disclosed. Conversely, information on how the disclosure process works will indicate some level of transparency to their employees, as employees were identified as one of the important stakeholders in e-Government initiatives (Ndou, 2004).

Theme conclusion

Findings showed evidence that participants were not informed on the obligatory disclosure of information and consent was not sought. The findings on the process of disclosure affirmed that a minimum of participation from employees was sought when deciding on publication of the information on the government websites. Furthermore, the status of the obligatory disclosure’s policy was not being made clear to them. A large number of employees raised questions on how the issue of obligatory disclosure was addressed by the Government. In addition, most participants believed that this disclosure was the organisation’s policy or directive, and therefore this could suggest that employees felt that it was not their responsibility. Based on these results, it can be claimed that employees have no control over their personal information disclosure on an organisation’s website and participants’ consent was not obtained before the publication of their personal information - thus reflecting a low amount of employees’ participation regarding obligatory disclosure.

As presented in section 5.1.3, sensitive information and unrelated information were found to be available publicly on government websites. Equally important is the high number of individuals exposed online. In fact, the participants were not expecting such diverse amounts of personal information (including irrelevant and unnecessary information) to be made available on their organisation’s website. Thus, ‘unreasonable’ employees’ personal information was disclosed on organisation websites.

Commentator: IT stakeholders

A commentator from MAMPU confirmed that there was no specific standard for a staff directory feature on government websites.

“There’s no standard. It’s up to the respective department on how to publish it.” (P023)	*“Takde tak standard. Dia terpulang kepada agensi tu sendiri nak buat macam mana.” (P023)*

Box 6-220: Theme 6-P023-commentator

By not having a standard guideline or policy, this confirmed the findings from participants about inconsistencies in the staff directory, and ultimately on the practice of obligatory disclosure. This was the reason why some agencies were employing obligatory disclosure in a different manner to another agency. The commentator also confirmed that the latest circular (at the time of interview) related to government websites was published in 2006 and entitled *Circular 1/2006: Public Sector Website/Portal Management*. According to the circular, the staff directory is a basic mandatory feature for public sector websites. It stated three attributes that should be disclosed, namely: telephone number; email address; and employees' work scope. However, the circular is silent on what extent of employees that should be included. Of direct reference to the guidelines, an interpretation could be made that all employees should be listed in the staff directory, because the staff directory must be provided according to work scope or agency's function.

It was also noted that Circular 1/2006 did mention the risk of spamming and advised organisations to publish email addresses statically instead of as hyperlinks. While concerns on the privacy risk were stated, this is limited to a single type of information and threat. Moreover, the preventive suggestion that was presented was incapable of avoiding spamming as the findings of this study discovered.

Furthermore, the commentator clarified that privacy issues were not an important criterion for consideration in the implementation of government websites, except for the privacy policy that was stated on the website itself:

"Yes, only that privacy policy." (P023)	*"Ya privacy policy tu aja lah." (P023)*

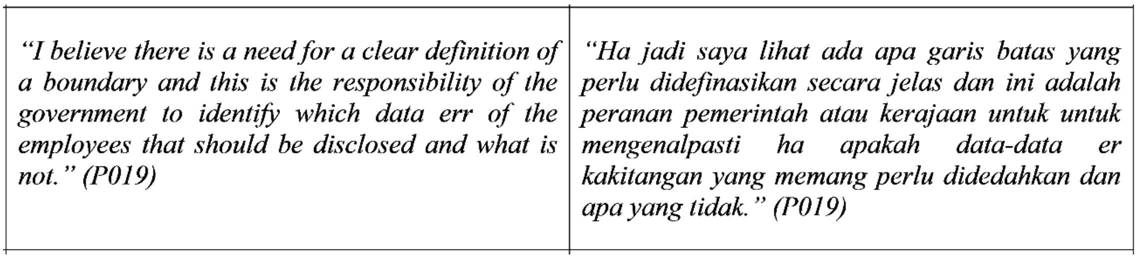
Box 6-221: Theme 6-P023-commentator

The privacy policy that was referred to by the commentator was found on every website during the web content analysis. Therefore, it can be seen that most public organisations were adhering to the Government policy by having their privacy policy on the websites, in line with Circular 1/2006. Nevertheless, as stated in chapter four, this privacy policy primarily focuses on website users (i.e. the public) and their information - specifically about a user's information that is submitted through the website and the collection of this information.

There was no indication of privacy protection for personal information that originates from the website. Although Circular 1/2006 did mention protected information - for example personal information, payment details, procurement information and information that relates to privacy - it was more on the security aspect rather than for privacy issues. This could indicate that government websites were more concerned with users’ privacy implications rather than that of employees (i.e. internal). The various types of personal information that were found from web content analysis can be linked to a lack of emphasis on employees’ privacy on government websites. Discoveries of sensitive information - such as national identification number, date of birth, or family members - strengthened the need for a set of guidelines or a robust policy which will also recognise the participation of employees on the website, specifically regarding their personal information. Therefore, although there were privacy policy statements displayed on government websites, the emphasis on privacy as an important issue in obligatory disclosure needs to be addressed.

Commentator

The importance of establishing a set of standard guidelines or a policy was recognised by commentators. This was one of the weaknesses mentioned by commentators. For instance, they directly touched on the practice of obligatory disclosure and felt that the lack of guidelines or policy made the area difficult for both employees and organisation. If there are clear guidelines in place, it will enable both the employees and the organisation to clearly understand how their personal information is used on the organisation’s website.



“I believe there is a need for a clear definition of a boundary and this is the responsibility of the government to identify which data err of the employees that should be disclosed and what is not.” (P019)	*“Ha jadi saya lihat ada apa garis batas yang perlu didefinasikan secara jelas dan ini adalah peranan pemerintah atau kerajaan untuk untuk mengenalpasti ha apakah data-data er kakitangan yang memang perlu didedahkan dan apa yang tidak.” (P019)*

Box 6-222: Theme 6-P019-commentator

In addition, from a macro perspective, they suggests that privacy issues should be included as part of a national agenda. While acknowledging that the Government has implemented initiatives to promote privacy in Malaysia, much more has to be done since current initiatives are limited and not comprehensive.

"But I saw it as a non-agenda, it is not a national agenda because one finding said that although we claim that security, or privacy or data disclosure is important but if it is not acknowledged as (a national) policy, then it is not going to be good for the people." (P022)	*"Tapi I nampak dia bukan bukan agenda, dia bukan a national agenda err because one findings says that walaupun kita, kita claim katakan er security atau atau pun privacy atau pun data disclosure ni sangat important tapi kalau dia tidak dipandang sebagai negara punya negara punya, apa ek keperluan macam yang penting tau sangat penting ha dasar (negara) then dia tidak akan jadi satu benda yang baik untuk rakyat." (P022)*

Box 6-223: Theme 6-P022-commentator

By incorporating privacy as a national agenda, it is believed that it will increase public awareness of privacy issues and public administration will therefore indirectly benefit from this awareness.

Both commentators highlighted the importance of establishing a comprehensive privacy policy and the role that an organisation plays in addressing privacy issues for employees. Lack of emphasis on privacy was identified as a factor for inconsistencies on obligatory disclosure. As a result, irrelevant personal information, an unreasonable number of individuals and information leakage were encountered in obligatory disclosure.

6.2.7 Concluding remark

This section has brought together the results of the two data collection techniques of this research. The web content analysis provided an overview of a realistic account of disclosure on government websites, whereas the in-depth semi-structured interviews provided deeper understandings of employees' experiences around obligatory disclosure. As a consequence, incorporating both results revealed a comprehensive picture regarding the disclosure.

CHAPTER 7

Discussion

7.1 Discussion

This section will discuss the findings with regards to the work of other scholars. It has been recognised that there is a lack of research considering disclosure of personal information by a third party. As stated in chapter one, this study is designed to capture individual perspectives of obligatory disclosure and their relation to privacy. Thus, this research will provide contextual knowledge and situational factors in understanding the privacy issues of obligatory disclosure.

The main case of this study, as presented in chapter three, is: *public employees' experiences over obligatory disclosure and its relation to their privacy,* while the embedded case is the: *personal information of public employees that is publicly available on public organisation's website*. This case was investigated by using multiple techniques, as explained in the same chapter. A conceptual framework – obligatory disclosure – was introduced in order to define the contextual direction of the phenomenon.

The practice of obligatory disclosure

Obligatory disclosure by government organisations is a common practice for many governments in the development of e-Government initiatives (Odendaal, 2003; Siar, 2005; Simpson, 2011; Badrul et al., 2014). However, the issue of disclosing personal information of employees raises privacy concerns as the information is disclosed publicly. This study selected some of the websites that emerged as top-ranked sites in MGPWA 2012 as samples for this study. The MGPWA assessment was benchmarked against two international assessment standards in order to ensure that the Malaysian

Government's website is in line with world standards. A commentator that conducted the assessment of MGPWA points out the outcome of having scored in the top-rank in the assessment:

"The website is (of) high quality." (P021)	*"Website ni berkualiti lah." (P021)*

Box 7-1: Discussion-P021

Findings indicated that obligatory disclosure promotes the disclosure of employees' personal information. Several features that assist in the dissemination of personal information were available on the websites. In addition, 23 different types of personal information comprising from six categories of personal information were identified, plus the implicit category of organisational names. A taxonomy of personal information was presented in section 5.1.2. The fact that an extensive amount of personal information can be found publicly from a single type of website (i.e. Government) raises concerns. In addition, as the sampled websites were considered as high quality government websites (of Malaysian standard) and the assessment method was benchmarked against the international standard, it raises questions on whether the disclosure is intentional and represents the aspiration of governments worldwide.

Furthermore, government websites are considered to be trustworthy platforms (Hsu, 2006) where personal information that is published is considered as accurate and authentic. From the point of view of valuable personal information, verified and truthful information is assumed to have a higher value and quality (van Dijck, 2013) which in this case may apply to information that was found from obligatory disclosure.

Obligatory disclosure disclosed individuals' distinctive traits such as name, photographic image, gender, age, date of birth etc. These identifying factors are normally used in official or business activities. For example, when opening a bank account, applying for a driving licence, registering in a hotel etc. In the online environment, this information is required in email password verification such as in Yahoo! mail and Gmail from Google. Also, *employment information* and *personal achievement information* may provide subjective information about an individual such as their social status, buying power, professional interest, organisational influence and even their career prospects. Despite the fact that salary information was absent from Malaysian websites, an employee's salary can be estimated from the employment information by analysing several attributes such as working grade and working title. Also, employees can be easily contacted and located since *contact information* and *geographical information* can be collected from the website. Another type of information is the *timeliness information*. This information basically informs of activities or events that were attended or organised by the organisation. Indirectly, employees' information was also revealed to the public.

Findings revealed that employees were exposed to higher privacy risks with obligatory disclosure. This was explained by the characteristic of obligatory disclosure that increased the vulnerability and risks of employees and were reported in some studies (Trend Micro Incorporated, 2012; Symantec Corporation, 2013; Symantec Corporation, 2016; Symantec Corporation, 2015). The easiness and low-cost strategy of collecting employees' personal information made it possible for anyone without any high technical capability to target an individual. This is in contrast with information on online social network (OSN), where at least published information can be configured to restrict viewers. In addition, to gather personal information from OSNs, researchers demonstrated technical techniques in order to acquire the personal information of individuals (He et al., 2006; Mislove et al., 2010). Due to the complexity of the techniques, additional skills are required for inferring information from OSNs.

Demographic properties

Individual demographic profiles were found to influence an individual's perception of privacy concerns (Joinson et al., 2010; Nosko et al., 2010; Zukowski & Brown, 2007; Janda & Fair, 2004). However, in obligatory disclosure there were no clear demographic characteristics that were found to influence participants. Age, gender, race, income and education did not provide sufficient evidence for any significant influence. Employees' work responsibilities or work experience were found to have some influence on how participants viewed obligatory disclosure. Two participants that were highly concerned with obligatory disclosure (from the beginning) were found to both be in the top management category. This could indicate that those with a higher level of authority tended to be more aware and concerned about privacy issues than those with less responsibility. However, another top management participant did not share similar privacy concerns and awareness. Instead, the participant was more focused on the benefit that the public could get from obligatory disclosure.

Three participants who experienced enforcement duties differed on privacy concerns regarding obligatory disclosure. One of them was not concerned about obligatory disclosure; another was concerned about specific types of information disclosure (i.e. photographs); and the third, was concerned with the privacy of employees. It can also be seen that participants who are involved in sensitive roles showed higher concerns compared to other participants.

In contrast, P015 is the only participant who was not bothered about his obligatory disclosure, and was also unsure about his information on the organisation’s website. Also, he admitted to forgetting his email password which gave the impression that this mode of communication is not important for him for his daily work. This could be due to his role as an office assistant that requires him to frequently work outside his office.

Participants with IT or computer-related background were observed to have higher privacy concerns regarding obligatory disclosure compared to those of other participants. Five participants four of whom had background knowledge in IT or computers, were particularly concerned with the disclosure of their personal information by their organisation. Two participants responded with a very high concerns on the practice of disclosing employees’ information, while one showed some reluctance and another agreed that obligatory disclosure brought privacy implications. The results could suggest that high knowledge of IT or computers is likely to influence more privacy concern for a person. The finding is in contrast to a previous study (Dinev & Hart, 2004b) but is consistent with the claim that the relationship of Internet knowledge and privacy is complex and multi-faceted (Li, 2011). In contrast, one participant, while showing high concern of information privacy in general, demonstrated low privacy concern regarding obligatory disclosure.

Even though maximum variation purposive sampling was conducted to increase the diversity of participants, it could be argued that the findings may be limited to certain public service categories. Similar studies that explore different job roles among employees may provide a different result. As presented in this study, employees in roles considered sensitive were found to be more concerned. Furthermore, it was suggested by many participants that sensitive job roles should not be disclosed.

A large working category of this study comprises the Professional and Management group and the Support group. It is therefore possible that the findings are represented by these two working groups. It should be noted that while the Top Management group were less represented, the findings indicate that this working group’s concerns about privacy are higher in regards to obligatory disclosure.

The result should also be interpreted in the Malaysian context as culture was identified to have an effect in obligatory disclosure. Researchers indicate that cultural values can influence how people perceive disclosure issues (Milberg et al., 2000; Krasnova et al., 2012). However, similar countries that share at least some basic characteristics with Malaysia may be of value in this context.

Whilst Bansal et al. (2010) identified that personal knowledge and experience of invasion of privacy were found to increase individuals’ privacy concerns, the findings of this study suggests that experience with obligatory disclosure may not necessarily increase users’ privacy concerns. It discovered that participants were uncomfortable with the situation. Even participants that had experienced privacy intrusion before (e.g. P018) were still willing to accept obligatory disclosure because of the benefit and its main purpose.

Henceforth, it is likely that certain situational factors may have a greater influence towards individuals’ privacy concerns. As suggested by Li et al. (2010), situational factors at specific levels are very likely to influence other factors that had an effect on privacy-related concerns.

Privacy perception of obligatory disclosure

Disclosure of personal information online will raise privacy concerns with Internet users as they are exposed to privacy risks (Choo, 2011). However, from the findings, obligatory disclosure was perceived as safe and not a risky phenomenon by most public employees. The lack of privacy awareness and privacy concern, particularly towards obligatory disclosure, was suggested to shape the employees’ perception. Lack of privacy awareness was suggested by the perception of a high sense of security among participants. Apart from that, participants may not have experienced any serious privacy violations caused by obligatory disclosure, where this experience may also influence privacy concerns of participants (Bansal et al., 2010). In fact, at the time of interview, few external incidents that may raise privacy concerns had occurred, for example: the launching of Malaysian Google Street View (Kamal, 2014) and the celebrity iCloud hack (Bloomberg, 2014). Neither issue was highlighted by participants to any significant degree, although Google Street View was mentioned by one participant; however this participant was unaware of the privacy implications from obligatory disclosure.

Culture was identified as a major factor that influences participants. Most of the participants saw cultural norms and practices of organisations as a push-factor for accepting obligatory disclosure. Organisational culture is suggested to guide the employees' perception and actions (Stahl & Elbeltagi, 2004). A global study by Bellman et al. (2004) found that cultural differences largely determine individuals' privacy concerns. Despite having neighbouring geographical areas, different countries showed different levels of privacy concern (Bellman et al., 2004; Milberg et al., 2000). According to Hofstede (2001), Malaysia is categorised as a collectivism country where it is suggested that Malaysians have low privacy concern as this is influenced by national cultural dimensions. Furthermore, collectivist culture is suggested to be more encouraging in disclosing personal information.

Findings also revealed that trust influences employees' privacy concerns. This study supports findings in e-commerce literature that trustworthiness is an important factor in mitigating users' privacy concern (Yousafzai et al., 2009). A high level of trust was noticeable among participants. Trust was suggested to influence users to a higher degree of self-disclosure (Beldad et al., 2011; Christofides et al., 2009). In this context, the study appears to indicate that trust in organisations influences users' willingness for publication of their personal information on an organisation's website. Individuals are more willing to be disclosed in obligatory disclosure when they have a higher trust in their organisation.

In an e-Government environment, trust in government leads to trust to government websites (Teo et al., 2009). Furthermore, as the sample of the current study is from an

Asian country, a high level of trust was observed, consistent with the findings from Hsu (2006).

Research has found that explicit communication of privacy policy or privacy statements can increase trust and alleviate privacy concerns (Andrade et al., 2002; Eastlick et al., 2006). A previous study discovered that online privacy statements on government websites have a positive influence on e-Government's users' trust (Beldad et al., 2012). However, in the current study, privacy statements and privacy policy on government websites were not found to have an influence on participants' trust. No supporting statement could be seen that this feature assisted in influencing the trust of employees. None of the participants made reference to the feature and it could be possible that participants are not bothered with privacy policy or statements. As found in OSN research, the majority of OSN users did not read the privacy policy (Jones & Soltren, 2005; O'Bien & Torres, 2012). OSN users cited 'not interested' and 'too long' as reasons for not reading the privacy policy (O'Bien & Torres, 2012).

As employees of an organisation, moreover a government organisation, findings show that participants have difficulties in disassociating themselves from their role as an employee. This suggests a high relationship factor that influence participants when discussing obligatory disclosure. In the context of an employment relationship, the influence is evident where employees associate the objectives of the organisation in their willingness for obligatory disclosure. Previous studies in e-commerce discovered that establishing a relationship with online organisations influences users' personal information disclosure (Olivero & Lunt, 2004; Norberg et al., 2007), and this argument was supported and extended to employment relationships by the current study.

Contextual integrity

As discovered by participants' data, the employees were found to demonstrate high privacy concerns and privacy awareness of their personal information when they participate in OSN sites. When discussing social media, higher privacy concern was shown by participants compared to obligatory disclosure. However, the similar concern was noticeably absent when the online platform was changed from social to professional. Privacy boundaries move dynamically as the context changes (Altman, 1975; Petronio, 2002). This suggest that changes from social to professional spheres had a significant impact towards employees' privacy concern and awareness. The findings are in line with the highly contextual nature of privacy (Li et al., 2010; Malhotra et al., 2004).

According to Nissenbaum (2004), the type and nature of information about individuals which is governed by context-specific norms is influenced by the decision of participants to see it as acceptable and thus expected to be revealed. Nissenbaum argues that it is the particular context that makes information privacy sensitive, instead of types of information. Findings from this study supports Nissenbaum's argument in the sense that the same types of information (e.g. employment information, personal attributes etc.) were considered sensitive by participants on social media, and were protected or anonymised, but were deemed acceptable when they appear on their organisation's website.

This contextual integrity involves respecting the norms of distribution and norms of appropriateness that are applicable to particular contexts. When these norms are violated, privacy invasions occurred (Nissenbaum, 2004). As obligatory disclosure is expected, and even demanded, by some participants, disclosure of personal information is deemed appropriate to be disclosed. Information flow from government websites was seen in the context of facilitating e-Government, intended for the public in order to achieve efficient government service delivery. When the norms of appropriateness are violated, either by publishing unnecessary information or listing irrelevant individuals, employees' privacy is breached. Employees reiterated that obligatory disclosure information is intended for professional purposes. If information is not used as expected, the norms of appropriateness are violated.

Employees were found to implement various strategies in protecting their personal information in OSN. This could be due to the element of control and ownership that is accorded to participants in OSN, while in obligatory disclosure less control was granted to employees. Furthermore, it is also possible that reported cases of fraud from the media could influence participants to believe that cyber-crimes are caused by social media. Even one participant, who had been a victim of information abuse (regarding working position) on Facebook, did not perceive obligatory disclosure as invading employees' privacy. This indicates that strong influence in contextual integrity in the context of employees' privacy.

Individuals' privacy management

Communication Privacy Management (CPM) theory addresses individuals' privacy management in relation to information boundary permeability, linkage and ownership (Petronio, 2002). Individuals manage the information boundary coordination between disclosure and privacy with a set of rules based on risk-benefit calculations to decide what information can be disclosed. In public personal information disclosure, employees construct boundaries by limiting types of personal information that they are willing to be published. Many participants, in an effort to protect their privacy, mentioned only certain information that they may allow to be shared on the website. They tend to use the withholding strategy to protect their privacy when there is a perceived risk involved. Therefore, an information boundary is created when employees filter what information to disclose (Petronio, 1991).

The CPM theory posits that information may flow across boundaries when it is perceived to have a lower risk and will lead to lower privacy concerns (Petronio, 2002). Employees that had the opportunity to control the flow of information, employed effective strategies to protect their privacy. It was observed that participants resort to filtering their personal information to control the flow of information. Nevertheless, most employees have limited control of their personal information in obligatory disclosure. Organisations were found to have major control of how and when information about employees can be disclosed.

In support of the theoretical perspective, this study discovered boundary turbulence resulting from obligatory disclosure. Boundary turbulence refers to situations when the co-owners of information do not effectively negotiate agreeable privacy rules (Petronio, 2002). The co-ownership of personal information happens when information is shared to other parties and co-owners need to mutually agree the third-party dissemination. From the findings, lack of employees' engagement on obligatory disclosure was observed. Employees' statements suggested minimum consent and consultation were sought by the organisation. The process of handling employees' personal information for website publication was not made transparent to them. This indicates that privacy rules were not negotiated mutually. It further suggests that the employees lack the power to negotiate in the boundary process, hence limiting the degree of boundary turbulence (Allen et al., 2007). This could possibly be the reason why employees showed low resistance for obligatory disclosure.

In CPM theory, one of the primary principles is that people believe that they own their information. During the interview, the disagreements regarding the ownership of personal information were noticeable when some participants viewed that the personal information disclosed belongs to the organisation. Employees that perceived that organisations own the information were showing less concern in managing obligatory disclosure information. Therefore, when individuals did not see the ownership of information, their privacy concern is reduced.

The results of this study extend the understanding of CPM in obligatory disclosure. This study found little employee resistance for obligatory disclosure. Possible reasons for this is that employees faced an organisational culture that is reinforced to them, and less ownership expectations regarding obligatory disclosure.

