Consumer Education on Digital Privacy:

Examining the Communication of Privacy Issues in Contemporary Digital Literacy Campaigns across the Globe

Student Name: Xiang Zhang
Student Number: 423296

Supervisor: Dr. Payal Arora

Master Media Studies: Media & Business
Erasmus School of History, Culture and Communication
Erasmus University Rotterdam

Master Thesis
June 22th, 2016

Consumer Education on Digital Privacy:
Examining the Communication of Privacy Issues in Contemporary
Digital Literacy Campaigns across the Globe

ABSTRACT

Abstract. Digital technologies are increasingly threatening consumer's right to privacy, in spite of the conveniences they have brought. Besides corporations and governments invading consumer privacy, there are numerous malicious actors compromising consumers' personal information. In spite of this, today's consumers do not possess sufficient knowledge and skills to tackle the rising risks posed on their digital privacy. The inadequacy of consumer privacy literacy combined with the growth of digital privacy risks has sparked the urgency for privacy education. However, to date, few studies have investigated this important arena of privacy education through digital literacy campaigns. Hence, this thesis critically examines the range of communication actors and processes involved in contemporary campaigns across the globe designed to educate consumers on privacy issues.

Qualitative content analysis is conducted on selected digital literacy campaigns from four different countries. The thesis comparatively analyzes the websites and social media activity of these campaigns to gauge the global approach to privacy literacy and the range of communication strategies employed to reach their consumers. The findings reveal that contemporary campaigns educate consumers across different media channels by communicating digital privacy risks initiated by companies, governments and malicious individuals and risk-coping solutions that contain privacy protection measures and demands for better protection of privacy rights. Among these campaigns, public education campaigns backed by governments differ from privacy activism campaigns driven by non-profits in terms of the scope of privacy issues, their interpretations of privacy and their positioning of the relationship between consumers and companies. Based on the findings, the thesis provides important implications that future global campaigns should focus on the communication of privacy risks and risk-coping solutions while using more interactive features on social media for engagement. The thesis further argues that the existing dimensions of digital privacy literacy needs to be expanded.

KEYWORDS: *Digital literacy, Consumer digital privacy, Privacy education, Cyber security, Privacy activism, Social media engagement*

Table of Contents

1. Introduction

As consumers are increasingly going online nowadays due to the unprecedented convenience brought by new technologies, they have been troubled and frustrated by various privacy concerns at the same time. The convenience therefore comes with a price. Threats to consumer's right to privacy are escalating, with advanced technologies available for businesses and governments to invade consumer digital privacy (Klitou, 2014). New media platforms, especially today's prevalent social networking sites, have led to increased interconnectivity and concentration of relationships while fostering information sharing among Internet users (Houghton, & Joinson, 2010). As a result of the increase in information sharing on social media, a considerable amount of personal information is circulating online. On Facebook, one of the leading social networking sites, with more than 1.65 billion monthly active users (MAUs) as of April 2016, there are around 300 million photo uploads every single day, while 4.75 billion pieces of content were shared on a daily basis as of May 2013 (Zephoria, 2016). The massive information posted by consumers is not only accessible to companies and governments but often, also available to any information seeker who has access to the Internet.

Consumer digital privacy is therefore under potential abuse when the Internet becomes a ubiquitous commodity, sparking unprecedented privacy concerns among consumers. In European Union (EU), 84% of Internet users felt worried about their privacy (Eurobarometer, 2010). According to Pew Research Center, 91% of adults in the US agreed that "consumers have lost control over how personal information is collected and used by companies", while 81% of parents expressed concerns towards advertisers' access to information about their children's online behaviors (Madden, 2015a). The majority of American adults are concerned about their personal data, but few Americans have made significant changes to their privacy and security behaviors. Around 54% Americans expressed difficulty in strengthening privacy protections (Madden, 2015b). Consumer privacy has become much more vulnerable in the digital era due to the growing capabilities of governments and businesses to invade the privacy of consumers, facilitated by the Internet (Mendel, Puddephatt, Wagner, Hawtin, & Torres, 2012).

Consumers' concerns over the vulnerability of digital privacy and their expressed difficulty regarding management of information online both largely result from their insufficiency of privacy literacy. With respect to awareness of institutional practices, most consumers are found to be lacking

sufficient knowledge of basic surveillance practices on websites (Park, 2011). In spite of a high penetration of electronic devices into people's daily life, consumers surveyed in the study of Park and Jang (2014) possess inadequate mobile-based privacy literacy, e.g., understanding of locational privacy and awareness of privacy threats in mobile use, with less than half of them equipped with basic information-related and location-related privacy knowledge and skills. The current challenge highlights the importance of studying consumer digital privacy and particularly emphasizes the urgency of educating consumers on such privacy issues.

In terms of the growing data collection nowadays, governments are one of the major information "trackers". As certain information is necessary for crime investigation or counter-terrorism purposes, governments usually are given legitimate access to consumer data and have compelling reasons for collecting such data (Solove, 2002b). However, it is unknown whether the data collected is abused or misused for purposes other than purely investigating crimes or countering terrorism. It is where the contradiction between national security and individual privacy comes in, epitomized by the recent heatedly debated Apple-FBI dispute. The FBI wanted to gain access to the iPhone of a shooter in the San Bernardino shooting, which was rejected by Apple (The New York Times, 2016). The FBI further issued a court order for the request, as it is usually a method to force companies to provide the access when they refuse to cooperate (Solove, 2002b). However, Apple supporters and privacy advocates claim that FBI's request violates the right to privacy and makes future government data collection easier (Solove, 2002b; The New York Times, 2016). The FBI and privacy advocates stand on opposite sides in the security-privacy debate, with the former for national security and the latter for individual privacy. Governments and privacy advocacy groups seem to have different interpretations towards privacy. As both sides engage in educating consumers on privacy issues (Van Hamel, 2011), it is of strong societal relevance to dive into how their privacy education initiatives vary from each other, which this thesis explores in depth.

Although Apple has refused to cooperate with the government, it cannot be denied that the company itself exercises tremendous power over consumer data by storing and having access to a huge amount of personal information of its consumers. In that sense, companies are also information "trackers". Other companies that center on consumer information, such as the omniscient Internet service providers (ISPs) and online marketers, also involve in collecting and storing of consumer data in their databases (Ashworth, & Free, 2006; Barnes, 2006; Strufe, 2009). Online marketing

technologies like cookies help marketers generate a huge dataset at a low cost by enabling them to track consumer information on spending patterns and preferences, which consumers can hardly avoid or detect (Ashworth, & Free, 2006).

However, consumers are suffering from even more digital privacy risks beyond those posed by governments and companies as mentioned. There have been an increasing number of malicious individuals, who are ready to steal personal information of consumers, out there on the Internet, with the help of malware or other tools in their hands. Consumer privacy is thus under threats of activities, such as identity theft, phishing, malware infection and so forth, conducted by those malicious individuals (Aimeur, Gambs, & Ho, 2010). According to the report by Sophos (2011), 43 and 40 percent of social networking site (SNS) users had been suffering from phishing and malware respectively by the end of 2010. Ransomware that is a type of malware has become one of the biggest cyber security threats in the first quarter of 2016, as nearly 2,900 new ransomware malware modifications were detected and the number of users who suffered from the high-profile attack increased by 30 percent compared to the previous quarter (Palmer, 2016).

Due to the huge volume of digital privacy risks posed by governments, companies and malicious individuals, it is high time that consumers should be made aware of current privacy risks and should develop necessary skills to protect their personal information against those risks. Digital literacy campaigns that aim to strengthen consumer privacy competencies thus are an important effort in the tackling of various privacy risks and should be placed in the frontline of contemporary studies. Previous research highlights the urgency for digital literacy initiatives on educating consumers on privacy issues (Dommeyer, & Gross, 2003; Nowak, & Phelps, 1992; Park, & Jang, 2014). Although there are already numerous digital literacy initiatives out there to raise consumer awareness of privacy issues (Van Hamel, 2011), few studies explore the diverse efforts deeply, systematically and cross-culturally. Thereby, this thesis embarks to fill the gap by critically examining these initiatives to guide policy makers, academics and corporations on the nature of such campaigns and their diversity and potential impact on consumers. Clearly, while digital literacy nowadays is of fundamental importance, there is a serious lag among consumers in the understanding of such matters.

Literacy is regarded by Pool as “one of the most fundamental human conditions in diffusing democratic potentials” (as cited in Park, 2011, p. 2). The core of literacy lies in reading and writing, but beyond that, it also relates to the management of information disseminated through different

media channels (Summey, 2013). In the 21st century, with the development of information and communications technologies (ICTs), literacy has become more intertwined with technology. A new set of literacy skills expand the boundaries of traditional literacy, with digital literacy as an indispensable part of the cohort. It is highly important for netizens to take good care of their information and communication online, since the Internet has significantly increased the threat to consumer privacy in terms of data tracking and collection (Hans, 2012). Therefore, digital literacy is about building people's knowledge on how to protect their privacy, with privacy literacy as an essential component of digital literacy. Digital privacy literacy refers to the extent to which Internet users are familiar with technical aspects of the Internet, aware of common institutional practices and understand current privacy policy (Park, 2011). There is a lack of legal protection of consumers' information, and they are worried about losing control of such information (Earp, & Baumer, 2003). Hence, digital literacy is critical for consumers to "survive" in the digital era because it enables them to perform basic tasks properly online and more importantly to avoid the spectrum of potential abuse of their personal information (Eshet-Alkalai, 2004; Park, 2011). The study of digital literacy with an emphasis on privacy literacy comes in a timely manner when consumers are living in a digital world haunted by a host of privacy concerns.

An important aspect of digital privacy literacy relates to the understanding of Terms and Conditions and privacy policies (Park, 2011). Terms and Conditions are online agreements that not only grant companies' permission to access personal information but also foster information flows between businesses and governments after a small click on "agree" (Hoback, Ramos, & Khanna, 2013; Solove, 2002b). The documentary "Terms and Conditions may apply" of Hoback et al. (2013) has shed light on how deeply problematic Terms and Conditions are and how those online agreements has cast threats on consumer digital privacy. However, Terms and Conditions are more complicated than the question of clicking or not clicking on "agree". Dilemmas exist for both companies and consumers. On the side of companies, they realize the need to respect consumer's right to privacy but at the same time have to drive profits and consider their own interests facilitated by consumer information. For consumers, they expect benefits, such as access to websites, use of services and monetary compensation, from companies but meanwhile are concerned about the handling of their personal data (Ashworth, & Free, 2006; Madden, 2015a). However, most consumers have to sacrifice their personal data in exchange of free service, and the trade-off is costly, which puts consumers in unpredictable

vulnerability by giving “companies control over your data, prose, pictures, personal information and even your freedom to simply quit a given website” (Melber, Hartzog, & Selinger, 2013).