Informational disclosure decisions

This study suggests the presence of privacy calculus (Dinev & Hart, 2006) in obligatory disclosure. In deciding whether to disclose personal information, an individual makes certain calculations for a privacy trade-off. The study demonstrates that perceived benefits from the disclosure of personal information can be categorised into two. Firstly, the benefit towards the organisation, and secondly the benefit towards the employees themselves. As public employees, most reflected that the benefit to the organisation is a primary consideration which will result in benefit to the country/government. Furthermore, personal benefits to employees, although stated, were overshadowed by the benefits for the organisation. Despite being aware of the risks involved, employees were willing to experience some loss of privacy to meet the organisation’s goals. Although participants mentioned receiving spam emails, unsolicited telephone calls, letters and faxes, they did not see this as a major issue. Despite the emotions caused by obligatory disclosure, participants still hinted at tolerating obligatory disclosure.

However, taking into account the bounded rationality arguments (Smith et al., 2011; Acquisti et al., 2015), the decision made by employees may be limited by knowledge. This is apparent with the lack of privacy concern and awareness that was shown regarding obligatory disclosure. Findings indicate that employees care for their privacy less than they should. As a consequence, employees' decisions are not based on a rational process but instead depend on their current knowledge.

Privacy concern

Privacy concern varies between online contexts. Internet users are exposed to a multitude of privacy risks due to personal information disclosure. In obligatory disclosure, several information privacy concerns were identified by the employees. This study found that most employees are concerned with the disclosure of personal information to outsiders, error, unauthorised secondary use and misuse of personal information. This dimension of privacy concern was suggested by Smith et al. (1996) and Dinev and Hart (2004a). Employees concerns were mostly the result of the nature of public disclosure of information.

Disclosing information publicly exposed 'Internet users' to risk of abuse and misuse of personal information (Dinev & Hart, 2004a). Employees believed that the potential for the misuse of information is considerable, as long as their information is published on the websites. In addition, personal information may be collected and used for unintended purposes to achieve a completely different aim than that which was originally intended (Culnan, 1993). Public availability of personal information was found to trigger employees' privacy concerns. Employees demonstrated uncertainty of their personal information towards invisible audience. As one participant likened himself to being 'exposed', this highlights the privacy concerns due to unintended audience. Unintended audience in the OSN environment was found to lead to misinterpretation of information when details are taken out of context (Wang et al., 2011) while in obligatory disclosure, participants are concerned about being monitored and the availability of personal information on the Internet (Dinev & Hart, 2004a). The accuracy of published personal information was also a concern for employees. Concern regarding errors refers to inadequate protection against deliberate and accidental error within personal information

(Smith et al., 1996). In obligatory disclosure, employees were more concerned with the inefficiency of measures to prevent errors in publishing employees' personal information.

In addition, participant concerns were also directed to possible intrusion into offline territory. Offline threats to personal safety were observed due to the ability of employees to be located. The impact of these associations between online disclosure and offline concerns subsequently resulted in higher privacy vulnerability for employees.

Privacy by design

As employees indicated that they have limited control over information disclosure on organisation websites, they brought forward the idea of minimising personal information disclosure. An organisation's approach to privacy may assist in ensuring preserving employees' privacy. The concept of privacy by design can be applied to obligatory disclosure from the website design perspectives. A potential area for website developers is to design a website interface that promotes employees' privacy, such as disclosing relevant details of employees, providing identification techniques when receiving public queries, an additional layer for public viewing and a dynamic disclosure design.

The basis of the privacy-by-design concept is to integrate privacy values at the earliest stage of the design specifications of technology (Cavoukian, 2012). In this research context, the seven principles of privacy by design can be extended to obligatory disclosure: 1) proactive not reactive: disclosure should anticipate and prevent a privacy-invasive attack before it takes place; 2) privacy as the default: organisations should present an explicit commitment to ensuring that maximum degree of privacy is delivered to employees; 3) privacy embedded into design: an organisation's website design and architecture must be embedded with privacy values as an integral component of the core functionality; 4) functionality-positive-sum, not zero-sum: obligatory disclosure should still meet both the organisations' and employees' objectives while at the same time protect employees' privacy; 5) end-to-end lifecycle protection: personal information of employees that will be disclosed on organisations' websites must be protected during the whole process from start to finish; 6) visibility and transparency: the process of obligatory disclosure must be made visible and transparent to all stakeholders (including employees); and 7) respect for users' privacy: usage of employees' personal information should be conducted in a manner that is consistent with respect for the individual’s privacy. Thus, a privacy-friendly obligatory disclosure can be achieved by applying privacy-by-design principles while not impeding delivery of services to the public.

Cognitive dissonance

The present study reveals a possible cognitive dissonance regarding the lack of connections between privacy loss in the personal and obligatory disclosure in the professional lives of government employees in Malaysia. As presented in the findings, higher concerns of privacy were shown under social circumstances as compared to professional circumstances. Loss of privacy under the social context was articulated well by employees. However, it is different when discussing obligatory disclosure. Participants in this study attempted to minimise the dissonance through higher trust to organisation and their roles as civil servants. More specifically, they may perceive it as unethical to challenge their own work ethics. This provides insight into the social psychological impact of obligatory disclosure in organisations with a high degree of trust and service ethos and may be particularly relevant within the specific cultural context.

This understanding can guide future policies so that governments/organisations can take responsibility and exercise a duty of care to educate and inform employees, who may be targeted in their personal lives through obligatory disclosure in their professional lives.

CHAPTER 8

Conclusion

8.1 Introduction

This chapter draws conclusions from the study, and presents a summary of the studies conducted as well as of the main contributions. It concludes with an assessment of the limitations and recommendations as well as providing suggestions for future research.

The main research question asks: ‘How would public employees describe organisational disclosure towards their privacy?’, and seeks to uncover and increase understanding regarding what is considered as a normal online phenomenon.

This research focuses on the disclosure of personal information through organisation websites from a public administration perspective. A conceptual framework introduced as ‘obligatory disclosure’ was developed for analysing the phenomenon of interest. Obligatory disclosure is defined as: *‘any information about an individual that is shared via any form of communication by an organisation (of which they are employee or member)’* which fitted well with the research interest. This conceptual framework brought together three main concepts which are privacy, the relationship between individual-organisation and e-Government for further investigation in the rest of this thesis.

The research question was examined through an interpretivist paradigm, through a single case embedded design approach. A web content analysis and in-depth semi-structured interview were employed to make sense of obligatory disclosure from the perspective of employees.

8.2 Significant research findings

This study introduced obligatory disclosure as a concept for disclosure of employees' personal information by organisations. The result of the thesis should be interpreted in the Malaysian context and within a particular time frame.

As presented in chapter six, the findings are as highlighted below:

1. There is low privacy concern and lack of privacy awareness among employees regarding obligatory disclosure.
2. Employees' privacy concern is influenced by specific context.
3. Obligatory disclosure impacts employees' privacy and productivity.
4. Obligatory disclosure leads to higher privacy vulnerabilities for employees.
5. Civil servants' organisational commitments reduce employees' privacy concerns.
6. Lack of emphasis on employees' privacy in public organisations results in unreasonable amounts of personal information disclosure.

While the practice of obligatory disclosure was seen as a normal practice, findings reveal that it violates an employee's privacy. Employees' privacy concerns are influenced by the context of disclosure, although the disclosure occurred within the same online environment i.e. the Internet and the same type of personal information. The potential benefits of obligatory disclosure influence an employee's willingness to disclosing their personal information, thus outweighing the risks. Though there are few employees who saw the practice as invading their privacy, they found it difficult to address their privacy concerns. Hence, a mechanism for a privacy-friendly disclosure design may be an effective measure in protecting employees' privacy.

8.3 Contributions of research

This thesis makes several contributions to knowledge. Firstly, it enhances understanding of a less-researched area of privacy, regarding the disclosure of personal information, i.e.

third-party disclosure. A clearer conceptual framework is introduced to contextually define the phenomenon. Privacy issues that result from disclosure that is not based on the individuals' choice were presented. Secondly, the findings extend knowledge of the contextual nature of privacy in a situation-specific environment. It indicates that context plays an influential role in individuals' privacy decisions in support of the contextual integrity theory (Nissenbaum, 2004). Thirdly, this thesis provides insights on individual's privacy management decisions that resulted from disclosure by other parties. The Communication Privacy Management (CPM) theory can be extended to investigate the tension between information disclosure and privacy (Petronio, 2002) in obligatory disclosure. Finally, this thesis contributes to the understanding of privacy by providing insights into considering a 'privacy-by-design' approach to organisation websites. This approach includes the idea that the obligatory disclosure should be designed and constructed in a way to minimise the amount of personal information disclosure.

This thesis has a practical contribution for organisations (e.g. Government) and website developers. The results showed that employees - who are an important element in an organisation - are experiencing privacy implications caused by obligatory disclosure. Organisations should take proactive steps to protect their important assets (employees). Formulating policy or guidelines that consider employees' privacy could assist in protecting employees as well as the organisation. In addition, engaging employees regarding the publication of their personal information should be encouraged. The findings also provide web designers with a possible direction for website (obligatory) disclosure design. The findings can assist designers of organisations' websites to minimise privacy implications and at the same time maintain the service provided.

For the methodological contribution, this research contributes to an under-explored method for examining personal information through an organisation's website. A case study involving web content analysis, documentation and in-depth semi-structured interviews was employed for this research. This research has developed a taxonomy of personal information that can be found within a single type of website (e.g. Government) by employing web content analysis. In addition, to evaluate the the disclosure on websites, the coded attributes can be adapted according to the actual disclosure or objective of the study. Thus, it offers a flexibile framework for replicating this type of research as presented in section 5.1.1. As far as this research is concerned, a systematic web content analysis technique was never employed for extracting personal information from websites. By employing web content analysis, a true picture of the extent of disclosure was acquired. Combining techniques of data collection has proved useful in examining the actual personal information that was disclosed, and what was perceived by the participants. This method can be replicated in other organisational settings or countries, or even extended with additional factors.

This study contributes to a better understanding of personal information disclosure through e-Government websites. It identifies and classifies different types of personal information disclosed in e-Government websites. The findings are tabulated as a taxonomy of personal information in section 5.1.2.

8.4 Revisiting research questions

This section briefly summarises the findings of the research in terms of each research question.

Main research question: How would public employees describe organisational disclosure and its relation to their privacy?

Obligatory disclosure was perceived as a channel of an e-Government initiative to improve public service delivery. As public employees, they focused on their role to ensure they achieved the organisation's objectives. Therefore, the context of disclosure plays an important role in disclosure decisions.

Further investigations reveal that public employees experience privacy threats and privacy violations due to obligatory disclosure. There was also a concern voiced by many participants that unnecessary disclosure and the irrelevancy of disclosure could violate their privacy and make them vulnerable. Though a few employees perceive obligatory disclosure as invading their privacy, most of the employees were willing to surrender some of their privacy to meet the organisation's objective. To them, their professionalism in public service and the benefits of obligatory disclosure to organisations exceeded the necessity of their personal privacy.

How does obligatory disclosure result in the disclosure of employees' personal information?
Sub question: What personal information of employees', if any, is publicly available on organisational websites?

Web content analysis raises an important issue related to privacy, which is the extensive disclosure of identifiable personal information. Organisation websites reveal six categories of personal information. In the pretext of promoting transparency and efficient delivery of services, up to 23 different types of personal information about employees are disclosed publicly on websites. The information ranges from personal attributes such as full name and photographic images to timeliness information (i.e. information regarding any event or activities to a specific time). A taxonomy of personal information of obligatory disclosure was developed and is presented in section 5.1.2. Disclosure of personal information largely originated from specific features of the websites - such as staff directory, organisation chart, announcement and information about an organisation's events or activities.

What does obligatory disclosure mean to employees?

To answer this research question, it is important for participants not to have any preconceived ideas about privacy that could possibly influence their answers. Therefore, this question was asked early in the research so as to capture their first perceptions on the issue. Obligatory disclosure generally was considered as safe, commonly practiced, and serving as an official communication channel. It was discovered that high commitment to public service ethos emerged as a major factor for participants, and a high level of organisational trust was evident in the findings. Hence low privacy concerns are observed from the participants regarding the disclosure of their personal information on an organisation's website. In contrast, some participants who believe that obligatory disclosure infringes their privacy was consistent about this belief throughout the interview. These participants are able to highlight privacy risks and violations as a result of obligatory disclosure.

How do employees perceive the issue of privacy with regard to obligatory disclosure?

In spite of employees showing high information privacy concern towards their personal information on the Internet and social media (e.g. Facebook), analysis identifies low privacy concerns and a lack of privacy awareness with respect to obligatory disclosure. This is possibly due to the contextual nature of privacy, in which an organisation's website's obligatory disclosure was seen as an official communication channel and the disclosure was considered appropriate and safe. This implies that the context of information disclosure plays an important role towards an individual's privacy as the individual's expectation varies according to specific contexts. Eventually, some employees perceive obligatory disclosure as disclosing unnecessary and irrelevant information, and are therefore vulnerable. For employees that have some IT or computer background, there is some evidence to suggest that these employees demonstrate higher privacy concerns compared to other employees.

How does obligatory disclosure impact employees' privacy, if any?

This research identifies key characteristics of obligatory disclosure: contactable, locatable, identifiable, searchable, accurate, verifiable and discoverable. These characteristics play a central role in providing an environment that increases employees' vulnerability due to the revelation of 'truthful' personal information on the Internet. Disclosing excessive employee's information and irrelevant disclosure are suggested as the privacy violation in obligatory disclosure, which could lead to various privacy attacks and privacy risks online or in the real world. Furthermore, a lack of emphasis on employees' privacy - such as a policy or guideline to protect employees' information, low employees' participation in the process of obligatory disclosure and limited regulatory protection - adds to the mounting risks to employees.

Sub question: What are the concerns of employees, if any, when their personal information is published on their organisation's website?

The issue of privacy came to light for most participants when they were questioned on the concept of personal information, privacy and social media. Participants seemed uncomfortable with having their personal information published on the organisation's website after experiencing it for some time. Indeed, most participants experienced privacy violations, although they were not initially aware of this, and many were concerned with privacy threats that were associated with the disclosure. In addition, besides concern over information privacy, concern towards personal safety was evident. As a result, risk towards the safety of employees and lower productivity are reported.

8.5 Recommendations

This study finds that the issue of employees' privacy was neglected and does not play an important role in the implementation of e-Government via an organisation's website. Participants generally expressed what they thought could be improved towards better disclosure.

Therefore, this study recommends:

The need for a regulatory approach to protect employees' information.

Public organisations (in this case the Government) should take necessary steps, via a regulatory approach, to protect the personal information of employees published on the organisation's website. This recommendation is made in light of the findings where information on a public organisation's website currently is not covered by any legislation.

A standard policy on obligatory disclosure with emphasis on the protection of employees' privacy.

A clear and standard policy (albeit internal) to define the development and implementation of obligatory disclosure is of paramount importance. This policy should incorporate the essence of privacy and personal information whilst not foregoing the organisation's objectives. This was made clear by participants in which they suggested developing a disclosure policy or checklist for those responsible for managing the disclosure. Higher participation of employees and greater transparency towards employees must be put into consideration when enacting the policy.

Continuous employees' education, training and awareness programmes on the issue of privacy and personal information in the context of public administration.

Participants raised concern over the knowledge and awareness of the web administrator. They reiterated that government employees who were responsible for the website, i.e. website administrator, should be more cautious prior to publishing personal information on the official website. This is to avoid publication of 'high value' personal information online which could be misused by interested parties and poses a greater risk to employees.

Privacy-friendly obligatory disclosure website design

Public organisations must look into re-designing their websites to incorporate elements of privacy. While this research is focusing on obligatory disclosure, the process of designing shouldn't be limited to obligatory disclosure. This concept is known as 'privacy by design' where it considers human values in the whole process of design stages (Cavoukian, 2012).

Various technical implementations are suggested by participants, for example developing an in-house portal for staff, creating a password or login for the public, as an access authorisation technique, standardised directories, and publishing documents or files in image format in order to make it difficult for a search engine to capture. In addition to these, other suggested implementations include the limiting of individual name appearances on the website during office hours only and configuring email addresses so that they cannot be copied easily and therefore to avoid email-blasting. The data presented above indicates that the participants would prefer minimisation of personal information disclosure in order to improve obligatory disclosure.

Privacy-embedded customer service delivery

Participants suggested methods to reduce the disclosure of employees' information, particularly in relation to the staff directories. Centralised customer service, e.g. via a Public Relation Officer (PRO) or dedicated staff, are among the most suggested techniques. Meanwhile, one participant suggests that only one main telephone number should be published on the website. These suggestions clearly present a strategy to limit personal information on the website. Instead of having a directory which displays employees' information, only one or two employees would be responsible for public queries from the website. Participants believed that it is the 'service' from the organisation that the public really need. As long as the service is delivered accordingly, the identity of employees who performed the service is secondary.

Therefore, this research suggests a new approach of customer service delivery. By implementing privacy-embedded customer service delivery, it could ensure that employees' privacy risks are minimised and at the same time provide efficient service to the citizens.

8.6 Limitations

This study has a number of limitations. Firstly, the sample for both government websites and participants is small and limited to a single country. A larger sample could have provided more data and richer findings. The sample of participants is very small and geographically limited to a single location, which was the administrative capital of Malaysia. In addition, a large number of participants are represented in two of the three working group categories. However, since maximum variation technique was implemented during the sampling, the findings may be able to be generalised with caution.

Although samples of government websites are small, and selecting top rank websites may present a view of the quality of a public organisation's website, it may not be representative of all government agency websites in Malaysia. Despite the sample of government websites being limited to a single country, the pilot study discovered that obligatory disclosure was found to be practiced in other countries as reported in the pilot study.

However, caution must be exercised in trying to generalise the findings. While this research attempts to provide realistic settings (i.e. workplace), it is possible that the settings create a higher contextual element of an organisation. It is possible that this environment may have given participants a greater association with their employers.

8.7 Future research

Given the research findings that are presented, it is apparent that there is need for further research into personal privacy caused by third-party disclosure, from multiple perspectives and approaches. This study provides a starting point to start addressing privacy challenges in relation to obligatory disclosure.

The focus of this study is at the individual level of organisation, i.e. employees. Future research could explore across different levels within organisations or inter-organisations. For example, within organisations there are various groups that employees can be affiliated with. Different groups can have a different set of privacy perceptions (Bélanger & Crossler, 2011). Another perspective is the possibility of the influence of a particular group's members that may influence the whole group's privacy concerns. In addition, the relationship between an individuals' role in the organisation and privacy concerns is another suggestion for future research.

Another valuable area is to gain understanding on how organisations take into consideration their employees' privacy concerns in their online offerings. The findings show a lack of employee's engagement in obligatory disclosure. Future studies could consider investigating and linking the organisational environment and employee engagement with privacy concerns.

Future research might also investigate further the factors that influence individuals and which factors affect employees most. Cross-cultural comparisons can be considered since culture is identified as a significant factor in obligatory disclosure.

The contextual nature of privacy may be investigated by exploring individuals' perception of their professional information on a specific professional OSN and an organisation's website. By focusing on certain types of information published in different contexts but in professional publication, a better understanding of privacy concerns or violations under different contexts can be acquired.

As this research is employing an interpretive paradigm, it would be interesting for this research to be conducted in other paradigms with other methods of data collection. The selection of participants can be widened to include more employees in various categories of organisations. Henceforth, findings can be generalisable for the whole population.

8.8 Final remarks

To conclude, this thesis focuses on a complex and multi-faceted topic which is privacy, in a situation-specific environment. More specifically, it attempts to uncover privacy issues concerning the practice of obligatory disclosure from the perspectives of individuals within the organisation itself. It provides an investigation into the relationship between obligatory disclosure on government websites and what it means to employees concerning their privacy.

This thesis raises a number of issues that need to be addressed in order to preserve an individuals' privacy caused by obligatory disclosure. On the one hand, the practice of obligatory disclosure offers benefits to employees, employers and organisations. On the other hand, such benefits come with privacy risks. This implies that a delicate balance in meeting the organisation's goals and preserving employees' privacy needs to be addressed. Furthermore, the publication of employees' information calls for a *privacy by design* approach. The findings of this thesis provide a practical opportunity for web designers to consider online privacy and take it into account. A mechanism for a dynamic privacy-friendly disclosure design may be an effective measure in protecting employees' privacy. In addition, this thesis provides an invaluable insight for those involved in the formulation of policy in organisations. As has been revealed by this research, a fresh direction in formulating policies in relation to obligatory disclosure is needed. Rather than over-focusing to the users/customers, the policy should also incorporate the employees, moreover when the risk was also shown to affect organisations.

The findings of this research could serve as a starting point of inquiry into obligatory disclosure. While obligatory disclosure was assumed as a normal phenomenon, findings revealed that it violated employees' privacy. The issues of privacy on the Internet will continue to become more evident in our lives and is one of the most pressing issues at this time (Belanger & Xu, 2015). Thus, the 'high value' of an individual's personal information should be seriously reconsidered before deploying it on to the Internet for publication.

References

Abel, F., Henze, N., Herder, E. & Krause, D., 2010. Interweaving Public User Profiles on the Web. In P. De Bra, A. Kobsa, & D. Chin, eds. *User Modeling, Adaptation, and Personalization: 18th International Conference, UMAP 2010, Big Island, HI, USA, June 20-24, 2010. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 16–27.

Ackerman, M.S., Cranor, L.F. & Reagle, J., 1999. Privacy in E-commerce: Examining User Scenarios and Privacy Preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce*. ACM, New York, pp. 1–8.

Ackerman, M.S. & Mainwaring, S.D., 2005. Privacy Issues and Human-Computer Interaction. In S. L. Garfinkel & L. F. Cranor, eds. *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly, pp. 381–400.

Acquisti, A., 2004. Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce - EC '04*, ACM, New York, p.21-29.

Acquisti, A., Brandimarte, L. & Loewenstein, G., 2015. Privacy and human behavior in the age of information. *Science*, 347(6221), pp.509–514.

Acquisti, A. & Gross, R., 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In G. Danezis & P. Golle, eds. *Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 36–58.

Acquisti, A. & Gross, R., 2009. Predicting Social Security numbers from public data. In *Proceedings of the National Academy of Sciences of the United States of America*. pp. 10975–10980.

Acquisti, A. & Grossklags, J., 2005. Privacy and rationality in individual decision making. *IEEE Computer Society*, 3(1), pp.26–33.

Agee, J., 2009. Developing qualitative research questions: a reflective process. *International Journal of Qualitative Studies in Education*, 22(4), pp.431–447.

Aguiton, C., Cardon, D., Castelain, A., Fremaux, P., Girard, H., Granjon F., Nepote, C., Smoreda, Z., Trupia, D. & Ziemlicki, C., 2009. Does Showing Off Help to Make Friends? Experimenting a Sociological Game on Self-Exhibition and Social Networks. In *Third International AAAI Conference on Weblogs and Social Media.* pp. 10–17. Available at: http://www.aaai.org/ocs/index.php/ICWSM/09/paper/view/178 [Accessed 10 July 2015].