As pointed out by Solove (2008), a possible reason why consumers surrender personal information to companies is that they have insufficient knowledge about how their data will be used in the future, and part of the existing privacy problem comes from their inability to assess potential risks concerning privacy. Therefore, their digital privacy literacy regarding understanding Terms and Conditions is also considered low. According to The Guardian, only 7% of British citizens read the whole Terms and Conditions when signing up for products and services online, while 43% of those who do not read the agreements explain that “they are boring or difficult to understand” (Smithers, 2011). The fact that the majority of consumers fail to read Terms and Conditions not only reflects their underdeveloped digital privacy literacy but also puts their right to privacy in danger. Hence, this thesis investigates how contemporary privacy education or digital literacy campaigns address and expand the understandings on such online agreements.

Overall, consumer privacy is under increasing danger in the digital era. However, digital privacy literacy of consumers nowadays is considered insufficient, and thereby, they lack the competencies to cope with the growing privacy risks. The growth of digital privacy threats combined with the insufficiency of consumer privacy competencies has sparked the need for digital privacy education and more importantly the urge for research diving into the nature of existing digital literacy campaigns. Although many studies have already paid attention to consumer’s digital privacy and called for digital privacy education (Dommeyer, & Gross, 2003; Nowak, & Phelps, 1992; Park, & Jang, 2014), few pursue to the studying of diverse campaigns that currently exist (Van Hamel, 2011). Therefore, the thesis uncovers and compares diverse digital literacy campaigns that educate consumers on digital privacy issues, answering the following research question:

RQ: How do digital literacy campaigns globally educate consumers on privacy issues?

The research question analyzes the range of communication strategies employed in contemporary digital literacy campaigns. In order to answer the main research question, the thesis divides the question into three sub-questions. Firstly, it is important to map out the digital privacy issues addressed in selected international campaigns. By looking into campaigns from different countries,

the thesis reveals the global dimension of digital privacy and the differing ways in which countries approach digital privacy issues and communicate them to their consumers, which thus leads to the first sub-question:

SQ1: What is the nature of contemporary digital literacy campaigns across the globe and what types of privacy issues do they focus on?

Secondly, privacy education can be initiated by various actors, such as governments, non-profit sectors, businesses or individuals, and there are at least two types of digital literacy campaigns, namely public education campaigns and privacy activism campaigns. Public education campaigns usually have huge involvement from governments due to their public nature (Van Hamel, 2011). Privacy education initiatives by governments are usually incorporated in the broader cyber security education initiatives. The strong national focus on cyber security is due to the fact that cyber security serves the interests of both individuals and the society or nations and that the demands to create cyber awareness and security among citizens are recognized by governments (Reid, & Van Niekerk, 2014). For another, privacy activism aims to advocate the right to privacy while also educating consumers through promoting the cause of privacy protection. Privacy activism campaigns are developed mostly by non-profit organizations serving as advocacy groups (Bennett, 2010). As mentioned, in the App-FBI dispute, governments and privacy advocates stand against each other, and they view consumer privacy in a different manner. Therefore, it is of strong societal and academic relevance to compare public education campaigns that have huge governmental involvement with privacy activism campaigns that are mainly developed by non-profits.

SQ2: How do public education campaigns differ from privacy activism campaigns?

Thirdly, campaigns usually embrace different channels or use diverse forms of messages so as to maximize effectiveness, not to mention campaigns for education purposes (Schooler, Chaffee, Flora, & Roser, 1998). Additionally, in the age of Web 2.0, social media are important to the success of diverse campaigns (Hanna, Rohm, & Crittenden, 2011). Therefore, it is important to explore how the contemporary digital literacy campaigns make use of social media, leading to the third sub-question:

SQ3: How do the existing campaigns or the institutions behind the campaigns use social media to educate and engage with consumers?

2. Theoretical Framework

2.1. Privacy in the Digital Era

The thesis aims to discover the way in which digital literacy campaigns are educating consumers on privacy issues. Therefore, in the first and current section, it is necessary to conceptualize "privacy" and see how it is situated in the digital era, while shedding light on diverse contemporary studies surrounding the topic. In the second section of the theoretical framework, privacy violations and consumer's privacy management to tackle those violations are discussed. Since a call for privacy education has been made in response to various privacy threats, digital literacy and privacy educational initiatives are focused on in the third and fourth section respectively.

2.1.1. Definitions of Privacy

Privacy is an important issue of global concern for freedom and democracy (Solove, 2008). However, conceptualizing the term "privacy" has been a difficult job for a long period of time (Finn, Wright, & Friedewald, 2013). There are various definitions proposed by different scholars regarding the concept of privacy. For instance, privacy can be defined as "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations" (Clarke, 2009). Altman (1976) summed up two groups of definitions. The first group focuses on the avoidance of interacting with other subjects. Bates' definition of privacy as "a person's feeling that others should be excluded from something" concerning that person falls under the category (as cited in Altman, 1976, p. 7). The second group emphasizes the involvement of control of the self. One of its representatives is Westin's definition of privacy as "the right of the individual to decide what information about himself should be communicated to others and under what conditions" (as cited in Altman, 1976, p. 8). In the above definitions, the dichotomous relationship between privacy and the state of being public, a.k.a. "publicness", has been touched upon (Weintraub, & Kumar, 1997), as the definitions all concern the exclusion of public scrutiny. It is thus difficult to conceptualize "privacy" without paying attention to the other side of the dichotomous pair that is "publicness".