Aimeur, E., Brassard, G. & Molins, P., 2012. Reconstructing Profiles from Information Disseminated on the Internet. In *2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2012 ASE/IEEE International Conference on Social Computing (SocialCom).* Amsterdam: IEEE, pp. 875–883.

Aïmeur, E. & Lafond, M., 2013. The Scourge of Internet Personal Data Collection. In *2013 International Conference on Availability, Reliability and Security*. IEEE, pp. 821–828.

Ajzen, I. & Fishbein, M., 1977. Attitude–Behavior Relations: A Theoretical Analysis and Review of Empirical Research. *Psychological Bulletin*, 84(5), pp.888–918.

Alcaide-Muñoz, L. & Rodríguez Bolívar, M.P., 2015. Understanding e-government research. *Internet Research*, 25(4), pp.633–673.

Allen, A.L., 1988. *Uneasy Access: Privacy for Women in a Free Society*, New Jersey, USA: Rowman & Littlefield.

Allen, M., Coopman, S., Hart, J. & Walker, K., 2007. Workplace Surveillance and Managing Privacy Boundaries. *Management Communication Quarterly*, 21(2), pp.172–200.

Allen, M., 2006. Social engineering: A Means to Violate a Computer System. *SANS Institute, InfoSec Reading Room*. Available at: http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529 [Accessed 18 January 2014].

Altman, I., 1977. Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, 33(3), pp.66–84.

Altman, I., 1975. *The Environment and Social Behaviour: Privacy, Personal Space, Territory, and Crowding*, Monterey, CA: Brooks/Cole Publishing.

Andrade, E.B., Kaltcheva, V. & Weitz, B., 2002. Self-Disclosure on the Web: the Impact of Privacy Policy, Reward, and Company Reputation. *Advances in Consumer Research*, 29, pp.350–353.

Anonymous, 2000. A Survey of Government and the Internet-Handle with Care: E-government is mostly a good thing, but it need watching. *The Economist*, pp.33–34. Available at: http://www.economist.com/displayStory.cfm?Story_ID=80866. [Accessed July 8, 2013].

Arksey, H. & Knight, P.T., 1999. *Interviewing for social scientists*, London: Sage Publications Ltd.

Asia Pacific Economic Cooperation Secretariat, 2005. *Apec Privacy Framework*, Singapore.

Babbie, E., 2010. *The Practice of Social Research* 12th Edition, Belmont, CA: Wadsworth Cengage Learning.

Badrul, N.A., Williams, S.A. & Lundqvist, K.O., 2014. Organisational Disclosure: Threats to Individual's Privacy? In *5th International Conference on Science & Technology: Applications in Industry & Education (ICSTIE)*. Penang, Malaysia, pp. 321–325.

Baker, D.L., 2009. Advancing E-Government performance in the United States through enhanced usability benchmarks. *Government Information Quarterly*, 26(1), pp.82–88.

Balakrishnan, V. & Shamim, A., 2013. Malaysian Facebookers: Motives and addictive behaviours unraveled. *Computers in Human Behavior*, 29(4), pp.1342–1349.

Baloglu, S. & Pekcan, Y. a., 2006. The website design and Internet site marketing practices of upscale and luxury hotels in Turkey. *Tourism Management*, 27(1), pp.171–176.

Bannister, F. & Connolly, R., 2011. The Trouble with Transparency: A Critical View of Openness in e-Government. *Policy & Internet*, 3(1), pp.158–187.

Bansal, G., Zahedi, F. "Mariam" & Gefen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), pp.138–150.

Barnes, B.B., 2006. A privacy paradox: Social networking in the United States. *First Monday*, 11(9), pp.1–10. Available at: http://firstmonday.org/article/view/1394/1312. [Accessed 18 July 2013].

Basu, A., 2003. Context-driven assessment of commercial Web sites. In *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. Hawaii: IEEE, pp.8–pp.

Bauer, C. & Scharl, A., 2000. Quantitive evaluation of Web site content and structure. *Internet Research*, 10(1), pp.31–44.

Baxter, P. & Jack, S., 2008. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, 13(4), pp.544–559.

Beattie, V., McInnes, B. & Fearnley, S., 2004. A methodology for analysing and evaluating narratives in annual reports: a comprehensive descriptive profile and metrics for disclosure quality attributes. *Accounting Forum*, 28(3), pp.205–236.

Bélanger, F. & Carter, L., 2008. Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2), pp.165–176.

Bélanger, F. & Crossler, R., 2011. Privacy in the digital age: a review of information privacy research in information systems. *Mis Quarterly*, 35(4), pp.1017–1041.

Belanger, F. & Hiller, J.S., 2006. A framework for e-government: privacy implications. *Business Process Management Journal*, 12(1), pp.48–60.

Bélanger, F. & Xu, H., 2015. The role of information systems research in shaping the future of information privacy. *Information Systems Journal*, 25(6), pp.573–578.

Beldad, A., van der Geest, T., de Jong, M. & Steehouder, M., 2012. A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Government Information Quarterly*, 29(1), pp.41–49.

Beldad, A., de Jong, M. & Steehouder, M., 2011. A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet. *The Information Society*, 27(4), pp.220–232.

Beldad, A.D. & Koehorst, R., 2015. It's Not About the Risks, I'm just Used to Doing It: Disclosure of Personal Information on Facebook Among Adolescent Dutch Users. In G. Meiselwitz, ed. *Social Computing and Social Media: 7th International Conference, SCSM 2015, Held as Part of HCI International 2015, Los Angeles, CA,* *USA, August 2-7, 2015, Proceedings*. Cham: Springer International Publishing, pp. 185–195.

Bellman, S., Johnson, E.J., Kobrin, S.J. & Lohse, G.L., 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5), pp.313–324.

Benbasat, I., Goldstein, D.K. & Mead, M., 1987. The Case Research Strategy in Studies of Information Systems Case Research. *MIS quarterly*, 3(3), pp.369–386.

Bernama, 2015. 1.6 juta pegawai perkhidmatan awam sehingga 2014. *Kosmo! Online*. Available at: http://www.kosmo.com.my/kosmo/content.asp?y=2015&dt=0312&pub=Kosmo&sec=Terkini&pg=bt_15.htm [Accessed 17 March 2016].

Bertot, J.C., Jaeger, P.T. & Grimes, J.M., 2010. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, 27(3), pp.264–271.

Besmer, A. & Lipford, H.R., 2010. Moving Beyond Untagging: Photo Privacy in a Tagged World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Atalanta: ACM, pp. 1563–1572.

BeVier, L.R., 1995. Information about individuals in the hands of government: Some reflections on mechanisms for privacy protection. *William and Mary Bill of Rights Journal*, 4, pp.455–504.

Bloomberg, 2014. Nudie pictures probe: Apple report ICloud was hacked. *Malay Mail Online*. Available at: http://www.themalaymailonline.com/world/article/nudie-pic-probe-apple-report-icloud-was-hacked [Accessed 11 May 2015].

Bogdanovic, D., Dowd, M., Wattam, E. & Adam A., 2012. Contesting methodologies: Evaluating focus group and privacy diary methods in a study of on-line privacy. *Journal of Information, Communication and Ethics in Society*, 10(4), pp.208–221.

Botosan, C.A., 1997. Disclosure Level and the Cost of Equity Capital. *The Accounting Review*, 72(3), pp.323–349.

Boyatzis, R., 1998. *Transforming qualitative information: Thematic analysis and code development*, Thousand Oaks, California: Sage Publications Inc.

boyd, D. & Eszter, H., 2010. Facebook privacy settings: Who cares? *First Monday*, 15(8). Available at: http://firstmonday.org/article/view/3086/2589 [Accessed 17 February 2015].

boyd, D. & Heer, J., 2006. Profiles as Conversation: Networked Identity Performance on Friendster. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*. Los Alamitos, CA: IEEE, p.59–69.

boyd, D.M., 2004. Friendster and publicly articulated social networking. In *Conference on Human factors and Computing Systems (CHI 2004)*. Vienna: ACM, pp. 1279–1282.

boyd, D.M. & Ellison, N.B., 2007. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), pp.210–230.

Braun, V. & Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), pp.77–101.

Braun, V., Clarke, V. & Terry, G., 2014. Thematic Analysis. In P. Rohlender & A. C. Lyons, eds. *Qualitative Research in Clinical and Health Psychology*. Palgrave Macmillan, pp. 95–113.

Brody, R.G., Brizee, W.B. & Cano, L., 2012. Flying under the radar: social engineering. *International Journal of Accounting and Information Management*, 20(4), pp.335–347.

Brown, M. & Muchira, R., 2004. Investigating the Relationship between Internet Privacy Concerns and Online Purchase Behavior. *Journal of Electronic Commerce Research*, 5(1), pp.62–70.

Bruns, A., 2013. From Homepages to Network Profiles: Balancing Personal and Social Identity. In J. Hartley, J. Burgess, & A. Bruns, eds. *A Companion to New Media Dynamics*. Oxford, UK: Wiley-Blackwell, pp. 417–428.

Bryman, A., 2012. *Social Research Methods* 4th Edition, New York: Oxford University Press.

Buchanan, T., Paine, C., Joinson A. & Reips, U., 2007. Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), pp.157–165.

Buenadicha, M., Chamorro, A., Miranda, F. & Gonzalez, O., 2001. A new Web assessment index: Spanish universities analysis. *Internet Research: Electronic Networking Applications and Policy*, 11(3), pp.226–234.

Bujang, Y.R. & Hussin, H., 2013. Should we be concerned with spam emails? A look at its impacts and implications. In *2013 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)*. Rabat: IEEE, pp. 1–6.

Burgoon, J.K., Parrot, R., Le Poire, B., Kelley, D., Walther, J. & Perry, D., 1989. Maintaining and Restoring Privacy through Communication in Different Types of Relationships. *Journal of Social and Personal Relationships*, 6(2), pp.131–158.

Caldwell, T., 2013. Spear-phishing: how to spot and mitigate the menace. *Computer Fraud & Security*, 2013(1), pp.11–16.

Caliendo, M., Michel, C., Dominik, P. & Sabine, S., 2008. *The Cost Impact of Spam Filters: Measuring the Effect of Information System Technologies in Organizations*, IZA Discussion Paper No. 3755.

Carter, L. & Bélanger, F., 2005. The utilization of e-government services: citizen trust, innovation and acceptance. *Information Systems Journal*, 15(1), pp.5–25.

Cavoukian, A., 2012. Privacy by Design. *IEEE Technology and Society*, (Winter 2012), pp.18–19.

Cavoukian, A., 2009. *Privacy by Design: The 7 Foundational Principles*, Ontario, Canada. Available at: https://www.ipc.on.ca/images/resources/7foundational principles.pdf [Accessed July 22, 2016].

Chellappa, R.K. & Sin, R.G., 2005. Personalization versus privacy: An empirical examination of the online consumer’s dilemma. *Information Technology & Management*, 6(2-3), pp.181–202.

Chen, J., Ping, W., Xu, Y. & Tan, B., 2009. Am I afraid of my peers? Understanding the antecedents of information privacy concerns in the online social context. In *Thirtieth International Conference on Information Systems, ICIS*, Paper 174.

Chen, K. & Rea, A.I., 2004. Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems*, 44(4), pp.85–92.

Choo, K.R., 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), pp.719–731.

Christofides, E., Muise, A. & Desmarais, S., 2009. Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior*, 12(3), pp.341–345.

Clarke, R., 1999. Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM*, 42(2), pp.60–67.

Collins, N.L. & Miller, L.C., 1994. Self-disclosure and liking: A meta-analytic review. *Psychological Bulletin*, 116(3), pp.457–475.

Conway, M., 2006. The subjective precision of computers: A methodological comparison with human coding in content analysis. *Journalism & Mass Communication Quarterly*, 83(1), pp.186–200.

Corbett, S., 2013. The retention of personal information online: A call for international regulation of privacy law. *Computer Law & Security Review*, 29(3), pp.246–254.

Corbin, J.M. & Strauss, A.L., 2008. *Basics of qualitative research: Techniques and procedures for developing grounded theory* 3rd Editio., Los Angeles: Sage Publications.

Cozby, P.C., 1973. Self-disclosure: A literature review. *Psychological Bulletin*, 79(2), pp.73–91.

Craik, K.H., 2009. Where Do We Look for Reputation. In *Reputation: A Network Interpretation*. Oxford Scholarship Online, pp. 1–18.

Creswell, J.W., 2007. *Qualitative Inquiry and Research Design* Second Edition, Sage Publications Inc.

Creswell, J.W., 2013a. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* 3rd ed., Thousand Oaks, California: Sage Publications Inc.

Creswell, J.W., 2013b. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* 4th ed., Thousand Oaks, California: Sage Publications Inc.

Creswell, J.W. & Clark, V.L.P., 2007. *Designing and conducting mixed methods research*, Thousand Oaks, California: Sage Publications Inc.

Creswell, J.W. & Miller, D.L., 2000. Determining Validity in Qualitative Inquiry. *Theory Into Practice*, 39(3), pp.124–130.

Crotty, M., 1998. *The foundations of social research: Meaning and perspectives in the research process*, Thousand Oaks: Sage Publications Inc.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A. & Sheikh, A., 2011. The case study approach. *BMC Medical Research Methodology*, 11:100.

Cuillier, D. & Piotrowski, S.J., 2009. Internet information-seeking and its relation to support for access to government records. *Government Information Quarterly*, 26(3), pp.441–449.

Cullen, R., 2009. Culture, identity and information privacy in the age of digital government. *Online Information Review*, 33(3), pp.405–421.

Culnan, M.J., 1993. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS Quarterly*, 17(3), pp.341–363.

Culnan, M.J. & Armstrong, P.K., 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1), pp.104–115.

Darke, P., Shanks, G. & Broadbent, M., 1998. Successfully completing case study research: Combining rigour, relevance and pragmatism. *Information Systems Journal*, 8(4), pp.273–289.

Davison, R.M. & Martinsons, M.G., 2011. Methodological practice and policy for organisationally and socially relevant IS research: an inclusive–exclusive perspective. *Journal of Information Technology*, 26(4), pp.288–293.

Debatin, B., Lovejoy, J., Horn, A. & Hughes, B., 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), pp.83–108.

DeCew, J.W., 1997. *In pursuit of privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press.

Demchak, C.C., Friis, C.S. & La Porte, T.M., 2000. Webbing governance: National differences in constructing the face of public organizations. In G. D. Garson, ed. *Handbook of public information systems*. New York: Marcel Dekker Publishers, pp. 179–196.

Denzin, N.K., 2008. The new paradigm dialogs and qualitative inquiry. *International Journal of Qualitative Studies in Education*, 21(4), pp.315–325.

Denzin, N.K. & Lincoln, Y.S., 2013. The Discipline and Practice of Qualitative Research. In N. K. Denzin & Y. S. Lincoln, eds. *Strategies of Qualitative Inquiry*. Sage Publications Inc, pp. 1–41.

Denzin, N.K. & Lincoln, Y.S., 2005. *The SAGE Handbook of Qualitative Research* Third Edition, Thousand Oaks, California: Sage Publications Inc.

Department of Economic and Social Affairs, 2012. *United Nations E-Government Survey 2012*, New York, USA.

Devos, T., Spini, D. & Schwartz, S.H., 2002. Conflicts among human values and trust in institutions. *The British journal of social psychology / the British Psychological Society*, 41(4), pp.481–494.

Dey, R., Tang, C., Ross, K. & Saxena, N., 2012. Estimating Age Privacy Leakage in Online Social Networks. In *IEEE INFOCOM: Mini- Conference*. IEEE, pp. 3118–3122.

Dey, R., Jelveh, Z. & Ross, K., 2012. Facebook users have become much more private:

A large-scale study. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. Lugano: IEEE, pp. 346–352.

van Dijck, J., 2013. "You have one identity": performing the self on Facebook and LinkedIn. *Media, Culture & Society*, 35, pp.199–215.

Dinev, T., Xu, H., Smith, J. & Hart, P., 2012. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), pp.295–316.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. & Colautti, C., 2006. Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, 15(4), pp.389–402.

Dinev, T. & Hart, P., 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), pp.61–80.

Dinev, T. & Hart, P., 2005. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), pp.7–29.

Dinev, T. & Hart, P., 2004a. Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), pp.413–422.

Dinev, T. & Hart, P., 2004b. Internet privacy, social awareness, and internet technical literacy – An exploratory investigation. In *Proceedings of 17th BledeCommerce Conference, eGlobal*. Bled, Slovania, pp. 1–12.

Duriau, V.J., Reger, R.K. & Pfarrer, M.D., 2007. A Content Analysis of the Content Analysis Literature in Organization Studies: Research Themes, Data Sources, and Methodological Refinements. *Organizational Research Methods*, 10(1), pp.5–34.

Dutta, P. & Bose, S., 2007. Web-based Corporate Reporting in Bangladesh:An Exploratory Study. *The Cost and Management*, 35(6), pp.29–45.

Dwyer, C., Hiltz, S.R. & Passerini, K., 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of the Thirteenth Americas Conference on Information Systems (AMCIS)*. Paper 339.

Dyer, W.G.J. & Wilkins, A.L., 1991. Better stories, not better constructs, to generate better theory: a rejoinder to Eisenhardt. *Academy of Management Review*, 16(3), pp.613–619.

Eastlick, M.A., Lotz, S.L. & Warrington, P., 2006. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), pp.877–886.

Eisenhardt, K.M., 1989. Agency Theory: An Assessment and Review. *The Academy of Management Review*, 14(1), pp.57–74.

Ellison, N., Heino, R. & Gibbs, J.L., 2006. Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment. *Journal of Computer-Mediated Communication*, 11(2), pp.415–441.

Emanuel, L., Neil, G., Bevan, C., Fraser, D., Stevanage, S., Whitty, M. & Jamison-Powell, S., 2014. Who am I? Representing the self offline and in different online contexts. *Computers in Human Behavior*, 41, pp.146–152.

Eschenfelder, K.R., 2004. Behind the Web site: An inside look at the production of Web-based textual government information. *Government Information Quarterly*, 21(3), pp.337–358.

Escobar-Rodríguez, T. & Carvajal-Trujillo, E., 2014. Online purchasing tickets for low cost carriers: An application of the unified theory of acceptance and use of technology (UTAUT) model. *Tourism Management*, 43, pp.70–88.

Ettredge, M., Richardson, V. & Scholz, S., 2001. The presentation of financial information at corporate web sites. *International Journal of Accounting Information Systems*,, 2, pp.149–168.

European Commission, 2015. *Future-proofing eGovernment for a Digital Single Market: An assessment of digital public service delivery in Europe-eGovernment Benchmark*, Luxemborg: European Union. Available at: https://www.capgemini.com/resource-file-access/resource/pdf/egov_benchmark _2014_insightreport.pdf. [Accessed 17 March 2016]

European Commission, 2016. *Reform of EU data protection rules*, Brussels: European Commision, Available at: http://ec.europa.eu/justice/data-protection/reform/ index_en.htm [Accessed 29 April 2016].

European Union, 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, European Union.

Evans, D. & Yen, D.C., 2006. E-Government: Evolving relationship of citizens and government, domestic, and international development. *Government Information Quarterly*, 23(2), pp.207–235.

Evans, J.R. & King, V.E., 1999. Business-to-Business Marketing and the World Wide Web: Planning, Managing, and Assessing Web Sites. *Industrial Marketing Management*, 28(4), pp.343–358.

Facebook, 2016. Company Info: Facebook Newsroom. *Facebook*. Available at: https://newsroom.fb.com/company-info/ [Accessed May 16, 2016].

Facebook, 2015. Statement of Rights and Responsibilities. *Facebook*. Available at: https://www.facebook.com/legal/terms [Accessed March 27, 2015].

Facetime Communications, 2008. *The Collaborative Internet: Usage Trends, End User Attitudes and IT Impact*. California: Facetime. Available at: http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/FTIME_US/F081031 C.pdf [Accessed 14 April 2016]

Faja, S. & Trimi, S., 2006. Influence of the Web Vendor’s Interventions on Privacy-Related Behaviors in E-Commerce. *Communications of the Association for Information Systems*, 17(27), pp.563–634.

Fallows, D., 2003. Spam: How it is hurting email and degrading life on the Internet, *Pew Internet & American Life Project*, Available at: http://www.pewinternet.org /2003/10/22/spam-how-it-is-hurting-email-and-degrading-life-on-the-internet/

[Accessed September 4, 2013]

Fasick, F.A., 1977. Some Uses of Untranscribed Tape Recordings in Survey Research. *Public Opinion Quarterly*, 41(4), pp.549–552.

Fath-Allah, A., Cheikhi, L., Al-Qutaish, R. & Idri, A., 2015. A Theoretical E-government Portals' Benchmarking Framework. In *10th International Conference on Intelligent Systems: Theories and Applications (SITA)*. Rabat, Morocco: IEEE, pp. 1–6.

Finn, R.L., Wright, D. & Friedewald, M., 2013. Seven Types of Privacy. In S. Gutwirth et al., eds. *In European data protection: Coming of age?*. Dordrecht: Springer Netherlands, pp. 3–32.

Floyd, D., Prentice-Dunn, S. & Rogers, R., 2000. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), pp.407–429.

Fogel, J. & Nehmad, E., 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), pp.153–160.

Fogg, B.J., 2002. Stanford Guidelines for Web Credibility. *A Research Summary from the Stanford Persuasive Technology Lab*. Available at: www.webcredibility.org/guidelines [Accessed 18 April 2016].

Fogg, B.J. & Tseng, H., 1999. Elements of computer credibility. In *Conference on Human Factors in Computing Systems - Proceedings*. Pittsburgh, PA: ACM, pp. 80–87.

Fox, S., Rainie, L., Horrigan, J. & Lenhart, A., 2000. Trust and privacy online: Why Americans want to rewrite the rules. *Pew Internet & American Life Project.* Available at: http://www.pewinternet.org [Accessed 23 July 2013].

Freelon, D., 2013. ReCal OIR : Ordinal, Interval, and Ratio Intercoder Reliability as a Web Service. *International Journal of Internet Science*, 8(1), pp.10–16.

Friedman, B., Kahn, P.H. & Howe, D.C., 2000. Trust online. *Communications of the ACM*, 43, pp.34–40.

FTC, 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report To Congress*, Available at: http://www.ftc.gov/reports/privacy2000/ privacy2000. pdf. [Accessed 18 May 2015]

Furnell, S. & Papadaki, M., 2008. Testing our defences or defending our tests: the obstacles to performing security assessment references. *Computer Fraud & Security*, 2008(5), pp.8–12.

Furnell, S.M., 2010. Online identity: Giving it all away? *Information Security Technical Report*, 15(2), pp.42–46.

Gallego, I., García, I. & Rodríguez, L., 2009. Universities' Websites: Disclosure Practices and the Revelation of Financial Information. *The International Journal of Digital Accounting Research*, 9, pp.153–192.

Gallego-Álvarez, I., Rodríguez-Domínguez, L. & García-Sánchez, I.-M., 2011. Information disclosed online by Spanish universities: content and explanatory factors. *Online Information Review*, 35(3), pp.360–385.

Garcia, A.C.B., Maciel, C. & Pinto, F.B., 2005. A Quality Inspection Method to Evaluate

E-Government Sites. In M. A. Wimmer et al., eds. *Electronic Government*. Springer Berlin Heidelberg, pp. 198–209.

García-sánchez, I.-M., Frías-Aceituno, J.-V. & Rodríguez-Domínguez, L., 2013. Determinants of Corporate Social Disclosure in Spanish Local Government. *Journal of Cleaner Production*, 39, pp.60–72.

van de Garde-Perik, E., Markopoulos, P., de Ruyter, B., Eggen, B. & IJsselsteijn, W., 2008. Investigating Privacy Attitudes and Behavior in Relation to Personalization. *Social Science Computer Review*, 26(1), pp.20–43.

Gatfield, T., Barker, M. & Graham, P., 1999. Measuring communication impact for university advertising materials. *Corporate Communications: An International Journal*, 4(2), pp.73–79.

Gefen, D. et al., 2005. Cultural diversity and trust in IT adoption: A comparison of potential e-Voters in the USA and South Africa. *Journal of Global Information Management*, 13(March), pp.54–78.

Germanakos, P., Christodoulou, E. & Samaras, G., 2007. A European Perspective of E-Government Presence – Where Do We Stand? The EU-10 Case. In M. A. Wimmer, H. A. Scholl, & A. Gronlund, eds. *Electronic Government: 6th International Conference, (EGOV 2007)*. Berlin-Heidelberg: Springer-Verlag, pp. 436–447.

Gilbert, D., Balestrini, P. & Littleboy, D., 2004. Barriers and benefits in the adoption of e-government. *International Journal of Public Sector Management*, 17(4), pp.286–301.

Giorgi, A., 2009. *The descriptive phenomenological method in psychology: A modified Husserlian approach*, Pittsburgh, PA, US: Duquesne University Press.

Goldbart, J. & Hustler, D., 2005. Ethnography. In B. Somekh & C. Lewin, eds. *Research Methods in the Social Sciences*. London: Sage Publications Inc, pp. 16–23.

Goldkuhl, G., 2004. Meanings of Pragmatism : Ways to conduct information systems research. In *Proceedings of the 2nd International Conference on Action in Language, Organisations and Information Systems (ALOIS)*. Linköping University, Linköping., pp. 17–18.

Goldkuhl, G., 2012. Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, 21(2), pp.135–146.

Gray, J.H. & Densten, I.L., 1998. Integrating quantitative and qualitative analysis using latent and manifest variables. *Quality & Quantity*, 32, pp.419–431.

Greene, J.C. & Caracelli, V.J., 2003. Making paradigmatic sense of mixed methods practice. In A. Tashakkori & C. Teddlie, eds. *Handbook of mixed methods in social and behavioral research*. California: Sage Publications Inc, pp. 91–110.

Greenleaf, G., 2013. Malaysia: ASEAN's first data privacy Act in force. *Privacy Laws & BUsiness International Report*, 126 (December), pp.11–14.

Grimmelikhuijsen, S., Porumbescu, G., Hong, B. & Im, T., 2013. The effect of transparency on trust in government: A cross-national comparative experiment. *Public Administration Review*, 73(4), pp.575–586.

Grimmelikhuijsen, S., 2010. Transparency of Public Decision Making: Towards Trust in

Local Government? *Policy & Internet*, 2(1), pp.5–35.

Gross, R. & Acquisti, A., 2005. Information Revelation and Privacy in Online Social Networks (The Facebook case). In *In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. WPES ’05. Alexandria, Virginia, USA: ACM Press, pp. 71–80.

Guba, E.G., 1990. The paradigm dialog. In E.G. Guba, ed. *The alternative paradigm dialog*. Newbury Park, CA: Sage, pp. 17–30.

Guba, E.G. & Lincoln, Y.S., 1994. Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln, eds. *Handbook of Qualitative Research*. Thousand Oaks, California: Sage, pp. 105–117.

Gundecha, P., Barbier, G. & Liu, H., 2011. Exploiting Vulnerability to Secure User Privacy on a Social Networking Site. In *17th ACM-SIGKDD Conference on Knowledge Discovery and Data Mining*. San Diego, CA, USA: ACM.

Gupta, B., Iyer, L. & Weisskirch, R., 2010. Facilitating Global E-Commerce: A Comparison of Consumers’ Willingness to Disclose Personal Information Online in the US and in India. *Journal of Electronic Commerce Research,* 11(1), pp.41–52.

Ha, L. & James, E.L., 1998. Interactivity reexamined: A baseline analysis of early business web sites. *Journal of Broadcasting & Electronic Media*, 42(February 2015), pp.457–474.

Haidar, G.G. & Abu Bakar, P.D.A.Z., 2012. E-Government Success in Malaysia Through Government Portal and Website Assessment. *International Journal of Computer Science Issues*, 9(5), pp.401–409.

Von Haldenwang, C., 2004. Electronic Government (E-Government) and Development. *The European Journal of Development Research*, 16(2), pp.417–432.

Halevi, T., Lewis, J. & Memon, N., 2013. Phishing, Personality Traits and Facebook. *arXiv preprint arXiv:1301.7643.* Available at: http://arxiv.org/abs/1301.7643 [Accessed 5 July 2013].

Hammersley, M., 2007. Methodological paradigms in Educational Research. Available at: http://www.tlrp.org/capacity/rm/wt/hammersley [Accessed 25 January 2016].

Hann, I., Hui, K., Lee, S. & Png, I., 2007. Overcoming Online Information Privacy Concerns: An Information Processing Theory Approach. *Journal of Management Information Systems,* 24(2), pp.13–42.

Hashim, R.S., 2007. Blogs of Their Own: A Story of Two Malaysian Women Bloggers. *3L Journal of Language Teaching, Linguistics and Literature, The Southeast Asian Journal of English Language Studies,* 13, pp.127–142.

Hassan, K.H., 2012. Personal data protection in employment: New legal challenges for Malaysia. *Computer Law & Security Review,* 28(6), pp.696–703.

Hawkey, K. & Inkpen, K.M., 2006. Keeping up appearances: understanding the dimensions of incidental information privacy. *Proceedings of ACM CHI 2006 Conference on Human Factors in Computing Systems,* ACM, pp.821–830.

He, J., Chu, W.W. & Liu, Z. (Victor), 2006. Inferring Privacy Information from Social Networks. In S. Mehrotra et al., eds. *Intelligence and Security Informatics: IEEE*

International Conference on Intelligence and Security Informatics, ISI 2006, San Diego, CA, USA, May 23-24, 2006. Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 154–165.

Hennick, M., Hutter, I. & Bailey, A., 2011. *Qualitative Research Methods,* Sage Publications Ltd.

Hew, K.F., 2011. Students’ and teachers' use of Facebook. *Computers in Human Behavior,* 27(2), pp.662–676.

Hofstede, G.H., 2001. *Culture’s consequences: Comparing values, behaviors, institutions, and organizations across nations,* Thousand Oaks, California: Sage Publications Inc.

Holsti, O.R., 1969. *Content Analysis for the Social Sciences and Humanities*, Reading MA: Addison-Wesley.

Holzer, M. & Kim, S.-T., 2005. *Digital Governance in Municipalities Worldwide (2005): A Longitudinal Assessment of Municipal Web sites throughout the World*, Available at: http://unpan1.un.org/intradoc/groups/public/documents/aspa/unpan012905.pdf. [Accessed 12 April 2016]

Hong, W. & Thong, J.Y.L., 2013. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, 37(1), pp.275–298.

Hoy, M.G. & Milne, G., 2010. Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising*, 10(2), pp.28–45.

Hsieh, H.-F. & Shannon, S.E., 2005. Three approaches to qualitative content analysis. *Qualitative health research*, 15(9), pp.1277–88.

Hsieh, Y.-C. (Jerrie), 2012. Hotel companies’ environmental policies and practices: a content analysis of their web pages. *International Journal of Contemporary Hospitality Management*, 24(1), pp.97–121.

Hsu, C. (Julia), 2006. Privacy concerns, privacy practices and web site categories: Toward a situational paradigm. *Online Information Review*, 30(5), pp.569–586.

Huang, Z., 2006. E-government practices at local levels: an analysis of US counties’ websites. *Issues in Information Systems*, 7(2), pp.165–170.

Huang, Z. & Benyoucef, M., 2014. Usability and credibility of e-government websites. *Government Information Quarterly*, 31(4), pp.584–595.

Hughes, R.L.D., 2015. Two concepts of privacy. *Computer Law & Security Review*, 31(4), pp.527–537.

Hussain, M.A., Elyas, T. & Nasseef, O.A., 2013. Research Paradigms: A slippery Slope for Fresh Researchers. *Life Science Journal*, 10(4), pp.2374–2381.

Hussein, M., Hirst, S., Salyers, V. & Osuji, J., 2014. Using Grounded Theory as a Method of Inquiry: Advantages and Disadvantages. *Qualitative Report*, 19(27), pp.1–15.

IBM, 1999. *IBM Multi-national consumer privacy survey*, Somers, NY. Available at: ftp://www6.software.ibm.com/software/security/privacy_survey_oct991.pdf [Accessed 21 March 2016]

Information Commisioner’s Office, 2016. *Conducting privacy impact assessments: code* *of practice*, UK. Available at: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf [Accessed 15 April 2016]

Introna, L.D. & Whitley, E.A, 2000. About experiments and style: A critique of laboratory research in information systems. *Information Technology & Management*, 13(3), pp.161–173.

Iofciu, T., Frankhauser, P., Abel, F. & Bishoff, K., 2011. Identifying Users Across Social Tagging Systems. In L. A. Adamic, R. A. Baeza-Yates, & S. Counts, eds. *Fifth International Conference on Weblogs and Social Media (ICWSM)*. Barcelona, Spain: The AAAI Press.

Irani, D., Webb, S., Pu, C. & Li, K., 2011. Modeling Unintended Leakage from Multiple Online Social Networks. *IEEE Computer Society*, pp.13–19.

ISO, 1998. *ISO 9241-11:1998 Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability*, Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=16883. [Accessed 2 December 2016]

Jacob, S.A. & Furgerson, S.P., 2012. Writing Interview Protocols and Conducting Interviews : Tips for Students New to the Field of Qualitative Research. *The Qualitative Report*, 17(2000), pp.1–10.

Jaeger, P.T., 2003. The endless wire: E-government as global phenomenon. *Government Information Quarterly*, 20(4), pp.323–331.

Janda, S. & Fair, L.L., 2004. Exploring consumer concerns related to the internet. *Journal of Internet commerce*, 3(1), pp.1–21.

Jang-Jaccard, J. & Nepal, S., 2014. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), pp.973–993.

Jensen, C., Potts, C. & Jensen, C., 2005. Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1-2), pp.203–227.

Jernigan, C. & Mistree, B.F.T., 2009. Gaydar: Facebook friendships expose sexual orientation. *First Monday*, 14(10). Available at: http://firstmonday.org/article/view/2611/2302 [Accessed 16 February 2015]

Ji, P. & Lieber, P.., 2010. Am I safe? Exploring relationships between primary territories and online privacy. *Journal of Internet Commerce*, 9(1), pp.3–22.

Johnson, M., Morgeson, F., Ilgen, D., Meyer, C. & Lloyd, J., 2006. Multiple professional identities: Examining differences in identification across work-related targets. *Journal of Applied Psychology*, 91(2), pp.498–506.

Joinson, A.N., 2008. '"Looking at",' "Looking up" or ' "Keeping up with" People? Motives and Uses of Facebook. In *Conference on Human Factors in Computing Systems*. Florence, Italy: ACM, pp. 1027–1036.

Joinson, A.N., Paine, C., Buchanan, T. & Reips, U., 2008. Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior*, 24(5), pp.2158–2171.

Joinson, A.N., Reips, U., Buchanan, T. & Schofield, C., 2010. Privacy, Trust, and Self-

Disclosure Online. *Human-Computer Interaction*, 25(1), pp.1–24.

Joinson, A.N., 2001. Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology,* 31(2), pp.177–192.

Joinson, A.N. & Paine, C.B., 2007. Self-disclosure, privacy and the Internet. In A. N. Joinson et al., eds. *The Oxford handbook of Internet psychology*. Oxford: Oxford University Press., pp. 235–250.

Jones, D. & Potts, L., 2010. Best practices for designing third party applications for contextually-aware tools. In *Proceedings of the 28th ACM International Conference on Design of Communication - SIGDOC '10*. ACM Press, p. 95.

Jones, H. & Soltren, H., 2005. Facebook: Threats to Privacy. *Project MAC: MIT Project on Mathematics and Computing, 1.*, December 1, pp.1–76.

Jones, R., Kumar, R., Pang, Bo. & Tomkins, A., 2008. Vanity Fair: Privacy in Querylog Bundles. In *Proceedings of the 17th ACM Conference on Information and Knowledge Management*. California, USA: ACM Press, pp. 853–862.

Jørgensen, M. & Phillips, L.J., 2002. *Discourse Analysis as Theory and Method,* London: Sage Publications Ltd.

Jose, A. & Lee, S., 2007. Environmental Reporting of Global Corporations: A Content Analysis based on Website Disclosures. *Journal of Business Ethics*, 72(4), pp.307–321.

Jourard, S.M. & Lasakow, P., 1958. Some factors in self-disclosure. *The Journal of Abnormal and Social Psychology,* Vol 56(1), pp.91–98.

Kaaya, J., 2004. Implementing e-government services in East Africa: Assessing status through content analysis of government websites. *Electronic Journal of E-government*, 2(1), pp.39–54. Available at: http://www.ejeg.com/issue/download.html?idArticle=21&a=bi&pagenumber=1&w=100 [Accessed August 6, 2013].

Kaisara, G. & Pather, S., 2011. The e-Government evaluation challenge: A South African Batho Pele-aligned service quality approach. *Government Information Quarterly,* 28(2), pp.211–221.

Kaliannan, M., Raman, M. & Dorasamy, M., 2009. ICT in the Context of Public Sector Service Delivery: A Malaysian Perpective. *WSEAS Transactions on Systems*, 8(4), pp.543–556.

Kamal, S.M., 2014. Google finally brings "Street View" to Malaysia. *Malay Mail Online*. Available at: http://www.themalaymailonline.com/malaysia/article/google-finally-brings-street-view-to-malaysia [Accessed May 11, 2016].

Kang, R., Brown, S. & Kiesler, S., 2013. Why Do People Seek Anonymity on the Internet?: Informing Policy and Design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '13. New York, NY, USA: ACM, pp. 2657–2666.

Karkin, N. & Janssen, M., 2014. Evaluating websites from a public value perspective: A review of Turkish local government websites. *International Journal of Information Management*, 34(3), pp.351–368.

Kawulich, B.B., 2004. Data Analysis Techniques in Qualitative Research. *Journal of Research in Education*, 14(1), pp.96–113.

Kehr, F., Kowatsch, T., Wentzel, D. & Fleisch, E., 2015. Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), pp.607–635.

Keith, M.J., Thompson, S., Hale, J. & Greer, C., 2012. Examining the Rationality of Location Data Disclosure through Mobile Devices. In *Thirty Third International Conference on Information Systems*. Orlando: AIS.

Keith, M.J., Thompson, S., Hale, J., Lowry, P. & Greer, C., 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human Computer Studies*, 71(12), pp.1163–1173.

Kim, D.J., Ferrin, D.L. & Rao, H.R., 2008. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), pp.544–564.

Van Knippenberg, D., Van Dick, R. & Tavares, S., 2007. Social identity and social exchange: Identification, support, and withdrawal from the job. *Journal of Applied Social Psychology*, 37(3), pp.457–477.

Van Knippenberg, D. & Van Schie, E.C.M., 2000. Foci and correlates of organizational identification. *Journal of Occupational and Organizational Psychology*, 73(2), pp.137–147.

Koch, R., Stelte, B. & Golling, M., 2012. Attack Trends in Present Computer Networks. In *IEEE 4th International Conference on Cyber Conflict (CYCON)*. pp. 269–280.

Kokolakis, S., 2015. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, pp.1–13.

Kolek, E. A. & Saunders, D., 2008. Online Disclosure: An Empirical Examination of Undergraduate Facebook Profiles. *Journal of Student Affairs Research and Practice*, 45(1), pp.1–25.

Kopackova, H., Michalek, K. & Cejna, K., 2010. Accessibility and findability of local e-government websites in the Czech Republic. *Universal Access in the Information Society*, 9(1), pp.51–61.

Kowatsch, T. & Maass, W., 2012. Critical privacy factors of internet of things services: An empirical investigation with domain experts. In *Lecture Notes in Business Information Processing*. Springer Berlin Heidelberg, pp. 200–211.

Kozikowski, P. & Groh, G., 2011. Inferring Profile Elements from Publicly Available Social Network Data. In *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom)*. IEEE, pp. 876–881.

Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T., 2010. Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), pp.109–125.

Krasnova, H., Veltri, N.F. & Günther, O., 2012. Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Business & Information Systems Engineering*, 4(3), pp.127–135.

Krippendorff, K., 1989. Content Analysis. *Departmental Papers (ASC)*, pp.403–407. Available at: http://repository.upenn.edu/asc.papers/266. [Acessed 13 November 2013]

Krippendorff, K., 2013. *Content Analysis: An Introduction to Its Methodology* Third Edition, Sage Publications Inc.

Krishnamurthy, B., Naryshkin, K. & Wills, C.E., 2011. Privacy leakage vs. protection measures: the growing disconnect. In *Web 2.0 Security and Privacy Workshop*. Oakland, CA, USA, pp. 1–10.

Krishnamurthy, B. & Wills, C., 2009. On the leakage of personally identifiable information via online social networks. In *Proceedings of the 2nd ACM Sigcomm Workshop on Online Social Networks (WOSN)*. Barcelona, Spain: ACM, pp. 7–12.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E., 2015. Advanced social engineering attacks. *Journal of Information Security and Applications*, 22(June), pp.113–122.

Krug, S., 2006. *Don't Make Me Think! A Common Sense Aproach to Web Usability* Second Edi. K. Whitehouse, ed., Berkeley, California: New Riders Publishing.

Külcü, Ö. & Henkoğlu, T., 2014. Privacy in social networks: An analysis of Facebook. *International Journal of Information Management*, 34, pp.761–769.

Kvale, S. & Brinkmann, S., 2009. *Interviews: Learning the Craft of Qualitative Research Interviewing* Second., Thousand Oaks, California: Sage Publications Inc.

Lacy, S. & Riffe, D., 1996. Sampling error and selecting intercoder reliability samples for nominal content categories. *Journalism and Mass Communication*, 73, pp.963–973.

Lah, F., 2008. Are IP addresses "Personally Identifiable Information"? *I/S: A Journal of Law and Policy for the Information Society*, 4(3), pp.681–706.

Lam, L.-F., Chen, K.-T. & Chen, L.-J., 2008. Involuntary information leakage in social network services. In K. Matsuura & E. Fujisaki, eds. *3rd International Workshop on Security (IWSEC 2008)*. Springer, pp. 163–183.

Lampe, C., Ellison, N. & Steinfield, C., 2006. A Face(book) in the Crowd: Social Searching vs. Social Browsing. In *Proceedings of the 2006 20th Anniversary Conference on Computer-Supported Cooperative Work CSCW '06*. Vancouver, Canada: ACM Press, pp. 167–170.

Lansley, G. & Longley, P., 2016. Deriving age and gender from forenames for consumer analytics. *Journal of Retailing and Consumer Services*, 30, pp.271–278.

Laric, M. V., Pitta, D.A. & Katsanis, L.P., 2009. Consumer Concerns for Healthcare Information Privacy: A Comparison of US and Canadian Perspectives. *Research in Healthcare Financial Management*, 12(1), pp.93–111.

LaRose, R. & Rifon, N., 2006. Your privacy is assured-of being disturbed: websites with and without privacy seals. *New Media & Society*, 8(6), pp.1009–1029.

Latif, M.H.A. & Masrek, M.N., 2010. Accessibility Evaluation on Malaysian E-Government Websites. *Journal of e-Government Studies and Best Practices*. Available at: http://www.ibimapublishing.com/journals/JEGSBP/2010/935272/935272.pdf. [Accessed 18 July 2015]

Laufer, R.S. & Wolfe, M., 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), pp.22–42.

Lederer, S., Mankoff, J., Dey, A. & Beckmann, C., 2003. Managing Personal Information Disclosure in Ubiquitous Computing Environments. In *Computer Science Division Technical Report UCB-CSD-03-1257*. Computer Science. University of California, Berkeley: Intel Research Berkley.

Lee, D., Im, S. & Taylor, C., 2008. Voluntary self-disclosure of information on the internet: a multimethod study of the motivations and consequences of disclosing information on blogs. *Psychology and Marketing*, 25(7), pp.692–710.

Lee, R.L. & Joseph, R.C., 2013. An examination of web disclosure and organizational transparency. *Computers in Human Behavior*, 29(6), pp.2218–2224.

Lee, Y. & Kozar, K.A., 2012. Understanding of website usability: Specifying and measuring constructs and their relationships. *Decision Support Systems*, 52(2), pp.450–463.

Lewis, S.C., Zamith, R. & Hermida, A., 2013. Content Analysis in an Era of Big Data: A Hybrid Approach to Computational and Manual Methods. *Journal of Broadcasting & Electronic Media*, 57(1), pp.34–42.

Li, H., Sarathy, R. & Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), pp.62–71.

Li, Y., 2011. Empirical Studies on Online Information Privacy Concerns : Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, 28(1), pp.453–496.

Li, Y., 2014. The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, 57, pp.343–354.

Li, Y., 2012. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), pp.471–481.

Liebermann, Y. & Stashevsky, S., 2002. Perceived risks as barriers to Internet and e-commerce usage. *Qualitative Market Research: An International Journal*, 5(4), pp.291–300.

Lincoln, Y.S. & Guba, E.G., 1985. *Naturalistic Inquiry*, Newbury Park, CA: Sage Publications Inc.

Lincoln, Y.S. & Guba, E.G., 2000. Paradigmatic controversies, contradictions, and emerging confluences. In N. K. Denzin & Y. S. Lincoln, eds. *The SAGE Handbook of Qualitative Research*. California: Sage Publications Inc, Thousand Oaks, pp. 163–188.

Linderman, A., 2001. Computer content analysis and manual coding techniques: A comparative analysis. In M. D. West, ed. *Theory, Method, and Practice in Computer Content Analysis*. Westport CT: Ablex Publishing.