With respect to the second group of definitions from Altman (1976) concerning "control of the self", the concept of privacy also relates to a right of human beings, the right to control their information. Privacy is usually described as a right in the sphere of law. Solove (2002a) argued that

there are six conceptions of privacy that overlap with each other at some points, namely “the right to be let alone”, “limited access to the self”, “secrecy”, “control over personal information”, “personhood” and “intimacy”. “The right to be let alone” was used by Warren and Brandeis (1890) to conceptualize privacy, who advocated the right to privacy and pointed out insufficient protections of the right by law in their article. Recently, a new privacy right, the “right to be forgotten”, was recognized in EU after the decision by EU’s Court of Justice which asked Google to erase search results upon certain requests (Bygrave, 2015). The “right to be forgotten” has been heatedly discussed in Europe for years. The right, as a result of the stay-forever nature of online content, grants individuals the right to ask Internet service providers (ISPs) to delete personal data that has no legitimate reasons for existing on the Internet (Rosen, 2012). The above legal discussions of privacy consider the concept as a human right, which needs to be protected.

Another way to better understand the concept of privacy is to look at the seven types of privacy developed by Finn et al. (2013). Firstly, “privacy of the person” is concerned with the secrecy of body characteristics, e.g., biometrics. “Privacy of behavior and action” refers to the right to keep personal activities private, while “privacy of thoughts and feelings” means the right not to have your thoughts and feelings exposed to others’ attention. “Privacy of communication” prevents people from the interception of communications. “Privacy of data and image” and “privacy of location and space” involves the protection of textual or visual information and location data respectively. Lastly, “privacy of association” concerns the right to associate oneself to anything without being spied on by others (Finn et al., 2013). Finn et al. (2013) expanded previous categories of privacy to the above seven types of privacy, with the aim to adapt them to ever-growing new technologies. When it comes to the new technologies and the prevalence of digital media, it is important to put the discussion of privacy under the context of the digital age.

2.1.2. Digital Privacy

In the digital era, technological developments have brought the topic of privacy to the frontline (Solove, 2008). The digital age is marked by massive information going online. The development of new information technologies has been constructing an information society where personal data is increasingly gathered, stored and shared (Byford, 1998). Digital privacy, or privacy in the digital era, thus places strong emphasis on personal information online and how the data is gathered into “digital

dossiers" by such companies as ISPs, cable companies, private sector entities and so forth, which then flows to the hands of governments or other companies. The dossiers might contain information on an individual's reading and purchasing habits, website activities and so forth and seem to be constructing a digital biography of the person involved (Solove, 2002b).

Considering the close relationship between digital privacy and personal information online, digital privacy heavily overlaps with another concept called "information privacy". Information privacy refers to "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves" (Clarke, 2009). Therefore, the control of information online is emphasized in conceptualizing digital privacy, which aligns with the second group of definitions by Altman (1976) concerning the involvement of control and the third conception of privacy by Solove (2002a) about "control over personal information". The context has changed in this new era, but previous conceptualizations of privacy lay a critical foundation for the concept of digital privacy.

With regard to privacy in the digital era, previous researchers who dived into the topic, such as Byford (1998) and Solove (2002b), have expressed a common concern that digital privacy is being put in danger due to the growing data tracking and collection by governmental and commercial sectors. The concern is where privacy education should come in. Privacy education shows strong significance in a sense that it helps safeguard consumer's right to privacy, but little research has been devoted to how consumers are being educated on privacy issues. Hence, this thesis strives to fill this gap in contemporary research. The second and the fourth section of the literature review will shed more light on existing research surrounding privacy risks and privacy education respectively, revealing the nature and extent of the research gap mentioned.

2.1.3. Consumer Digital Privacy

Consumers possess a wide range of rights. Privacy has been recognized as one of those consumer rights because of relevant legislative efforts (Goodwin, 1991). Consumer's right to privacy literally refers to the right to privacy held by consumers, meaning that they have control over their personal information (Franzak, Pitta, & Fritsche, 2001). The conceptualization of consumer privacy by Goodwin (1991) uses two dimensions, a.k.a. control over information dissemination and control over unwanted intrusions by others. Control over information dissemination concerns whether consumers' personal data are collected or released without their knowledge, while unwanted intrusions that

consumers have the right to limit include marketer-initiated push marketing, e.g., telemarketing and spam (Goodwin, 1991; Milne, & Rohm, 2000). Slightly different from Goodwin's (1991), another two-dimension conceptualization of consumer privacy by Caudill and Murphy (2000) and Culnan (1995) concerns whether consumers have control of information use and whether they are informed about data collection. To summarize, consumer digital privacy can be defined as consumer's right to control their information online and exclude unwanted intrusions through digital media while informed about the handling of their personal data on the Internet.

From the above discussion, it is found that the exploration of how to conceptualize consumer digital privacy has been done extensively. However, previous research seldom looked into how digital privacy is defined differently by different institutions. Governments and non-profit organizations have a different view on what digital privacy is, demonstrated in the above-mentioned Apple-FBI dispute. Therefore, the thesis will dive into the differences based on the analysis of two types of digital literacy campaigns, namely public education campaigns backed by governments and privacy activism campaigns by non-profit organizations, with an aim to add to the existing conceptualizations.