LinkedIn, 2015. About LinkedIn. Available at: https://press.linkedin.com/about-linkedin [Accessed June 15, 2015].

Lombard, M., Snyder-Duch, J. & Bracken, C.C., 2002. Content Analysis in Mass Communication Assessment and Reporting of Intercoder Reliability. *Human Communication Research*, 28(4), pp.587–604.

Lombard, M., Snyder-Duch, J. & Bracken, C.C., 2004. *Practical Resources for Assessing and Reporting Intercoder Reliability in Content Analysis Research Projects*. Available at: http://www.temple.edu/sct/mmc/reliability [Accessed September 17, 2013].

De Long, D.W. & Fahey, L., 2000. Diagnosing cultural barriers to knowledge management. *Academy of Management Perspectives*, 14(4), pp.113–127.

Lowry, P.B., Cao, J. & Everard, A., 2011. Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *Journal of Management Information Systems*, 27(4), pp.163–200.

Luo, X., Brody, R., Seazzu, A. & Burd, S., 2011. Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal*, 24(3), pp.1–8.

Lwin, M., Wirtz, J. & Williams, J.D., 2007. Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(4), pp.572–585.

Lwin, M.O. & Williams, J.D., 2003. A model interpreting the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters*, 14(4), pp.257–252.

Madden, M., Fox, S., Smith, A. & Vitak, J., 2007. Digital Footprints: Online identity management and search in the age of transparency, *Pew Internet & American Life Project* Washington. Available at: http://www.pewinternet.org/PPF/r/229 /report_display.asp. [Accessed 4 January 2015]

Madden, M. & Smith, A., 2010. Reputation Management and Social Media, *Pew Internet & American Life Project*, Washington. Available at: http://www.pewinternet.org /2010/05/26/reputation-management-and-social-media/. [Accessed 9 January 2015]

Malheiros, M., Preibusch, S. & Sasse, M.A., 2013. "Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. In *Sixth International Conference on Trust & Trustworthy Computing. Lecture Notes in Computer Science, vol. 7904*.

Malhotra, N.K., Kim, S.S. & Agarwal, J., 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale,, and a Causal Model. *Information Systems Research*.

van Manen, M., 1990. *Researching lived experience: Human science for an action sensitive pedagogy*, Ontario: Althouse Press.

Mangold, W.G. & Faulds, D.J., 2009. Social media: The new hybrid element of the promotion mix. *Business Horizons*, 52(4), pp.357–365.

Marcus, G.E. & Cushman, D., 1982. Ethnographies as Texts. *Annual Review of Anthropology*, 11(1982), pp.25–69.

Margulis, S.T., 2003. On the Status and Contribution of Westin’s and Altman's Theories of Privacy. *Journal of Social Issues*, 59(2), pp.411–429.

Margulis, S.T., 2011. Three Theories of Privacy: An Overview. In S. Trepte & L. Reinecke, eds. *Privacy online: Perspectives on Privacy and Self- Disclosure in the Social Web*. Berlin: Springer Berlin Heidelberg, pp. 9–17.

Markham, A.N., 2004. Internet Communication as a Tool for Qualitative Research. In D. Silverman, ed. *Qualitative Research: Theory, Method and Practice*. London: Sage Publications Inc, pp. 95–124.

Marshall, C. & Rossman, G.B., 2011. *Designing Qualitative Research* 5th Edition, Sage Publications, Inc.

Marshall, C.C. & Lindley, S.E., 2014. Searching for Myself: Motivations and Strategies for Self-search. In *Proceedings of the SIGHI Conference on Human Factors in Computing Systems*. Toronto, Canada: ACM Press, pp. 3675–3684.

Mateos, P., 2007. A review of name-based ethnicity classification methods and their potential in population studies. *Population, Space and Place,* 13(4), pp.243–263.

Mateos, P., Longley, P.A. & O’Sullivan, D., 2011. Ethnicity and population structure in personal naming networks. *PLoS ONE,* 6(9), p.e22943.

McCallister, E. & Scarfone, K., 2010. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Recommendations of the National Institute of Standards and Technology. *NIST Special Publication 800-122*.

McMillan, S.J., 2000. The Microscope and the Moving Target: The Challenge of Applying Content Analysis to the World Wide Web. *Journalism and Mass Communication Quarterly,* 11(1), pp.80–98.

Mengle, G.S., 2016. Fake profile of former top cop under scanner. *The Hindu*. Available at: http://www.thehindu.com/news/cities/mumbai/news/fake-profile-of-former-top-cop-under-scanner/article8914803.ece [Accessed July 30, 2016].

Mertens, D., 2010. *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods* Third Edition, Thousand Oaks, California: Sage Publications Inc.

Mesch, G.S., 2012. Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in Human Behavior*, 28(4), pp.1471–1477.

Mesch, G.S. & Beker, G., 2010. Are Norms of Disclosure of Online and Offline Personal Information Associated with the Disclosure of Personal Information Online. *Human Communication Research*, 36(4), pp.570–592.

Metzger, M.J., 2007. Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, 12(2), pp.1–27.

Metzger, M.J., 2006. Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure. *Communication Research*, 33(3), pp.155–179.

Metzger, M.J., 2004. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, 9(4), p.00.

Milberg, S.J. et al., 1995. Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12), pp.65–74.

Milberg, S.J., Smith, H.J. & Burke, S.J., 2000. Information privacy: Corporate management and national regulation. *Organization Science*, 11(1), pp.35–37.

Miles, M.B., Huberman, A.M. & Saldana, J., 2014. *Qualitative Data Analysis* 3rd Edition, Sage Publications Inc.

Miltgen, C.L. & Peyrat-Guillard, D., 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, 23(2), pp.103–125.

Mislove, A., Viswanath, B., Gummadi, K. & Druschel, P., 2010. You are who you know: inferring user profiles in online social networks. In *Proceedings of the third ACM international conference on Web search and data mining*. ACM, pp. 251–260.

Moustakas, C., 1994. *Phenomenological Research Methods*, Thousand Oaks, California: Sage Publications Inc.

Moustakas, E., Ranganathan, C. & Duquenoy, P., 2005. Combating Spam Through Legislation: A Comparative Analysis of US and European Approaches. In *Second conference on email and anti-spam CEAS 2005*. California, USA.

Multimedia Development Corporation, 2012. *Malaysia Government Portals and Websites Assessment (MGPWA) 2012*, Cyberjaya, Malaysia.

Nam, C., Song, C., Lee, E. & Park, C., 2006. Consumers ’ Privacy Concerns and Willingness to Provide Marketing-Related Personal. *Advances in Consumer Research*, 33(1), pp.212–217.

Nam, T., 2014. Determining the type of e-government use. *Government Information Quarterly*, 31(2), pp.211–220.

Nanchahal, K., Mangtani, P., Alston, M. & dos Santos Silva, I., 2001. Development and validation of a computerized South Asian names and group recognition algorithm (SANGRA) for use in British health-related studies. *Journal of Public Health Medicine*, 23(4), pp.278–285.

Ndou, V., 2004. E-government for Developing Countries: Opportunities and Challenges. *The Electronic Journal on Information System in Developing Countries*, 18(1), pp.1–24.

Ness, K.E. & Mirza, A. M., 1991. Corporate social disclosure: A note on a test of agency theory. *The British Accounting Review*, 23, pp.211–217.

Neuendorf, K.A., 2002. *The Content Analysis Guidebook,* Thousand Oaks US: Sage Publications Inc.

Neuman, S.B., 2009. *Social research methods: Qualitative and quantitative approaches* 7th Edition, Boston: Allyn & Bacon.

Nguyen, M., Bin, Y.S. & Campbell, A., 2012. Comparing Online and Offline Self-Disclosure: A Systematic Review. *Cyberpsychology, behavior and social networking*, 15(2), pp.103–11.

Niemietz v. Germany, 1992. *Niemietz v Germany,* 16 EHRR 97.

Nissenbaum, H., 2004. Privacy as Contextual Integrity. *Washington Law Review*, 79(1), pp.101–139.

Nissenbaum, H., 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, California: Stanford University Press.

Norberg, P.A., Horne, D.R. & Horne, D.A., 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1), pp.100–126.

Nosko, A., Wood, E. & Molema, S., 2010. All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior*, 26(3), pp.406–418.

O'Bien, D. & Torres, A., 2012. Social Networking and Online Privacy: Facebook Users' Perceptions. *Irish Journal of Management*, pp.63–98.

Odendaal, N., 2003. Information and communication technology and local governance: Understanding the difference between cities in developed and emerging economies. *Computers, Environment and Urban Systems*, 27, pp.585–607.

Office of the Australian Information Commissioner, 2010. *Privacy Impact assessment Guide*, Australia. [Accessed 2 April 2016]

Oh, O., Chakraborty, R., Rao, H.R. & Upadhyaya, S., 2009. An exploration of unintended online private information disclosure in educational institutions across four countries. In *eCrime Researchers Summit, eCRIME'09*. IEEE, pp. 1–11.

Olivero, N. & Lunt, P., 2004. Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, 25(2), pp.243–262.

Orlikowski, W.J. & Baroudi, J.J., 1991. Studying Information Technology in Organizations: Research Approaches and Assumptions. *Source: Information Systems Research*, 2(1), pp.1–28.

Paine, C., Reips, U., Stieger, S., Joinson, A. & Buchanan, T., 2007. Internet users' perceptions of "privacy concerns" and "privacy actions." *International Journal of Human-Computer Studies*, 65(6), pp.526–536.

Panopoulou, E., Tambouris, E. & Tarabanis, K., 2008. A framework for evaluating web sites of public authorities. *Aslib Proceedings*, 60(5), pp.517–546.

Parajuli, J., 2007. A content analysis of selected government web sites: A case study of Nepal. *The Electronic Journal of e-Government*, 5(1), pp.87–94.

Paris, M., 2006. Website accessibility: A survey of local e-government websites and legislation in Northern Ireland. *Universal Access in the Information Society*, 4(4), pp.292–299.

Patsioura, F., Kitsiou, S. & Markos, A., 2009. Evaluation of greek public hospital websites. In *ICE-B-2009 International Conference on E-business*. pp. 223–229.

Patton, M.Q., 2002. *Qualitative Research and Evaluation Methods* 3rd ed., Thousand Oaks, California: Sage Publications Inc.

Pavlou, P.A., Liang, H. & Xue, Y., 2007. Understanding and Mitigating Uncertainty in

Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly*, 31(1), pp.105–136.

Pellissier, R., 2008. *Business Research Made Easy*, Juta Academic.

Pesce, J.P., Casas, D., Rauber, G. & Almeida, V., 2012. Privacy attacks in social media using photo tagging networks: a case study with Facebook. In *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*. Lyon, France: ACM, p. Article 4.

Peslak, A.R., 2005. An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics*, 59(4), pp.327–345.

Peter, J. & Lauf, E., 2002. Reliability in Cross-National Content Analysis. *Journalism and Mass Communication Quarterly*, 79(4), pp.815–832.

Petronio, S., 2002. *Boundaries of Privacy: Dialectics of Disclosure*, State University of New York Press.

Petronio, S.S., 1991. Communication boundary management: a theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, pp.311–335.

Phelps, J., Nowak, G. & Ferrell, G., 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1), pp.27–41.

Pina, V., Torres, L. & Royo, S., 2007. Are ICTs Improving Transparency and Accountability in the EU Regional and Local Governments? An Empirical Study. *Public Administration*, 85(2), pp.449–472.

Pinto, M., Guerro, D., Fernandez-Ramos, A. & Doucer, A., 2009. Information provided by Spanish university websites on their assessment and quality processes. *Scientometrics*, 81(1), pp.265–289.

Pinto, M., Guerrero, D. & Granell, X., 2014. Dissemination of information and visibility of the European Higher Education Area through the websites of Spanish universities: A longitudinal metric analysis, 2007-2012. *Scientometrics*, 98(2), pp.1235–1255.

Pinto, M., Sales, D. & Doucet, A., 2007. Metric analysis of the information visibility and diffusion about the European Higher Education Area on Spanish University websites. *Scientometrics*, 72(2), pp.345–370.

Piotrowski, S.J. & Van Ryzin, G.G., 2007. Citizen attitudes toward transparency in local government. *The American Review of Public Administration*, 37(3), pp.306–323.

Poland, B.D., 1995. Transcription Quality as an Aspect of Rigor in Qualitative Research. *Qualitative Inquiry*, 1(3), pp.290–310.

La Porte, T.M., Demchak, C.C. & Friis, C., 2001. Webbing governance: global trends across national-level public agencies. *Communications of the ACM*, 44(1), pp.63–67.

La Porte, T.M., Demchak, C.C. & De Jong, M., 2002. Democracy and Bureaucracy in the Age of the Web: Empirical Findings and Theoretical Speculations. *Administration & Society*, 34(4), pp.411–446.

Potter, W.J. & Levine-Donnerstein, D., 1999. Rethinking validity and reliability in content analysis. *Journal of Applied Communication Research*, 27(3), pp.258–284.

Ragan, S., 2016. Phishing attacks targeting W-2 data hit 41 organizations in Q1 2016. *CSO online*. Available at: http://www.csoonline.com/article/3048263/security/ phishing-attacks-targeting-w-2-data-hit-41-organizations-in-q1-2016.html [Accessed July 8, 2016].

Rainie, L. et al., 2013. Anonymity, Privacy, and Security Online, *Pew Internet & American Life Project* Washington. Available at: http://pewinternet.org/Reports/2013/Anonymity-online.aspx. [Accessed 19 February 2016]

Razavi, M.N. & Iverson, L., 2006. A grounded theory of information sharing behavior in a personal learning space. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work - CSCW '06*. p. 459.

Redford, E.S., 1969. *Democracy in the administrative state*, New York: Oxford University Press.

Reips, U., 2011. Privacy and the disclosure of information on the Internet: Issues and measurement. In B. Agata, A. Przepiórka, & T. Rowiński, eds. *Internet in Psychological Research*. Warzawa, Poland: UKSW Publishing House, pp. 71–104.

Reynolds, B., Venkatananthan, J., Gonçalves, J. & Kostakos V., 2011. Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours. In P. Campos et al., eds. *Human-Computer Interaction -- INTERACT 2011: 13th IFIP TC 13 International Conference, Lisbon, Portugal, September 5-9, 2011, Proceedings, Part III*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 204–215.

Richards, L., 2014. *Handling Qualitative Data: A Practical Guide* Third Edit., Sage Publications Inc.

Rindfleisch, T.C., 1997. Privacy, information technology, and health care. *Communications of the ACM*, 40(8), pp.92–100.

Ritchie, J. & Lewis, J., 2003. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, London: Sage Publications.

Rogers, R.W., 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology: Interdisciplinary and Applied*, 91(1), pp.93–114.

Rohm, A. & Milne, G., 2004. Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, 57(9), pp.1000–1011.

Rossler, B., 2005. *The Value of Privacy*, Cambridge, UK: Polity Press.

Rossman, G.B. & Rallis, S.F., 2011. *Learning in the Field: An Introduction to Qualitative Research* 3rd Edition., Thousand Oaks, California: Sage Publications Inc.

Rothbard, N.P. & Ramarajan, L., 2009. Checking your identities at the door? Positive relationships between nonwork and work identities. In L. M. Roberts & J. E. Dutton, eds. *Exploring positive identities and organizations: Building a theoretical and* *research foundation*. New York: Routledge, pp. 125–148.

Saldana, J., 2013. *The Coding Manual for Qualitative Researchers* 2nd Edition, Sage Publications Inc.

Salem, F., 2007. Benchmarking the e-government bulldozer: beyond measuring the tread marks. *Measuring Business Excellence,* 11(4), pp.9–22.

Salin, A.S.A.P. & Abidin, Z.Z., 2011. Being Transparent–An Evidence of a Local Authority in Malaysia. In *2011 International Conference on Sociality and Economics Development*. IACSIT Press Singapore, pp. 363–366.

Samkin, G. & Schneider, A., 2014. Using university websites to profile accounting academics and their research output: A three country study. *Meditari Accounting Research*, 22(1), pp.77–106.

Sarantakos, S., 2013. *Social Research* 4th Edition, Palgrave Macmillan.

Savin-Baden, M. & Major, C.H., 2013. *Qualitative Research : The essential guide to theory and practice.* 1st Editio., London, UK: Routledge.

Scassa, T., 2014. Privacy and Open Government. *Future Internet*, 6(2), pp.397–413. Available at: http://www.mdpi.com/1999-5903/6/2/397/ [Accessed July 13, 2014].

Schilit, B., Hong, J. & Gruteser, M., 2003. Wireless Location Privacy Protection. *Computer,* (December), pp.135–137.

Schrammel, J., Köffel, C. & Tscheligi, M., 2009. How Much do You Tell? Information Disclosure Behaviour in Different Types of Online Communities. In *Proceedings of the Fourth International Conference on Communities and Technologies, ACM*. New York, USA, pp. 275–284.

Shareef, M.A., Kumar, V., Kumar, U. & Dwivedi, Y., 2011. E-Government Adoption Model (GAM): Differing service maturity levels. *Government Information Quarterly*, 28(1), pp.17–35.

Sharma, S. & Crossler, R.E., 2014. Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications*, 13(5), pp.305–319.

Sheehan, K.B. & Hoy, M.G., 2000. Dimensions of Privacy Concern among Online Consumers. *Journal of Public Policy & Marketing*, 19(1), pp.62–73.

Sheldon, P., 2008. Student Favorite: Facebook and Motives for its Use. *Southwestern Mass Communication Journal*, 23(2), pp.39–53.

Shenton, A.A., 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, 22, pp.63–75.

Shieh, J.-C., 2012. From website log to findability. *The Electronic Library*, 30(5), pp.707–720.

Shim, D.C. & Eom, T.H., 2009. Anticorruption effects of information communication and technology (ICT) and social capital. *International Review of Administrative Sciences,* 75(1), pp.99–116.

Shim, D.C. & Eom, T.H., 2008. E-Government and Anti-Corruption: Empirical Analysis of International Data. *International Journal of Public Administration*, 31(3), pp.298–316.

Shokri, R., Theodorakopoulos, G., Le Boudec, J. & Hubaux, J., 2011. Quantifying location privacy. In *Proceedings - IEEE Symposium on Security and Privacy*. Berkeley, CA: IEEE, pp. 247–262.

Siar, S. V, 2005. E-governance at the Local Government Level in the Philippines: An Assessment of City Government Websites. *Philippine Journal of Development*, 32(2), pp.135–168.

Simons, H., 1996. The paradox of case study. *Cambridge Journal of Education*, 26(2), pp.225–240.

Simpson, A.C., 2011. On privacy and public data: a study of data.gov.uk. *Journal of Privacy and Confidentiality*, 3(1), pp.51–65.

Sipior, J.C., Ward, B.T. & Bonner, P.G., 2004. Should spam be on the menu? *Communications of the ACM - Wireless sensor networks*, 47(6), pp.59–63.

Skeels, M.M. & Grudin, J., 2009. When social networks cross boundaries: A case study of workplace use of Facebook and LinkedIn. In *GROUP '09 Proceedings of the ACM 2009 international conference on Supporting group work*. Florida, USA: ACM Press, pp. 95–103.

Slane, B.H., 2000. Killing the Goose? Information Privacy Issues on the Web. Available at: http://www.privacy.org.nz/news-and-publications/speeches-and-presentations/killing-the-goose-information-privacy-issues-on-the-web/ [Accessed May 12, 2014].

Smith, A.G., 2001. Applying evaluation criteria to New Zealand government websites. *International Journal of Information Management*, 21(2), pp.137–149.

Smith, D., 2013. Life's certainties: death, taxes and APTs. *Network Security*, 2013(2), pp.19–20.

Smith, H.J., Milberg, S., Burke, S. & Hall, 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2), pp.167–196.

Smith, H.J., 1993. Privacy Policies and Practices: Inside the Organizational Maze. *Communication of the ACM*, 36(12), pp.104–122.

Smith, H.J., Dinev, T. & Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), pp.989–1015.

Snead, J.T. & Wright, E., 2014. E-government research in the United States. *Government Information Quarterly*, 31(1), pp.129–136.

Solove, D.J., 2006. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), pp.477–560.

Solove, D.J., 2002. Conceptualizing privacy. *California Law Review*, 90(4), pp.1087–1155.

Solove, D.J., 2007. *The future of reputation: Gossip, rumor, and privacy on the internet*, New Haven, CT: Yale University Press.

Spiekermann, S., 2012. The challenges of privacy by design. *Communications of the*

ACM, 55(7), p.38.

Stahl, B.C., 2008. The Impact of the UK Human Rights Act 1998 on Privacy Protection in the Workplace. In R. Subramaniam, ed. *Computer Security, Privacy, and Politics : Current Issues, Challenges, and Solutions*. IRM Press, pp. 55–68.

Stahl, B.C. & Elbeltagi, I., 2004. Cultural Universality Versus Particularity in CMC. *Journal of Global Information Technology Management*, 7(4), pp.47–65.

Stake, R.E., 1995. *The art of case study research*, Thousand Oaks, California: Sage Publications Inc.

Stamoulis, D.S. & Georgiadis, P., 2000. Vision , Roles and Steps for Governments in Transition to the Digital Age. In *Proceedings of 11th International Workshop on Database and Expert Systems Applications*. London: IEEE, pp. 369–376.

Stan, L., 1999. An introduction to phenomenological research. Available at: http://www.sld.demon.co.uk/resmethy.pdf. [Accessed August 20, 2013]

Stanton, J.M., 2003. Information Technology and Privacy: A Boundary Management Perspective. In S. Clarke et al., eds. *Socio-Technical and Human Cognition Elements of Information Systems*. Information Science Publishing, pp. 79–103.

Stanton, J.M. & Stam, K.R., 2003. Information Technology, Privacy, and Power within Organizations: a view from Boundary Theory and Social Exchange perspectives . *Surveillance and Society*, 1(2), pp.152–190.

Stemler, S., 2001. An overview of content analysis. *Practical assessment, research & evaluation*, (17), pp.1–7.

Stephey, M.J., 2008. Sarah Palin’s E-Mail Hacked. *TIME*, 2008. Available at: http://content.time.com/time/politics/article/0,8599,1842097,00.html [Accessed August 1, 2016]

Stewart, K.A. & Segars, A.H., 2002. An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1), pp.36–49.

Stone, E., Gueutal, H., Gardner, D. & McClure, S., 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68(3), pp.459–468.

Stopfer, J.M. & Gosling, S.D., 2013. Online social networks in the work context. In D. Derks & A. Bakker, eds. *The Psychology of Digital Media at Work*. Psychology Press, pp. 39–59.

Strauss, A. & Corbin, J., 1994. Grounded theory methodology: An overview. In *Handbook of qualitative research*. Sage Publications, pp. 273–285.

Strauss, A. & Corbin, J., 1998. *Basics of qualitative research: Techniques and procedures for developing grounded theory* Second Edi., Thousand Oaks, California: Sage Publications Inc.

Strauss, A.. & Corbin, J., 1990. *Basics of qualitative research*, Newbury Park, CA: Sage Publications Inc.