At the same time, when privacy is referred to a consumer right, the academic discussion usually falls into the sphere of law (Rosen, 2012; Warren, & Brandeis, 1890). Other law-related studies on consumer digital privacy have provided policy implications in terms of privacy protection (Franzak et al., 2001; Goodwin, 1991). Besides a strong legal focus of digital privacy research, another type of such studies is related to the sphere of marketing. For example, Culnan (1995) discussed consumer privacy issues surrounding name removal procedures in direct marketing. Although it is suggested by the previous studies that laws should be polished to better protect consumer digital privacy and marketers should take more responsibility, consumer privacy education is also important to digital privacy protection (Van Hamel, 2011). However, there is a lack of research devoted to consumer privacy education in the digital age and how digital privacy issues are communicated in digital literacy campaigns. The thesis serves to fill this gap by analyzing how the selected public and advocacy campaigns provide consumers with a meaningful view on what they regard as urgent privacy issues in the digital age.

2.2. Violations and Management of Consumer Digital Privacy

After conceptualizing privacy in the digital era, the second section addresses different privacy

violations and the status quo of consumers' management of their digital privacy. Having a clear view on violations and management of consumer digital privacy by reviewing relevant research lays a crucial foundation for analyzing how digital literacy campaigns deal with those violations and help consumers better manage their digital privacy.

2.2.1. Consumer Privacy Violations Online

Studies on consumer privacy in the digital age have expressed a common concern that new technologies have generated threats to consumer's right to privacy in spite of bringing certain benefits or convenience. Solove (2006) summed up four basic groups of privacy violations, namely "information collection", "information processing", "information dissemination" and "invasion". Firstly, "information collection" concerns collecting personal data and includes harmful activities in terms of surveillance and interrogation. Secondly, "information processing" threatens privacy through storing and reusing personal information. It consists of five activities, a.k.a. aggregation, identification, insecurity, secondary use and exclusion. Thirdly, "information dissemination" involves the spreading out of personal information, which contains breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion. Lastly, "invasion" is about intruding into private affairs. Activities of this category include intrusion and decisional interference (Solove, 2006).

According to the two dimensions of consumer privacy by Caudill and Murphy (2000), violations occur when consumers are not given the ability to control their information or not well informed about the collection and use of their personal data. Consumers, businesses or marketers and governments are three main stakeholders heavily involved in various privacy issues (Foxman, & Kilcoyne, 1993). Consumers are data sources per se, while companies and governments have been criticized for violating consumer privacy. Besides companies and governments, malicious individuals involved in cybercrimes are also posing threats to consumer privacy (Aimeur et al., 2010). In that sense, cyber security intertwines with privacy. Therefore, the discussion of consumer privacy violations in the digital era is divided into three sub-sections according to the three actors involved in violating consumer privacy, namely businesses, governments and malicious individuals.

2.2.1.1. Privacy Violations by Businesses

Since the Internet is increasingly used for commerce and marketing purposes, it paves the way

for companies to track consumers' online behaviors and collect a huge amount of their personal data (Ashworth, & Free, 2006). Marketers' data collection using new technologies invades consumer privacy rights and generates increasing concern among consumers (Foxman, & Kilcoyne, 1993). Wang, Lee and Wang (1998) proposed four types of Internet marketing activities that violate consumer privacy, namely "improper acquisition" (including improper access, collection and monitoring), "improper storage", "improper use" (including improper analysis and transfer) and "privacy invasion" (concerning unwanted solicitation), which are well in line with Solove's (2006) four groups of privacy violations.

Due to the privacy concerns mentioned, consumers should have taken good care of their personal information, but "customers knowingly give up some of their privacy in this transaction in return for something of value – a product discount, credit, future coupons on heavily used items, and so forth" (Caudill, & Murphy, 2000, p. 7). Relevant studies have placed emphases on the trade-off between consumers and companies. Ashworth and Free (2006) came up with an exchange model of online marketing, where consumers consciously or unconsciously give information to companies in exchange for benefits including use of services and compensations. Marketer-consumer interactions in the exchange process contain consumer's corporate website or third party website visit and software download as well as marketer's direct emails or spam (Ashworth, & Free, 2006). With regard to consumers' willingness to provide personal information for marketers, consumers have the least willingness to offer their financial and personal identifier information, as the use of this type of information causes the biggest concern (Phelps, Nowak, & Ferrell, 2000). There has been an ongoing debate on the consumer-company relationship pertaining to digital privacy. Culnan and Bies (2003) summarized three perspectives regarding the relationship, namely the corporate, activist and centrist perspective. The corporate perspective argues that limiting companies' access to consumer information hinders companies' efficient operation and fulfillment of social responsibility. On the other hand, the activist perspective advocates that new technologies, if not used properly, damage consumer digital privacy (Culnan, & Bies, 2003). The centrist perspective stands between the above two perspectives, promoting a balance between company's interests and consumer's individual privacy (Culnan, & Bies, 2003; Sarathy, & Robertson, 2003).

Social networking sites belong to another type of businesses that might involve in violating consumer digital privacy. Although the ability to control information online is an important dimension

of consumer privacy in the digital era, social media users express concerns that they are losing control over information posted on social media as well as the occurrence of certain privacy violations (Caudill, & Murphy, 2000; Culnan, 1995; Houghton, & Joinson, 2010; Milne, & Rohm, 2000). Since consumers, especially younger ones, are revealing a considerable amount of information on social media, their information can not only be used by anyone using those platforms but also serve the interest of the omniscient social networking service providers per se (Barnes, 2006; Strufe, 2009). Firstly, third parties can use public information harvesting to scrape any information from social media web pages. With those harvested data, it is possible for companies to construct "social interaction graphs" of social media users about their interactions on certain topics (Erlandsson, Boldt, & Johnson, 2012). Secondly, social network sites, such as Facebook and Twitter, which are providing the platforms, collect and store a huger amount of and more in-depth user data into their databases. They can disclose the information to third parties or use it for other purposes and thus potentially invade consumer privacy, acting like "Big Brothers" (Jones, & Soltren, 2005; Strufe, 2009).