Strauss, A., 1987. *Qualitative analysis for social scientists*, New York, Cambridge: University Press.

Stutzman, F., Gross, R. & Acquisti, A., 2013. Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. *Journal of Privacy and Confidentiality*, 4(2), pp.7–41.

Symantec Corporation, 2013. *Internet Security Threat Report 2013 Volume 18*, Mountain View, CA 94043 USA. Available at: http://www.symantec.com/content/en/us /enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf. [Accessed 11 January 2015]

Symantec Corporation, 2015. *Internet Security Threat Report 2015 Volume 20*, Mountain View, CA. Available at https://www.symantec.com/security-center/threat-report [Accessed 15 May 2015]

Symantec Corporation, 2016. *Internet Security Threat Report 2016 Volume 21*, Mountain View, CA. Available at https://www.symantec.com/security-center/threat-report [Accessed 29 April 2016]

Tate, M.A., 2010. *Web Wisdom: How to Evaluate and Create Information Quality on the Web* 2nd Editio., Florida: CRC Press.

Taylor, J. & Watkinson, D., 2007. Indexing reliability for condition survey data. *The Conservator*, 30(1), pp.49–62.

van Teijlingen, E. & Hundley, V., 2001. The importance of pilot studies. *Social Research Update*, (35), pp.33–6. Available at: http://sru.soc.surrey.ac.uk/SRU35.html. [Accessed 19 August 2013]

Teo, T.S.H., Srivastava, S.C. & Jiang, L., 2009. Trust and Electronic Government Success: An Empirical Study. *Journal of Management Information Systems*, 25(3), pp.99–132.

Thayer, A., Evans, M., McBride, A., Queen, M. & Spyridakis, J., 2007. Content Analysis as a Best Practice in Technical Communication Research. *Journal of Technical Writing and Communication*, 37(3), pp.267–279.

Thomas, J.C. & Streib, G., 2003. The New Face of Government: Citizen-Initiated Contacts in the Era of E-Government. *Journal of Public Administration Research Theory*, 13(1), pp.83–102.

Tidwell, L.C. & Walther, J.B., 2002. Computer-Mediated Communication Effects on Disclosure, Impressions, and Interpersonal Evaluations: Getting to Know One Another a Bit at a Time. *Human Communication Research*, 28(3), pp.317–348.

Treasury Board of Canada Secretariat, 2012. *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks Guidelines*, Canada.

Treeratpituk, P. & Giles, C., 2012. Name-Ethnicity Classification and Ethnicity-Sensitive Name Matching. In *Twenty-Sixth AAAI Conference on Artificial Intelligence*. Toronto, Canada, pp. 1141–1147.

Trend Micro Incorporated, 2012. *Spear-Phishing Email: Most Favored APT Attack Bait*, Available at: http://www.trendmicro.co.uk/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.

Tu, C., 2002. The relationship between social presence and online privacy. *The Internet and Higher Education*, 5(4), pp.293–318.

Tufekci, Z., 2008. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 28(1), pp.20–36.

Tufford, L. & Newman, P., 2012. Bracketing in Qualitative Research. *Qualitative Social Work*, 11(1), pp.80–96.

Turner, D.W.I., 2010. Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report*, 15(3), pp.754–760.

Tzermias, Z., Prevelakis, V. & Ioannidis, S., 2014. Privacy Risks from Public Data Sources. In N. Cuppens-Boulahia et al., eds. *ICT Systems Security and Privacy Protection: 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 156–168.

United Nations Department of Economic and Social Affairs, 2002. *Benchmarking E-government: A Global Perspective:Assessing the progress of the UN member states*, New York.

United Nations Department of Economic and Social Affairs, 2014. *United Nations E-Government Survey 2014: E-Government for the Future We Want*, New York.

Vaismoradi, M., Turunen, H. & Bondas, T., 2013. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, 15(3), pp.398–405.

Veljkovic, N., Bogdanovic-Dinic, S. & Stoimenov, L., 2014. Benchmarking open government: An open data perspective. *Government Information Quarterly*, 31, pp.278–290.

Walsham, G., 2006. Doing interpretive research. *European Journal of Information Systems*, 15(3), pp.320–330.

Walsham, G., 1995. Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, 4(2), pp.74–81.

Walther, J.B., Van Der Heide, B., Kim, S., Westerman, D. & Tong, S., 2008. The role of friends' appearance and behavior on evaluations of individuals on facebook: Are we known by the company we keep? *Human Communication Research*, 34(1), pp.28–49.

Wan, C.S., 2002. The web sites of international tourist hotels and tour wholesalers in Taiwan. *Tourism Management*, 23(1), pp.155–160.

Wang, S., Beatty, S.E. & Foxx, W., 2004. Signaling the trustworthiness of small online retailers. *Journal of Interactive Marketing*, 18(1), pp.53–69.

Wang, S.S. et al., 2010. Face off: Implications of visual cues on initiating friendship on Facebook. *Computers in Human Behavior*, 26(2), pp.226–234.

Wang, Y., Komanduri, S., Leon, P., Norcie, G., Acquisti, A. & Cranor, L., 2011. "I regretted the minute I pressed share": A Qualitative Study of Regrets on Facebook. In *Symposioum on Usable Privacy and Security 2011, Pittsburgh (USA)*. pp. 1–16.

Wang, Y.S., 2008. Assessing e-commerce systems success: A respecification and validation of the DeLone and McLean model of IS success. *Information Systems Journal*, 18, pp.529–557.

Ward, S., Bridges, K. & Chitty, B., 2005. Do Incentives Matter? An Examination of Online Privacy Concerns and Willingness to Provide Personal and Financial Information. *Journal of Marketing Communication*, 11(1), pp.21–40.

Warren, S.D. & Brandeis, L.D., 1890. The Right to Privacy. *Harvard Law Review*, 4(5), pp.193–220.

Waseda University, 2012. *The 2012 Waseda University International e-Government Ranking*, Available at: http://www.e-gov.waseda.ac.jp/images/Press Released on e-Gov ranking 2012.pdf. [Accessed 22 April 2016]

Waseda University & International Academy of CIO (IAC), 2015. *WASEDA–IAC 11th International E-Government Ranking 2015*, Tokyo.

Waters, S. & Ackerman, J., 2011. Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure. *Journal of Computer-Mediated Communication*, 17(1), pp.101–115.

Wathen, C.N. & Burkell, J., 2002. Believe it or not: Factors influencing credibility on the Web. *Journal of the American Society for Information Science and Technology*, 53(2), pp.134–144.

Webber, R., 2007. Using names to segment customers by cultural, ethnic or religious origin. *Journal of Direct, Data and Digital Marketing Practice*, 8(3), pp.226–242.

Weerakkody, V., Irani, Z., Lee, H., Osman, I. & Hindi, N., 2013. E-government implementation: A bird’s eye view of issues relating to costs, opportunities, benefits and risks. *Information Systems Frontiers*, 17(4), pp.889–915.

Weible, R.J., 1993. *Privacy and data: an empirical study of the influence and types and data and situational context upon privacy perceptions*. Mississippi State University.

Welch, E.W. & Hinnant, C.C., 2003. Internet use, transparency, and interactivity effects on trust in government. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*. IEEE, p. 144.

West, D.M., 2007. *Global E-Government, 2007*, Rhodes Island, US. Available at: http://www.insidepolitics.org/egovtdata.hatml. [Accessed 7 November 2015]

Westin, A.F., 1967. *Privacy and Freedom.*, New York: Atheneum.

White, B., 2003. Web accessibility, mobility and findability. In *Proceedings of the IEEE first Latin American web congress, LA-WEB 2003*. Santiago de Chile, pp. 239–241.

White, T.B., 2004. Consumer Disclosure and Disclosure Avoidance: A Motivational Framework. *Journal of Consumer Psychology*, 14(1-2), pp.41–51.

Wilkinson, D. & Thelwall, M., 2011. Researching Personal Information on the Public Web: Methods and Ethics. *Social Science Computer Review*, 29(4), pp.387–401.

Williams van Rooij, S. & Lemp, L.K., 2010. Positioning e-Learning Graduate Certificate Programs: Niche Marketing in Higher Education. *Services Marketing Quarterly*, 31(3), pp.296–319.

Williams, S.M. & Ho Wern Pei, C.-A., 1999. Corporate social disclosures by listed companies on their web sites: an international comparison. *The International Journal of Accounting*, 34(3), pp.389–419.

Willig, C., 2001. *Introducing qualitative research in psychology: Adventures in theory and method*, Buckingham: Open University Press.

Willoughby, M., Gómez, H.G. & Lozano, M.Á.F., 2010. Making e-government attractive. *Service Business*, 4(1), pp.49–62.

Wilson, D. & Valacich, J.S., 2012. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. In *Proceedings of the 33rd International Conference on Information Systems*. Orlando.

Wirtz, J., Lwin, M.O. & Williams, J.D., 2007. Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, 18(4), pp.326–348.

Wisniewski, P.J., Wilson, D.C. & Lipford, H.R., 2011. A New Social Order: Mechanisms for Social Network Site Boundary Regulation. In *Proceedings of the Seventeenth Americas Conference on Information Systems*. Detroit, MI.

Wlasuk, A., 2011. Bugs in the human hardware. *TechRepublic*. Available at: www.techrepublic.com/blog/security/bugs-in-the-human-hardware/ [Accessed July 8, 2016].

Wondracek, G., Holz, T., Kirda, E. & Kruegel, C., 2010. A practical attack to de-anonymize social network users. In *Proceedings - IEEE Symposium on Security and Privacy*. Oakland, CA, USA: IEEE, pp. 223–238.

Wu, Y., 2014. Protecting personal data in E-government: A cross-country study. *Government Information Quarterly*, 31(1), pp.150–159.

Xu, H., Dinev, T., Smith, H. & Hart, P., 2008. Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. In *Proceedings of the 29th International Conference on Information Systems*. Paris, pp. 1–16.

Xu, H., Dinev, T., Smith, J. & Hart P., 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association of Information Systems*, 12(12), pp.798–824.

Xu, H., 2007. The Effects of Self-Construal and Perceived Control on Privacy Concerns. In *Proceedings of the 28th International Conference on Information Systems*. Montreal, pp. 1–14.

Xu, H., Teo, H., Tan, B. & Agarwal, R., 2009. The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, 26(3), pp.135–173.

Yang, Y., Lutes, J., Li, F., Luo, B. & Liu, P., 2012. Stalking Online: on User Privacy in Social Networks. In *Proceedings of the Second ACM Conference on Data and Application Security and Privacy*. San Antonio, Texas, USA: ACM, pp. 37–48.

Yao, M.Z., Rice, R.E. & Wallis, K., 2007. Predicting User Concerns About Online Privacy. *Journal of the American Society for Information Science and Technology (58)5,*, 58(5), pp.710–722.

Yin, R.K., 2014. *Case Study Research: Design and Methods* 5th Edition, Sage Publications Inc.

Youn, S., 2009. Determinants of online privacy concern and its influence on privacy protection behaviours among young adolescents. *Journal of Consumer Affairs*, 43(3), pp.389 – 418.

Youn, S., 2005. Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media.*, 49(1), pp.86–110.

Young, A. & Quan-Haase, A., 2009. Information revelation and internet privacy concerns on social network sites: a case study of Facebook. In *In Proceedings of the fourth international conference on Communities and technologies ACM*. ACM, pp. 265–274.

Yousafzai, S., Pallister, J. & Foxall, G., 2009. Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, 29(5), pp.591–605.

Zhang, Y. & Wildemuth, B.M., 2009. Qualitative Analysis of Content. In B. M. Wildemuth, ed. *Applications of Social Research Method to Questions in Information and Library Science*. Westport, CT: Libraries Unlimited, pp. 308–319.

Zhao, J.J. & Zhao, S.Y., 2010. Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, 27(1), pp.49–56.

Zhao, Q., 2010. E-Government evaluation of delivering public services to citizens among cities in the Yangtze River Delta. *The International Information & Library Review*, 42(3), pp.208–211.

Zheleva, E. & Getoor, L., 2009. To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles. In *18th International Conference on World Wide Web*. ACM, pp. 531–540.

Zhou, X., 2004. E-Government in China: A Content Analysis of National and Provincial Web Sites. *Journal of Computer-Mediated Communication*, 9(4). DO - 10.1111/j.1083-6101.2004.tb00297.x.

Zukowski, T. & Brown, I., 2007. Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 Annual Research Conference of the South African institute of Computer Scientist and Information Technologist on IT Research in Developing Countries*. Port Elizabeth, South Africa: ACM Press, pp. 197–204.

Zviran, M., 2008. User‘s Perspectives on Privacy in Web-Based Applications. *Journal of Computer Information Systems*, 48(4), pp.97–105.

Zwick, D. & Dholakia, N., 2004. Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing. *Journal of Macromarketing*, 24(1), pp.31–43.

Appendix A: Initial research questions

RQ1.	What personal information of employees, if any, is publicly available on organisational websites?
RQ2.	What does online organisational disclosure of personal information means to employees?
RQ3.	How does obligatory disclosure have an impact on privacy of employees?
RQ4.	What are the concerns of employees, if any, when their personal information is published on organisation’s website? *Sub RQ: What steps do they take to protect their privacy?*
RQ5.	How does this situation affect their behaviour, if any, when they are online?
RQ6.	What guidelines should there be on disclosing employees’ information on organisational websites?

Appendix B: Research information sheet

School of System Engineering
Whiteknights
Reading
Berkshire
RG6 6AY
United Kingdom

Researcher (principal): Nurul Amin bin Badrul
Email: n.a.badrul@pgr.reading.ac.uk
Phone: +44 (0) 118 378 6423 | Ext. 6423
Researcher (role):Ph.D Student

Appendix A: INFORMATION SHEET

INVESTIGATION ON INTRUSION OF PRIVACY THROUGH ORGANISATIONAL DISCLOSURE

INFORMATION SHEET FOR INTERVIEW PARTICIPANTS

Thank you for showing an interest in this project. Please read this information sheet carefully before deciding whether or not to participate. If you decide to participate we thank you. If you decide not to take part there will be no disadvantage to you and we thank you for considering our request.

Why are we doing this study?

I am a PhD student at the University of Reading, United Kingdom and am conducting a research project about employees perspective on personal information disclosure on organisation website towards their privacy.

What is the purpose of the study?

This project will explore privacy issues surrounding personal information disclosures by third parties. It is interested in investigating employees' perspective on organizational disclosure towards their privacy.

Who would we like, is eligible, to participate in the study? Why have I been invited?

We are looking for participants who are employed in the government sector and are familiar with online environment.

Do I have to take part?

You may withdraw from participation in the project at any time and without any disadvantage to yourself of any kind.

What will be involved if you take part?

Should you agree to take part in this project, you will be asked to participate in a semi-structured interview that will be between 45 minutes to an hour. The interview will be recorded using an audio recording device and following this data will be transcribed for further analysis and interpretation. You may refuse to answer any question you do not wish to answer, and you may end interview at any time.

Confidentiality, storage and disposal of information

All responses will remain strictly confidential. Data collected during this study will be retained for 5 years after completing this research period in a secure location and then destroyed. The information gained will be used for the above objectives, will not be used for any other purpose and will not be recorded in excess of what is required. Any publication of these results will also maintain confidentiality and no individually identifying information will be shared. Only myself and if necessary my supervisor Prof. Shirley Williams and Dr. Karsten Lundqvist will have access to the data.

Are there any benefits/risks to taking part [e.g. health]?

There are no known or anticipated risks to you as a participant in this study.

What expenses and/or payment or equivalent be made for participation in the study?

Participants for the interviews will receive up to MYR25 for expenses.

What will the results of the study be used for?

The study findings may be presented to conferences, journals, seminars or PhD Programme Committee, only my supervisors, thesis examiners and I will have access to the data itself.

Who has reviewed the study?

This project has been reviewed by the University of Reading Research Ethics Committee and has been given a favourable opinion for conduct.

Contact details for further questions, or in the event of a complaint

If you have any questions about this project, either now or in the future, please feel free to contact:

Name: Nurul Amin bin Badrul
Telephone: +44 (0) 118 378 6423 | Ext. 6423
E-mail : n.a.badrul@pgr.reading.ac.uk
Fax :

Thank you for your help.

Appendix C: Consent form

University of Reading

Appendix B: CONSENT FORM

Consent Form

1. I have read and had explained to me by …**Nurul Amin bin Badrul**………………………..…

   the accompanying Information Sheet relating to the project on:

   Investigation on Intrusion of Privacy Through Organisational Disclosure
   ……………………………………………………………………………………………...

2. I have had explained to me the purposes of the project and what will be required of me, and any questions I have had have been answered to my satisfaction. I agree to the arrangements described in the Information Sheet in so far as they relate to my participation.

3. I understand that participation is entirely voluntary and that I have the right to withdraw from the project any time, and that this will be without detriment.

4. ***Researcher to delete (a) and (b) if GP will not be contacted, or (b) if no response from GP is required***

   ~~a) I authorise the Investigator to consult my General Practitioner, and provide their name and address details overleaf.~~

   ~~b) I authorise my General Practitioner to disclose any information which may be relevant to my proposed participation in the project.~~

5. I agree to the interview/session being video/audio taped. ***(delete if not applicable)***

6. This application has been reviewed by the University Research Ethics Committee and has been given a favourable ethical opinion for conduct.

7. I have received a copy of this Consent Form and of the accompanying Information Sheet.

   Name: ………………………………………………………………………………

   Signed: …………………………………………...………………………………

   Date: …………………………………………………….………………………

Appendix D: Demographic form

Participant Demographic Questions

For Classification Purposes Only

A. Personal Background

1 Gender: Male □ Female □ Prefer not to say□

2 Age Group: below 20 □ 20-25 □ 26-30 □ 31-35 □ 36-40 □
41-45 □ 46-50 □ 51-55 □ 56-60 □ 60 above□

3 Ethnicity: Malay □ Chinese □ Indian □ Kadazan □
Iban □ Others □ Prefer not to say □

4 Marital Status: Single □ Married □ Divorce □ Prefer not to say □

5 Highest education level: SPM / SPMV □ SKM / Cert □ STPM/ Diploma □ Degree □ Master□
PhD □ Others □

B. Employment Details

1 Working experience with government:
1-5yrs □ 6-10yrs □ 11-15yrs □ 16-20yrs □ 21-25yrs □
26-30yrs □ 31-35yrs □ Prefer not to say □

2 Working group category:
Support □ P&P □ JUSA □

3 Grade: □

4 Ministry/Dept/ Agencies: □

5 Monthly income: below RM2000 □ RM2001-RM4000 □ RM4001-RM6000 □
RM6001-RM8000 □ RM8001-RM10000 □ RM10,001 above □
Prefer not to say □

6 Employment Status
Permanent □ Contract □ Part Time □

Appendix E: Interview questions

Participants' questions (government employees)

1. Could you tell me what information is available on a government website?
2. Have you ever come across information related to employees on official organisation websites?
3. Why is information about employees published on government websites?
4. In your opinion, how do you perceive publishing employees' information on government websites?
5. Could you tell me about your information that is published on your organisation's website?
6. How do you know that your information has been published on your organisation's website?
7. What do you understand by the term 'personal information'?
8. What do you understand by 'privacy'?
9. Could you tell me about your information that is found on the Internet?
10. How do you deal with your information on the Internet?
11. Could you describe information about you that is published on your social media account?
12. Could you tell me about your concerns around your information on social media?
13. Do you think that publishing information about employees on government websites has any privacy issues? Why?
14. How does this disclosure affect your privacy?
15. Could you tell me the process of publishing your information on your organisation's website?
16. How do you describe the existing publication of personal information on government websites? Do you have any suggestions about this situation?

Commentators (Academics)

1. Could you tell me how the Malaysian Government is concerned about the issue of personal information disclosure on the Internet?
2. How is their awareness of privacy?
3. In your opinion, what do you think about the publication of employees' information on government websites?

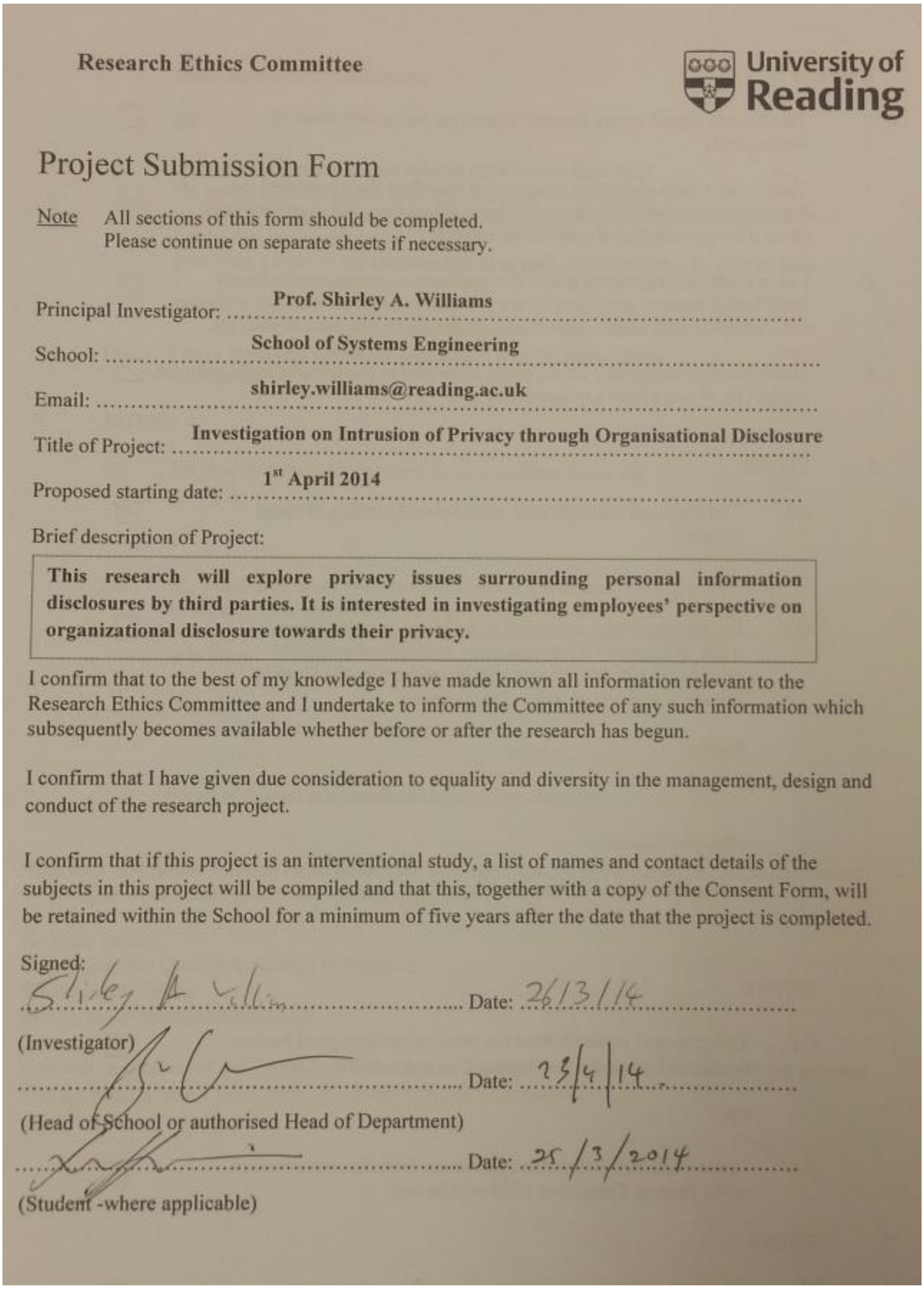
Commentator (IT Stakeholder)

1. Could you tell me the role of MAMPU in relation to government websites?
2. How important is employees' information on government websites?
3. Is there any standard regarding the publication of employees' information?