Therefore, consumers should understand how their information is being handled by businesses. Privacy education helps protect consumer digital privacy by informing consumers of violations by companies. Recent studies focus too much on those violations instead of how consumers are being educated or how they should be educated. The thesis looks into how digital literacy campaigns address those violations in order to better educate consumers on digital privacy issues.

2.2.1.2. Privacy Violations by Governments

The second main actor that might involve in violating consumer digital privacy is the government. As mentioned, companies are collecting personal information into their "digital dossiers" which contain digital biographies of consumers. The data are growingly flowing to governments after gathered in those dossiers (Solove, 2002b). Especially since the September 11 attacks, the US government has been actively engaging in data mining (Solove, 2007). For one thing, governments show huge willingness to pay for the information supplied by database firms. For another, certain law enforcement grants governments' access to data collected by companies for investigating criminal activities or for counter-terrorism purposes. If companies reject the cooperation with governments, governments might force companies to provide the information through subpoena or court order (Solove, 2002b). With an increasing amount of data being exposed to governments, there are potential

violations against consumer's right to privacy.

There has been a heated debate pertaining to the contradiction between national security and individual privacy. Similar to the three perspectives of consumer-company relationship by Culnan and Bies (2003), there are also three perspectives regarding the contradiction. The main representatives of the for-security perspective are usually governments or governmental officials. They have compelling reasons to collect and then use consumer information, as those data can assist governments in detecting criminal activities or countering terrorism (Solove, 2002b). The "nothing to hide" argument can be cited to support data collection practices by governments, stating that people "have nothing to hide" if they are not engaged in illegal activities (Solove, 2007). The for-privacy perspective demonstrates the concern that government data mining, if not constrained adequately, violates consumer privacy through monitoring consumers' private lives and interfering with their freedom of association, for which "privacy of association" is threatened specifically (Finn et al., 2013; Solove, 2002b). The centrist perspective proposes a balance between national security and individual privacy. Privacy measures on the web should be ensured, but meanwhile national security should also be attached importance to (Thuraisingham, 2002). In the selected digital literacy campaigns, it is therefore important to find out how public education and privacy activism campaigns stand differently in the three perspectives of security-privacy debate and the three by Culnan and Bies (2003).

A recent case concerning the contradiction between individual privacy and national security is the Apple-FBI dispute, which has been discussed. In this issue, the FBI stands for the for-security perspective because they argue that attaining information from the shooter's iPhone is helpful for further investigation. However, Apple supporters and privacy advocates are for privacy, saying that FBI's request would violate privacy rights and cause more similar requests in the future (Solove, 2002b; The New York Times, 2016). In the dispute, governments and privacy advocates seem to view consumer privacy differently. With little timely research paying attention to the Apple-FBI dispute and different perceptions by governments and privacy advocates in terms of consumer digital privacy coming out from the dispute, the thesis serves as a pioneer to address this respect by comparing public education campaigns backed by governments and privacy activism campaigns by non-profits.

2.2.1.3. Privacy Violations by Malicious Individuals

Besides companies and governments, malicious individuals can also use the Internet to intrude

into consumer digital privacy. The information revolution has exposed consumers to the danger of various cybercrimes that are threatening consumer digital privacy (Smith, 2004). Consumer privacy is potentially threatened by activities, such as identity theft, phishing, malware infection and so forth, conducted by malicious individuals (Aimeur et al., 2010).

Speaking of cybercrimes that trigger privacy concerns, several studies have attached importance to online identity theft, which has been mentioned as one of the malicious activities, and its harms towards digital privacy. Online interactions are demanding consumer personal information, and a "map" of a person can be drawn with his or her histories of searching, reading, messaging, shopping and so forth (Aïmeur, & Schőnfeld, 2011; Phillips, 2002). The map containing a wide range of data is an important informational source of identity theft (Aïmeur, & Schőnfeld, 2011). The study on identity theft by Milne, Rohm and Bahl (2004) points out that consumers' privacy is threatened when they visit certain websites or complete certain transactions on the Internet. Their information is also in danger if companies break their promises to share the information with third parties or when corporate databases are hacked, which thus leads to the leakage of information. Additionally, individuals can develop malicious applications, such as Trojan applications, or viruses to invade personal computers to steal consumer information (Erlandsson et al., 2012; Smith, 2004). Therefore, cyber security issues caused by malicious users are putting consumer digital privacy at risk.

From the above discussion, the development of information technologies and the increasing ubiquitousness of the Internet have brought various threats to consumer digital privacy, despite the fact that the interconnectivity and convenience of people's life has been enhanced (Houghton, & Joinson, 2010). Violations against consumer digital privacy are caused by three main actors, namely companies, governments and malicious individuals. Due to those violations, educating consumers on privacy issues becomes urgent (Dommeyer, & Gross, 2003; Nowak, & Phelps, 1992; Park, & Jang, 2014). Therefore, this thesis analyzes privacy awareness campaigns to outline existing methods of educating consumers and to provide future suggestions on digital privacy education. This effort pays heed to the urgency in tackling the growing privacy concerns and violations. As there are already educational initiatives out there to raise consumers' privacy awareness, it is necessary to discover how those initiatives inform consumers of various privacy violations. With the majority of research focusing on diverse violations instead of the communication of those violations in educational campaigns, the thesis sheds light on the latter aspect.