Commentator (MGPWA)

1. What is the purpose of the annual assessment of government websites?
2. What is the role of MDEC in MGPWA?
3. Could you please describe the MGPWA evaluation methodology?

Appendix F: Ethical approval



Research Ethics Committee

University of Reading

Project Submission Form

Note All sections of this form should be completed.
Please continue on separate sheets if necessary.

Principal Investigator: Prof. Shirley A. Williams

School: School of Systems Engineering

Email: shirley.williams@reading.ac.uk

Title of Project: Investigation on Intrusion of Privacy through Organisational Disclosure

Proposed starting date: 1st April 2014

Brief description of Project:

This research will explore privacy issues surrounding personal information disclosures by third parties. It is interested in investigating employees' perspective on organizational disclosure towards their privacy.

I confirm that to the best of my knowledge I have made known all information relevant to the Research Ethics Committee and I undertake to inform the Committee of any such information which subsequently becomes available whether before or after the research has begun.

I confirm that I have given due consideration to equality and diversity in the management, design and conduct of the research project.

I confirm that if this project is an interventional study, a list of names and contact details of the subjects in this project will be compiled and that this, together with a copy of the Consent Form, will be retained within the School for a minimum of five years after the date that the project is completed.

Signed:

Shirley A Willi...................... Date: 26/3/14

(Investigator)

.... Date: 23/4/14

(Head of School or authorised Head of Department)

.... Date: 25/3/2014

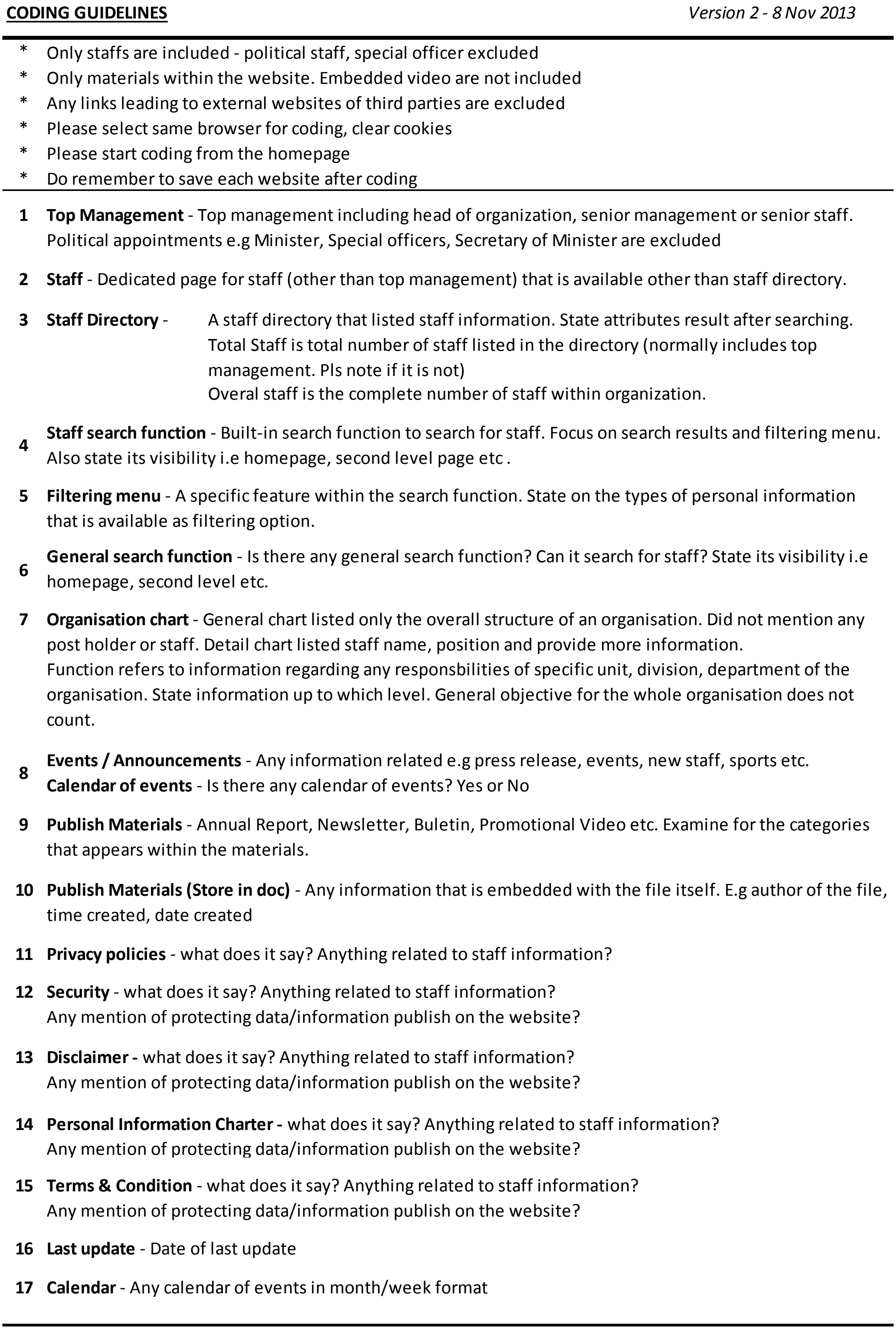
(Student -where applicable)

Appendix G: Coding scheme

a. Coding category

Category	Definition	Example
Personal Information	Information that could be directly related or associated with an individual	Full name, photographic image (name related), gender (inferred by photo), personal ID number
Personal Achievement	Information about specific acomplishment and success	Education qualification, award
Employent Information	Information about full time work	Position, working grade, work scope, salary
Contact Information	Information that could be used to (directly) communicate with an individual	Email, telephone number, fax number
Geographical	Information regarding the specific location of individual	Postal address, location map, direction to address
Timeliness	Information regarding when any event or activities occur or references to specific time	Today, tomorrow, last week, date

b. Coding guideline



CODING GUIDELINES *Version 2 - 8 Nov 2013*

* Only staffs are included - political staff, special officer excluded
* Only materials within the website. Embedded video are not included
* Any links leading to external websites of third parties are excluded
* Please select same browser for coding, clear cookies
* Please start coding from the homepage
* Do remember to save each website after coding

1 **Top Management** - Top management including head of organization, senior management or senior staff. Political appointments e.g Minister, Special officers, Secretary of Minister are excluded

2 **Staff** - Dedicated page for staff (other than top management) that is available other than staff directory.

3 **Staff Directory** - A staff directory that listed staff information. State attributes result after searching.
Total Staff is total number of staff listed in the directory (normally includes top management. Pls note if it is not)
Overal staff is the complete number of staff within organization.

4 **Staff search function** - Built-in search function to search for staff. Focus on search results and filtering menu. Also state its visibility i.e homepage, second level page etc .

5 **Filtering menu** - A specific feature within the search function. State on the types of personal information that is available as filtering option.

6 **General search function** - Is there any general search function? Can it search for staff? State its visibility i.e homepage, second level etc.

7 **Organisation chart** - General chart listed only the overall structure of an organisation. Did not mention any post holder or staff. Detail chart listed staff name, position and provide more information.
Function refers to information regarding any responsbilities of specific unit, division, department of the organisation. State information up to which level. General objective for the whole organisation does not count.

8 **Events / Announcements** - Any information related e.g press release, events, new staff, sports etc.
Calendar of events - Is there any calendar of events? Yes or No

9 **Publish Materials** - Annual Report, Newsletter, Buletin, Promotional Video etc. Examine for the categories that appears within the materials.

10 **Publish Materials (Store in doc)** - Any information that is embedded with the file itself. E.g author of the file, time created, date created

11 **Privacy policies** - what does it say? Anything related to staff information?

12 **Security** - what does it say? Anything related to staff information?
Any mention of protecting data/information publish on the website?

13 **Disclaimer -** what does it say? Anything related to staff information?
Any mention of protecting data/information publish on the website?

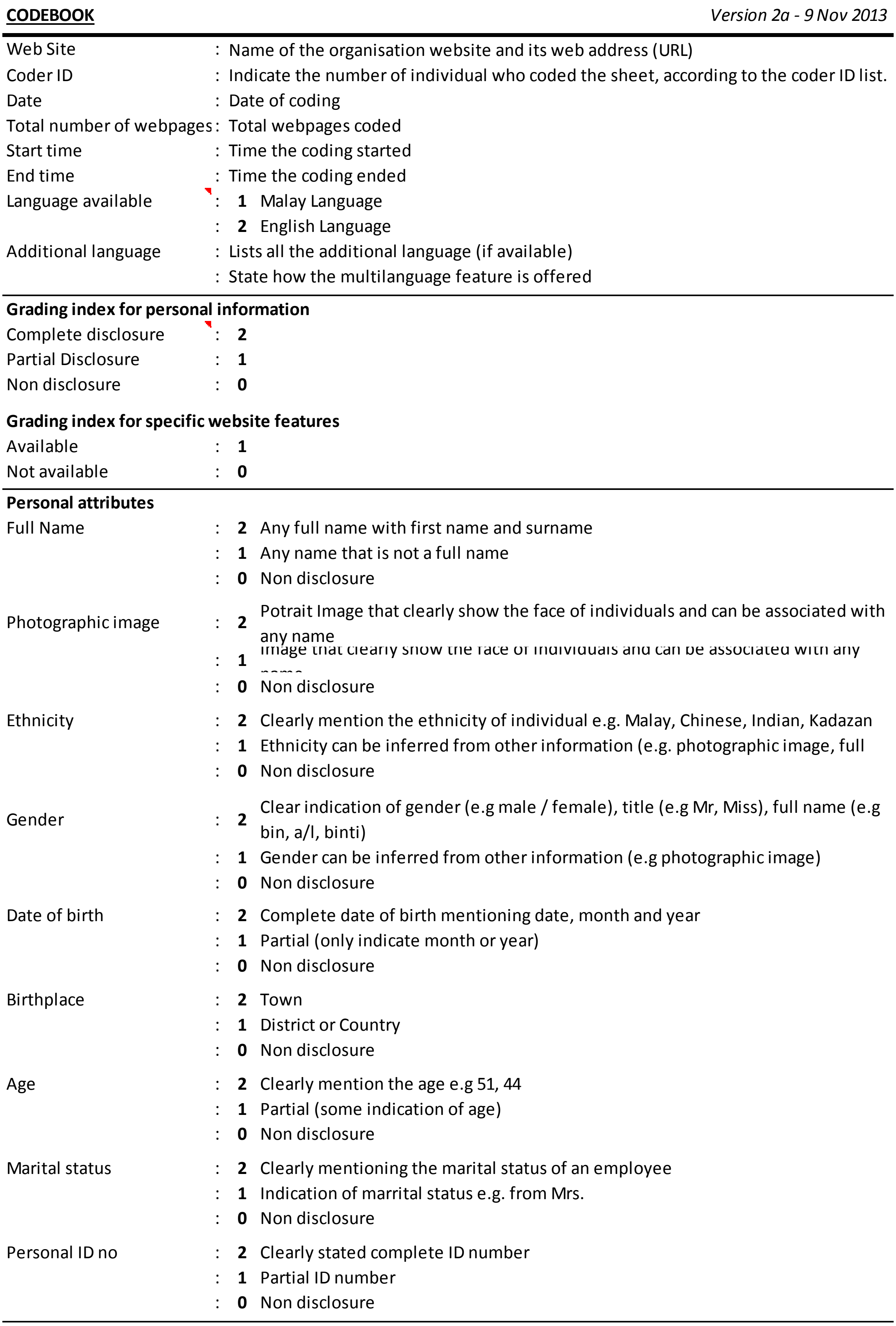
14 **Personal Information Charter -** what does it say? Anything related to staff information?
Any mention of protecting data/information publish on the website?

15 **Terms & Condition** - what does it say? Anything related to staff information?
Any mention of protecting data/information publish on the website?

16 **Last update** - Date of last update

17 **Calendar** - Any calendar of events in month/week format

c. Code book



CODEBOOK *Version 2a - 9 Nov 2013*

Web Site	:	Name of the organisation website and its web address (URL)	
Coder ID	:	Indicate the number of individual who coded the sheet, according to the coder ID list.	
Date	:	Date of coding	
Total number of webpages	:	Total webpages coded	
Start time	:	Time the coding started	
End time	:	Time the coding ended	
Language available	:	**1**	Malay Language
	:	**2**	English Language
Additional language	:	Lists all the additional language (if available)	
	:	State how the multilanguage feature is offered	
Grading index for personal information			
Complete disclosure	:	**2**	
Partial Disclosure	:	**1**	
Non disclosure	:	**0**	
Grading index for specific website features			
Available	:	**1**	
Not available	:	**0**	
Personal attributes			
Full Name	:	**2**	Any full name with first name and surname
	:	**1**	Any name that is not a full name
	:	**0**	Non disclosure
Photographic image	:	**2**	Potrait Image that clearly show the face of individuals and can be associated with any name
	:	**1**	image that clearly show the face of individuals and can be associated with any name
	:	**0**	Non disclosure
Ethnicity	:	**2**	Clearly mention the ethnicity of individual e.g. Malay, Chinese, Indian, Kadazan
	:	**1**	Ethnicity can be inferred from other information (e.g. photographic image, full
	:	**0**	Non disclosure
Gender	:	**2**	Clear indication of gender (e.g male / female), title (e.g Mr, Miss), full name (e.g bin, a/l, binti)
	:	**1**	Gender can be inferred from other information (e.g photographic image)
	:	**0**	Non disclosure
Date of birth	:	**2**	Complete date of birth mentioning date, month and year
	:	**1**	Partial (only indicate month or year)
	:	**0**	Non disclosure
Birthplace	:	**2**	Town
	:	**1**	District or Country
	:	**0**	Non disclosure
Age	:	**2**	Clearly mention the age e.g 51, 44
	:	**1**	Partial (some indication of age)
	:	**0**	Non disclosure
Marital status	:	**2**	Clearly mentioning the marital status of an employee
	:	**1**	Indication of marrital status e.g. from Mrs.
	:	**0**	Non disclosure
Personal ID no	:	**2**	Clearly stated complete ID number
	:	**1**	Partial ID number
	:	**0**	Non disclosure

Personal achievement			
Qualification	:	**2**	Clearly mentioning the institution, course, year of qualification
	:	**1**	Partial (any indication of qualification) e.g from title Dr.
	:	**0**	Non disclosure
Awards	:	**2**	Clearly mentioning the date of awarded, name of the award and presented by
	:	**1**	Partial (any indication of qualification)
	:	**0**	Non disclosure
Employment Information			
Position	:	**2**	Clearly stated position held in organisation with reference to Unit/Division (e.g Director of Admin, Assistant Officer of Procurement)
	:	**1**	Stated position held within organisation
	:	**0**	Non disclosure
Grade	:	**2**	Clearly stated the working grade of employee (e.g DG41)
	:	**1**	Partially stated the grade or hierarchy in the organization (e.g only DG or Grade
	:	**0**	Non disclosure
Salary	:	**2**	Clearly stated the salary
	:	**1**	Partial salary (e.g range of salary)
	:	**0**	Non disclosure
Work scope	:	**2**	Stated the role and responsibilities of an individual
	:	**1**	Stated the role and responsibilities of a unit / division of an individual
	:	**0**	Non disclosure
Contact Information			
Email address	:	**2**	personal email address
	:	**1**	official email address. General email address excluded
	:	**0**	Non disclosure
Telephone number	:	**2**	Handphone number to contact individuals
	:	**1**	Dedicated landline number to contact individuals including extensions
	:	**0**	Non disclosure
Fax no	:	**2**	Direct fax number
	:	**1**	General fax number
	:	**0**	Non disclosure
Geographical Information			
Physical address	:	**2**	Complete postal address of organization with map
	:	**1**	Complete postal address of organization
	:	**0**	Non disclosure
Direction	:	**2**	Complete direction to organization with information of parking, public
	:	**1**	Any direction to organization (e.g map with direction)
	:	**0**	Non disclosure
Location	:	**2**	Accuracy up to level or block
	:	**1**	Accuracy up to building / complex
	:	**0**	Non disclosure
Timeliness			
Before	:	**2**	Complete information before events / activities occur (time, date)
	:	**1**	Any information related to time before it occurs (next month, this afternoon, last
	:	**0**	Non disclosure
After	:	**2**	Complete information after any events / activities occured (time, date)
	:	**1**	Any information related to time after it happened (next month, this afternoon,
	:	**0**	Non disclosure
Opening hours	:	**2**	Clearly stated opening hours, lunch break, working day
	:	**1**	Partial information of above
	:	**0**	Non disclosure

Specific website features			
Staff directory	:	**1**	How to access it? Home page, 2nd level, 3rd level? Please code personal information available.
	:	**0**	Not available
Staff search function	:	**1**	How to access it? Home page, 2nd level, 3rd level?
	:	**0**	Not available
Filtering menu	:	**1**	Please code personal information on the filtering menu
	:	**0**	Not available
General search function	:	**1**	How to access it? Home page, 2nd level, 3rd level? Can it be used to search staff?
	:	**0**	Not available
Organisation Chart	:	**1**	Is it a general chart or detail chart? If detail chart, please code personal information available.
	:	**0**	Not available
Privacy policies	:	**1**	What is stated? How does it relate to information about employees?
	:	**0**	Not available
Security policies	:	**1**	What is stated? How does it relate to information about employees?
	:	**0**	Not available
Disclaimer	:	**1**	What is stated? How does it relate to information about employees?
	:	**0**	Not available
Personal information chart	:	**1**	What is stated? How does it relate to information about employees?
	:	**0**	Not available
Terms and conditions	:	**1**	What is stated? How does it relate to information about employees?
	:	**0**	Not available
Date of last update	:	**1**	State the date of last updated
	:	**0**	Not available
Calendar	:	**1**	Investigate the feature for any information of events or announcement
	:	**0**	Not available

d. Coding form

CODING FORM

Part 1 - Direct website analysis
Web Site ____________________
Total no of web pages _________
Coder ________________________
Date _________________________

Start time: ________________________________
End time: _________________________________
Language Available : _______________________
Additional language: _______________________

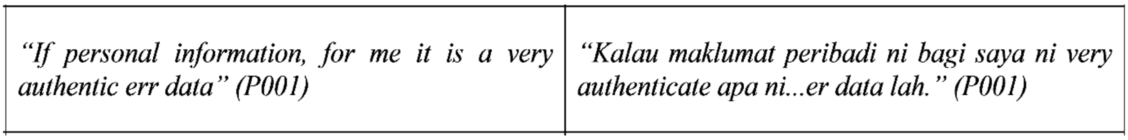
	Personal Attributes									Personal Achievement		Employment Information				Contact Information			Location Information			Timeliness		
	Full Name	Photographic Image	Ethnicity	Gender	Date of birth	Birthplace	Age	Maritalstatus	Personal ID No	Qualification	Award	Position	Grade	Salary	Work Scope	Email address	Tel No	Fax No	Physicaladdress	Direction	Location	Before	After	Opening hours
Disclosure (Y/N)																								
A Top Management																								
How many disclosed? _____																								
B Staff																								
How many disclosed? _____																								
C Staff Directory																								
How many disclosed? _____																								
Total of staff _____																								
Overall staff _____																								
D Staff Search Function																								
a. Access - Homepage or ?																								
b. Filtering menu																								
E General Search Function																								
a. Access - Homepage or ?																								
b. Ability to search for staff																								
F Organization																								
a. General Chart																								
b. Detail Org Chart																								
c. Function of Dept/Unit																								

Coding form (continue)

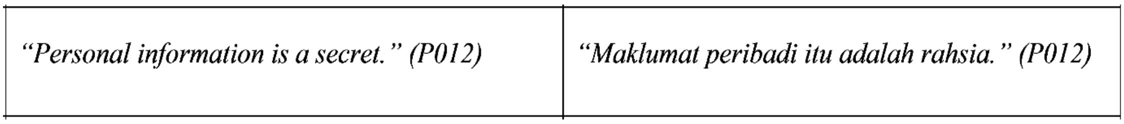
G Events/Announcements																								
a. Calendar of Events																								
H Publish Materials (In Content)																								
I Publish Materials (Store in doc)																								
J Privacy policies																								
K Security policies																								
L Disclaimer																								
M Personal Information Charter																								
N Terms & Condition																								
O Date of last update																								
P Calendar																								

Appendix H: List of interview quotations

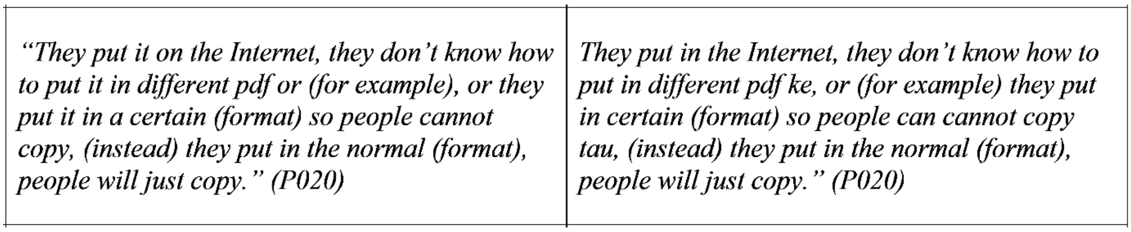
Below is a list of all the quotes and where they can be found in the thesis. Also included here are the quotes which are not included in the main body of the thesis.