2.2.2. Terms and Conditions and Privacy Policies

With violations of digital privacy by businesses and governments discussed, it is important now to shed light on Terms and Conditions and privacy policies that prevail in online businesses. Those agreements pressure consumers to agree to grant companies' control over their information (Gindin, 2009). They also allow governments' access to user data for legal reasons, enabling government-private sector information flows (Hoback, Ramos, & Khanna, 2013; Solove, 2002b).

Terms and Conditions particularly prevail in ISPs and social networking sites (Terms of service, n.d.). The lengthy agreements give social networking sites different scope of control over users' content (Smith, 2013). Since "selecting 'Agree' serves as an electronic signature", consumers are supposed to think twice or even more before clicking the box (Pidaparthy, 2011). However, only 7% of British citizens read the whole Terms and Conditions (Smithers, 2011). Being length and difficult to read has become a common problem of Terms and Conditions. But meanwhile, it is difficult for companies to shorten the lengthy and user-unfriendly Terms and Conditions because they are exposed to potential legal troubles if they do not explain matters in detail (Pidaparthy, 2011).

Some studies have already started to address issues surrounding Terms and Conditions. Hans (2012) studied privacy policies and Terms and Conditions of Google, Facebook and Twitter and discovered the existing of unfairness and "information asymmetries" between users and those websites in terms of digital privacy, while asking the Federal Trade Commission (FTC) to refine its approaches to prevent violations towards consumer privacy by companies. Gindin (2009) focused on a legal case involving the FTC and Sears. The FTC accused Sears of disclosing insufficient information of its Tracking Application in Terms and Conditions. Problems related to digital contracting, privacy and advertising raised from the case were discussed in a holistic manner, and there was a call for educating consumers on behavioral advertising and related issues. The report by Van Alsenoy et al. (2015) criticized the unfair contract terms of Facebook, which violates the Unfair Contract Terms Directive (UCTD).

However, compared to the large amount of coverage on problems concerning Terms and Conditions and privacy policies by mainstream media (Pidaparthy, 2011; Smith, 2013; Smithers, 2011), there are surprisingly few studies on the topic. Further, the above few studies in the field of Terms and Conditions have a strong focus on legality (Gindin, 2009; Hans, 2012; Van Alsenoy et al.,

2015). Therefore, this thesis not only serves to fill the insufficiency of research addressing Terms and Conditions but also explores the topic in a non-legal manner by looking into how digital literacy campaigns communicate the problematic Terms and Conditions and privacy policies to consumers.

2.2.3. Consumer's Management of Digital Privacy

As different violations of consumer privacy have been discussed, it is then necessary to look at how consumers manage their digital privacy to cope with privacy threats. Knowing the current state of consumer's management of privacy nowadays is of great importance to the understanding of the role and efficacy of digital literacy campaigns in educating consumers on privacy issues.

Madden (2012) explored how users manage their digital privacy on social networking sites. Approximately half of users surveyed feel it is hard to manage their privacy regarding their profiles on social media platforms. There are three major methods for managing privacy and reputation on social media, namely unfriending someone, deleting comments and untagging pictures. Users also adjust privacy settings to restrict access to their profiles as another way of managing their digital privacy (Madden, 2012). Milne et al. (2004) mapped out consumer privacy protection behaviors online, which include reading privacy policies, rejecting unnecessary cookies, encrypting e-mail and so forth. However, the study found that less than half of consumers surveyed performed those privacy protection behaviors (Milne et al., 2004). Speaking of Terms and Conditions and privacy policies, the results align with the findings from the study of Smithers (2011) that consumers do not pay much attention to those agreements even though they are important.

The study by Youn (2009) sheds light on digital privacy management among young consumers. Two types of strategies for privacy management by both youngsters and adults were summarized, namely approach strategies and avoidance strategies. The approach strategies include giving false or incomplete information ("fabricate") and turning to privacy-enhancing technologies or other people for help ("seek"). In terms of the "seek" strategy, youngsters do not possess enough knowledge to use privacy-enhancing technologies but are able to turn to elder people, e.g., parents or teachers, for advice or support. The avoidance strategies refer to how consumers withhold certain information or stop using certain websites ("refrain"). The adoption of the strategies is influenced by consumers' privacy concerns online (Youn, 2009). Furthermore, as Dommeyer and Gross (2003) pointed out, consumers tend to use privacy management strategies that require less effort. After reviewing the

above studies, it is summarized that consumers perceive privacy management online as something difficult. Also, most of their control over personal information is limited to managing the information they put online, while consumers can do little with the back-stage data tracking (Milne et al., 2004; Youn, 2009). Due to the uneasiness of managing online privacy, the thesis digs deep into the methods digital literacy campaigns use to help consumers better manage their online information.

2.3. Literacy in the Digital Age

After reviewing relevant research on privacy violations and consumer's management of digital privacy, this section addresses consumer digital literacy, with an emphasis on privacy literacy. Privacy literacy is important for consumers to tackle those violations and better manage their online information (Park, 2011), while privacy education helps improve consumer digital literacy. Therefore, this section serves as a transitional section between the second and the fourth section.