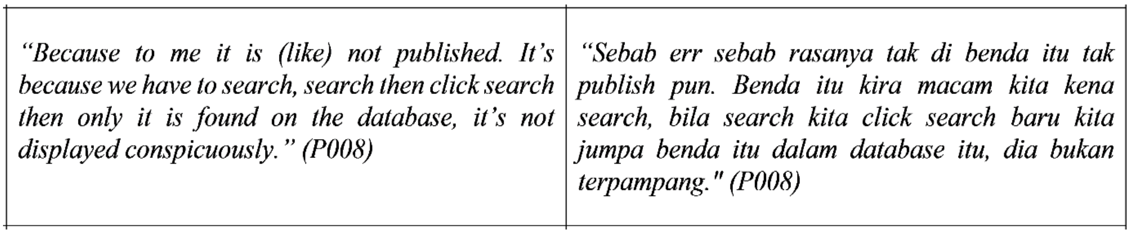
"If personal information, for me it is a very authentic err data" (P001)	*"Kalau maklumat peribadi ni bagi saya ni very authenticate apa ni...er data lah." (P001)*



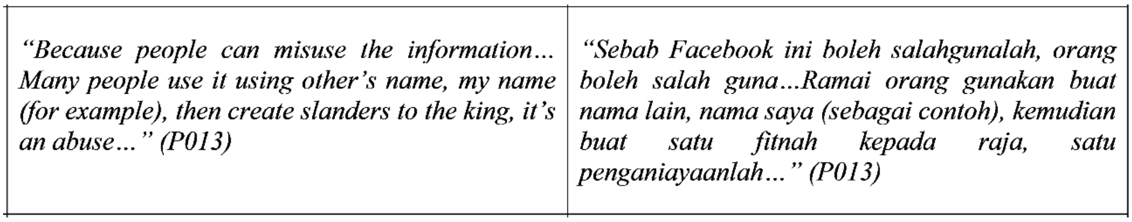
"Personal information is a secret." (P012)	*"Maklumat peribadi itu adalah rahsia." (P012)*



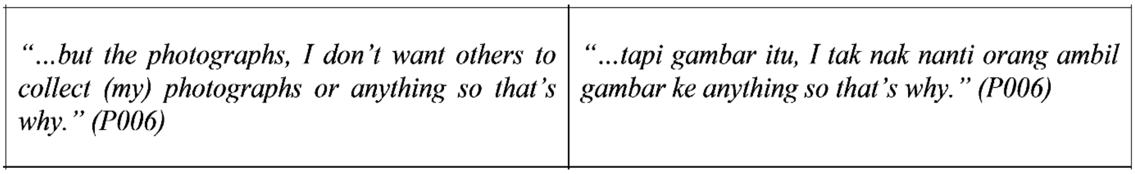
"They put it on the Internet, they don't know how to put it in different pdf or (for example), or they put it in a certain (format) so people cannot copy, (instead) they put in the normal (format), people will just copy." (P020)	*They put in the Internet, they don't know how to put in different pdf ke, or (for example) they put in certain (format) so people can cannot copy tau, (instead) they put in the normal (format), people will just copy." (P020)*



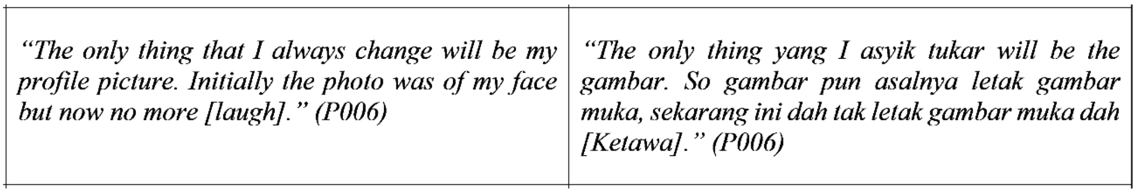
"Because to me it is (like) not published. It's because we have to search, search then click search then only it is found on the database, it's not displayed conspicuously." (P008)	*"Sebab err sebab rasanya tak di benda itu tak publish pun. Benda itu kira macam kita kena search, bila search kita click search baru kita jumpa benda itu dalam database itu, dia bukan terpampang." (P008)*



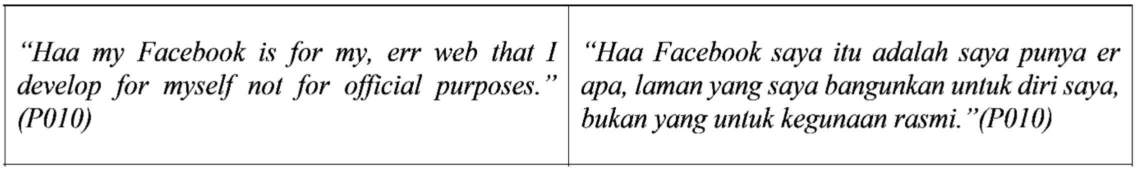
"Because people can misuse the information... Many people use it using other's name, my name (for example), then create slanders to the king, it's an abuse..." (P013)	*"Sebab Facebook ini boleh salahgunalah, orang boleh salah guna...Ramai orang gunakan buat nama lain, nama saya (sebagai contoh), kemudian buat satu fitnah kepada raja, satu penganiayaanlah..." (P013)*



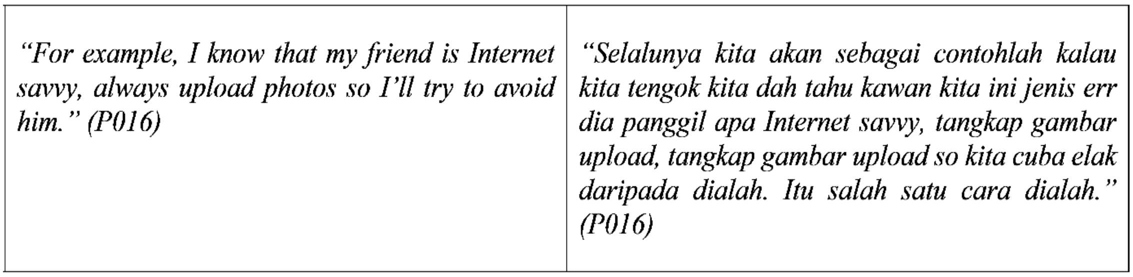
"...but the photographs, I don't want others to collect (my) photographs or anything so that's why." (P006)	*"...tapi gambar itu, I tak nak nanti orang ambil gambar ke anything so that's why." (P006)*



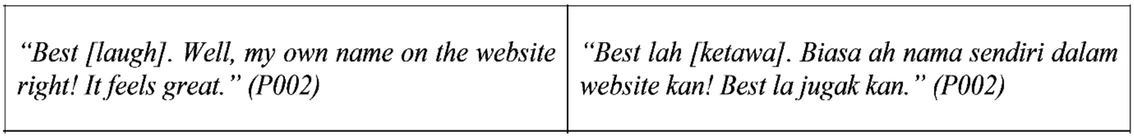
"The only thing that I always change will be my profile picture. Initially the photo was of my face but now no more [laugh]." (P006)	*"The only thing yang I asyik tukar will be the gambar. So gambar pun asalnya letak gambar muka, sekarang ini dah tak letak gambar muka dah [Ketawa]." (P006)*



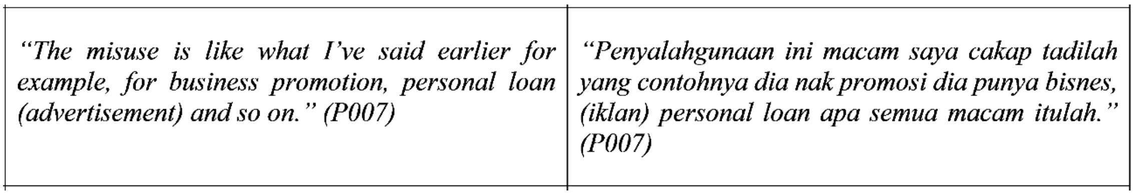
"Haa my Facebook is for my, err web that I develop for myself not for official purposes." (P010)	*"Haa Facebook saya itu adalah saya punya er apa, laman yang saya bangunkan untuk diri saya, bukan yang untuk kegunaan rasmi."(P010)*



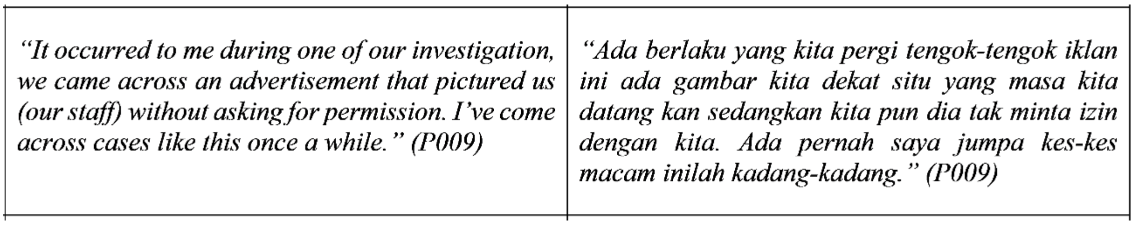
"For example, I know that my friend is Internet savvy, always upload photos so I'll try to avoid him." (P016)	*"Selalunya kita akan sebagai contohlah kalau kita tengok kita dah tahu kawan kita ini jenis err dia panggil apa Internet savvy, tangkap gambar upload, tangkap gambar upload so kita cuba elak daripada dialah. Itu salah satu cara dialah." (P016)*



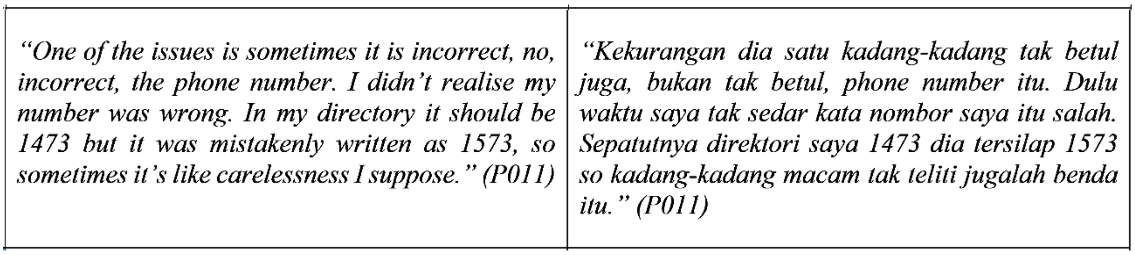
"Best [laugh]. Well, my own name on the website right! It feels great." (P002)	*"Best lah [ketawa]. Biasa ah nama sendiri dalam website kan! Best la jugak kan." (P002)*



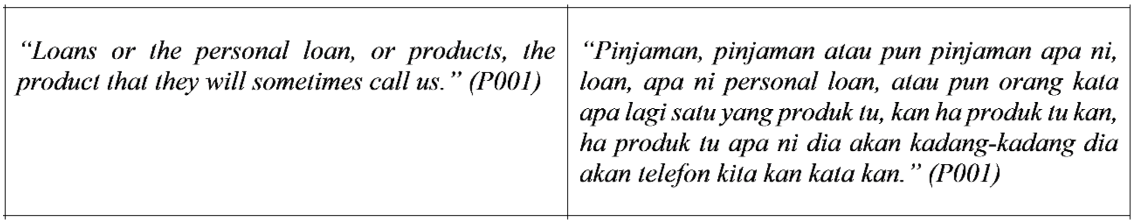
"The misuse is like what I've said earlier for example, for business promotion, personal loan (advertisement) and so on." (P007)	*"Penyalahgunaan ini macam saya cakap tadilah yang contohnya dia nak promosi dia punya bisnes, (iklan) personal loan apa semua macam itulah." (P007)*



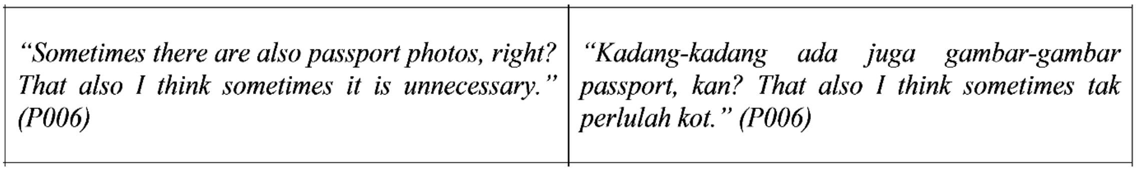
"It occurred to me during one of our investigation, we came across an advertisement that pictured us (our staff) without asking for permission. I've come across cases like this once a while." (P009)	*"Ada berlaku yang kita pergi tengok-tengok iklan ini ada gambar kita dekat situ yang masa kita datang kan sedangkan kita pun dia tak minta izin dengan kita. Ada pernah saya jumpa kes-kes macam inilah kadang-kadang." (P009)*



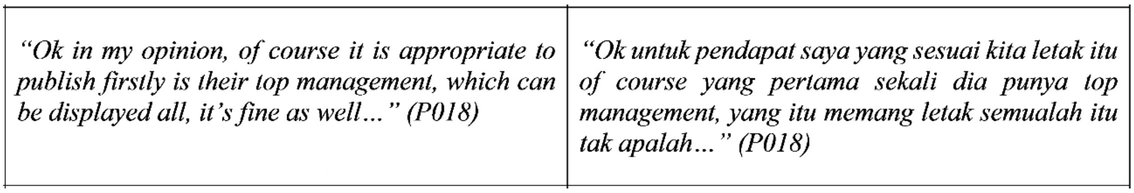
"One of the issues is sometimes it is incorrect, no, incorrect, the phone number. I didn't realise my number was wrong. In my directory it should be 1473 but it was mistakenly written as 1573, so sometimes it's like carelessness I suppose." (P011)	*"Kekurangan dia satu kadang-kadang tak betul juga, bukan tak betul, phone number itu. Dulu waktu saya tak sedar kata nombor saya itu salah. Sepatutnya direktori saya 1473 dia tersilap 1573 so kadang-kadang macam tak teliti jugalah benda itu." (P011)*



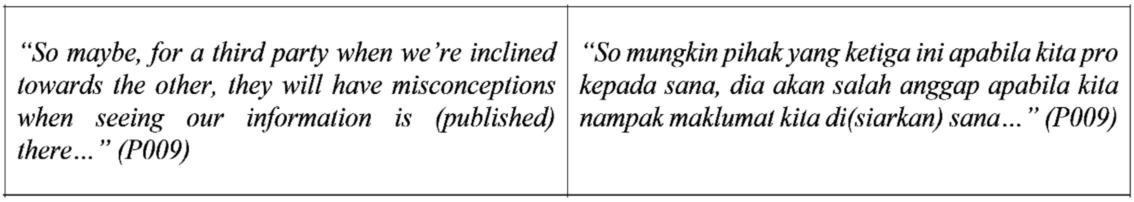
"Loans or the personal loan, or products, the product that they will sometimes call us." (P001)	*"Pinjaman, pinjaman atau pun pinjaman apa ni, loan, apa ni personal loan, atau pun orang kata apa lagi satu yang produk tu, kan ha produk tu kan, ha produk tu apa ni dia akan kadang-kadang dia akan telefon kita kan kata kan." (P001)*



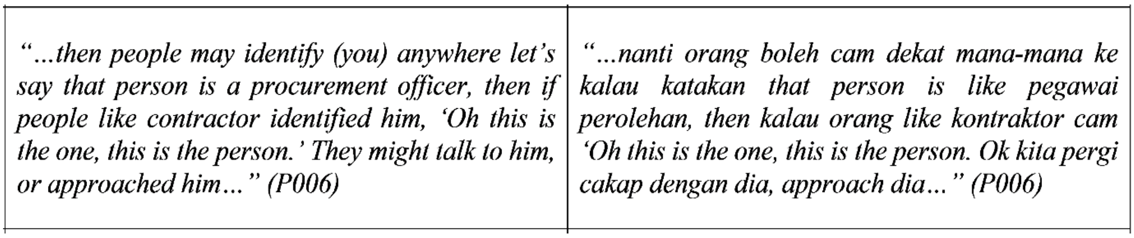
"Sometimes there are also passport photos, right? That also I think sometimes it is unnecessary." (P006)	*"Kadang-kadang ada juga gambar-gambar passport, kan? That also I think sometimes tak perlulah kot." (P006)*



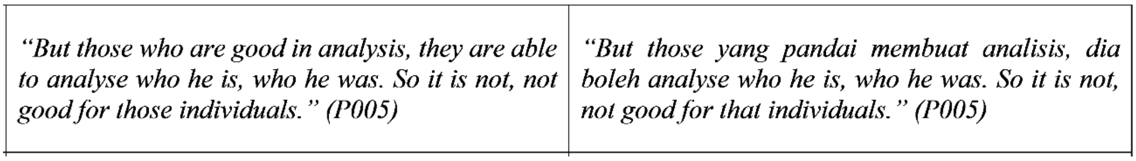
"Ok in my opinion, of course it is appropriate to publish firstly is their top management, which can be displayed all, it's fine as well…" (P018)	*"Ok untuk pendapat saya yang sesuai kita letak itu of course yang pertama sekali dia punya top management, yang itu memang letak semualah itu tak apalah…" (P018)*



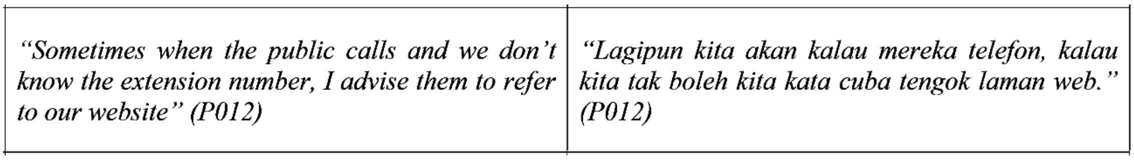
"So maybe, for a third party when we're inclined towards the other, they will have misconceptions when seeing our information is (published) there…" (P009)	*"So mungkin pihak yang ketiga ini apabila kita pro kepada sana, dia akan salah anggap apabila kita nampak maklumat kita di(siarkan) sana…" (P009)*



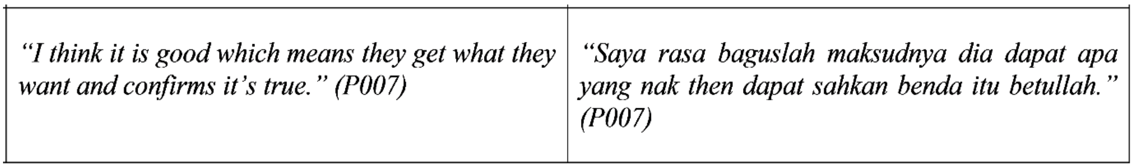
"...then people may identify (you) anywhere let's say that person is a procurement officer, then if people like contractor identified him, 'Oh this is the one, this is the person.' They might talk to him, or approached him..." (P006)	*"...nanti orang boleh cam dekat mana-mana ke kalau katakan that person is like pegawai perolehan, then kalau orang like kontraktor cam 'Oh this is the one, this is the person. Ok kita pergi cakap dengan dia, approach dia..." (P006)*



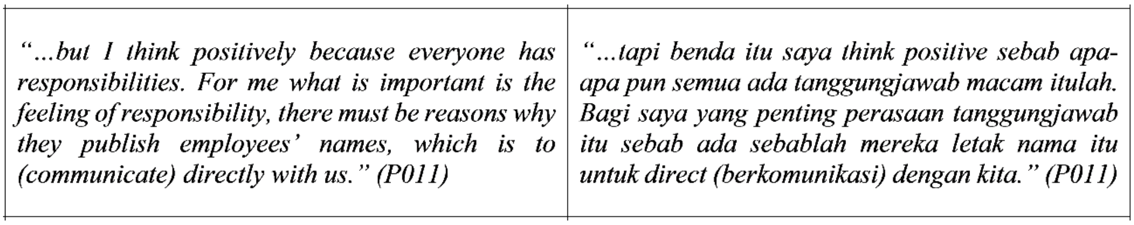
"But those who are good in analysis, they are able to analyse who he is, who he was. So it is not, not good for those individuals." (P005)	*"But those yang pandai membuat analisis, dia boleh analyse who he is, who he was. So it is not, not good for that individuals." (P005)*



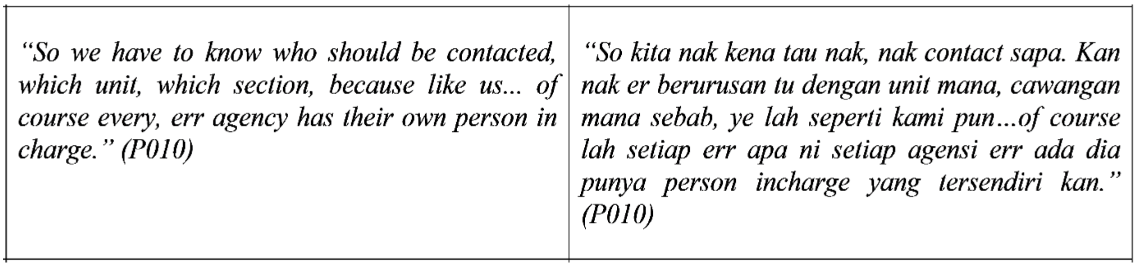
"Sometimes when the public calls and we don't know the extension number, I advise them to refer to our website" (P012)	*"Lagipun kita akan kalau mereka telefon, kalau kita tak boleh kita kata cuba tengok laman web." (P012)*



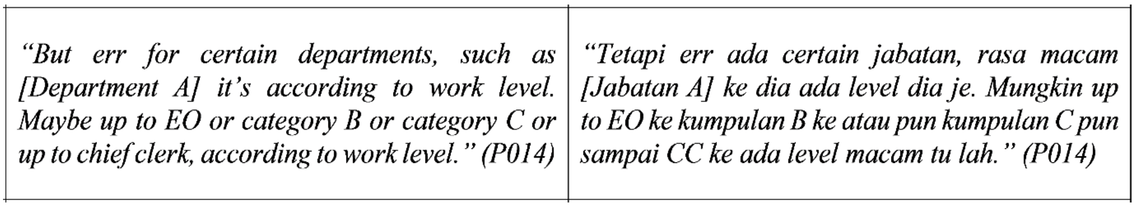
"I think it is good which means they get what they want and confirms it's true." (P007)	*"Saya rasa baguslah maksudnya dia dapat apa yang nak then dapat sahkan benda itu betullah." (P007)*



"...but I think positively because everyone has responsibilities. For me what is important is the feeling of responsibility, there must be reasons why they publish employees' names, which is to (communicate) directly with us." (P011)	*"...tapi benda itu saya think positive sebab apa-apa pun semua ada tanggungjawab macam itulah. Bagi saya yang penting perasaan tanggungjawab itu sebab ada sebablah mereka letak nama itu untuk direct (berkomunikasi) dengan kita." (P011)*



"So we have to know who should be contacted, which unit, which section, because like us... of course every, err agency has their own person in charge." (P010)	*"So kita nak kena tau nak, nak contact sapa. Kan nak er berurusan tu dengan unit mana, cawangan mana sebab, ye lah seperti kami pun...of course lah setiap err apa ni setiap agensi err ada dia punya person incharge yang tersendiri kan." (P010)*



"But err for certain departments, such as [Department A] it's according to work level. Maybe up to EO or category B or category C or up to chief clerk, according to work level." (P014)	*"Tetapi err ada certain jabatan, rasa macam [Jabatan A] ke dia ada level dia je. Mungkin up to EO ke kumpulan B ke atau pun kumpulan C pun sampai CC ke ada level macam tu lah." (P014)*