2.3.1. Literacy

Literacy is not limited to reading and writing but meanwhile concerns the ability to engage in various types of communication and manage the information transmitted across different communication channels (Summey, 2013). With the development of technologies, the concept of "new literacy" is brought up by scholars to distinguish it from old or traditional literacy. According to Coiro, Knobel, Lankshear and Leu (2014), there are various ways to define the newness of "new literacy". One perspective relates reading and writing on paper to traditional literacy while doing the same on screens is associated with new literacy. This perspective is popular among scholars. With regard to this, the type of media used or the form of content determines if the literacy is new or old. Generally, print media or print texts are discussed under the concept of old literacy, while using new media platforms is related to new literacy. However, old and new literacy are difficult to define and distinguish, as old literacy can be applied to new text and vice versa (Moje, 2009). Another perspective according to Coiro et al. (2014) concerns the constantly changing nature of literacy. For instance, email could be regarded as "old" literacy when instant messaging emerged. "New literacies change regularly as technology opens new possibilities for communication and information" (Leu, Kinzer, Coiro, & Cammack, 2004, p. 1570). The unstable nature of literacy due to constantly changing technologies is another reason for the difficulty to distinguish between old and new literacy.

Normally, new literacy is closely connected to the development of technologies and the context of digital age. It serves as an umbrella term covering Internet literacy, digital literacy, new media literacy and so forth (Coiro et al., 2014). However, according to Summey (2013), digital literacy is a more appropriate word for describing the literacy in the digital era. The thesis adopts Summey's (2013) view and thus uses digital literacy instead of new literacy. The reasons for turning to Summey (2013) and a detailed review of literature surrounding digital literacy are addressed in the following part.

2.3.2. Digital Literacy

As mentioned, Coiro et al. (2014) regarded digital literacy as an important component of new literacy. However, Summey (2013) argues that digital literacy covers broader area of nowadays literacy than new literacy and is thus more appropriate in describing the "new" version of literacy in the 21st century, as it recognizes the "irrevocable impact" brought by technology. Additionally, the previous discussions have shed light on the confusion between new and old literacy. Therefore, "digital literacy" would be a clearer and more appropriate word for conceptualizing literacy in the digital age. The thesis adopts Summey's (2013) definition that regards digital literacy as important skills to manage information and communication in the digital era.

The importance of digital literacy also lies in various aspects. Eshet-Alkalai (2004) described it as a "survival skill" in the digital era, since it enables Internet users to perform basic tasks in digital environments. Those tasks include reading visual representations (photo-visual literacy), reproducing new and meaningful materials (reproduction literacy), accessing information through using hypermedia and non-linear thinking (branching literacy), evaluating information wisely (information literacy) and avoiding harms while deriving benefits from digital communication (socio-emotional literacy) (Eshet-Alkalai, 2004). Hence, digital literacy is a multimodal literacy and is more complicated than traditional literacy that existed before the prosperity of the Internet. Furthermore, digital literacy is an essential requirement for members in today's "technologically engaged society" where they are supposed to possess the ability to evaluate digital information critically and create original content with digital media (Berson, & Berson, 2006). "Digital literacy builds the foundation for productive functioning as a global citizen and addresses the development of skills needed for the evolving cyber-domain" (Berson, & Berson, 2006, p. 142), which aligns with Eshet-Alkalai's (2004) "survival skill". Therefore, the study of digital literacy is urgent in the information age, which makes

the thesis highly relevant and timely.

Due to the development of technologies and the arrival of digital age, literacy studies nowadays are shifting their focus to digital literacy. Existing studies have addressed the multimodality of digital literacy and explored different types of literacy in the digital era (Eshet-Alkalai, 2004; Moje, 2009). However, as a need to raise public literacy has been recognized (Leu et al., 2004), the question concerning how digital literacy, e.g., privacy literacy (to be discussed in the next part), can be improved through educational initiatives or awareness campaigns remained unsolved. The thesis thus aims to address the question by providing insights into those awareness campaigns on digital privacy as well as implications for enhancing consumer digital privacy.

2.3.3. Privacy Literacy

Privacy literacy has been highlighted as an essential component of digital literacy. Digital literacy involves the assessment, evaluation and analysis of digital forms of information and concerns safety and security in digitized environments where privacy protections are crucial (Berson, & Berson, 2006). Park (2011) divided digital privacy literacy into three dimensions, namely “familiarity with technical aspects of the Internet”, “awareness of common institutional practices”, and “understanding of current privacy policy”. Online privacy literacy is composed of factual and procedural knowledge (Trepte et al., 2015). Park’s (2011) three dimensions of digital privacy literacy would fall under the factual knowledge concerning “knowing that”, while Youn’s (2009) two types of privacy management strategies, a.k.a. approach strategies and avoidance strategies, would fall under the procedural knowledge related to “knowing how”, in light of the conceptualization of Trepte et al. (2015).

Similar to consumer’s management of privacy, consumer’s knowledge of privacy is also inadequate, which has been indicated by most studies surrounding digital privacy literacy. The study by Park and Jang (2014) focused on understanding consumer privacy-related knowledge in mobile communication and found that there was a low level of information-location privacy literacy held by consumers surveyed. Although there has been increasing popularity and familiarity in terms of mobile use, consumers possess little knowledge concerning information-location surveillance and privacy settings (Park, & Jang, 2014). The study by Dommeyer and Gross (2003) investigated consumers’ understanding of regulations and practices on privacy issues and also found that their privacy knowledge was inadequate. In specific areas such as data collection practices and name removal

mechanisms, consumer privacy literacy is also considered low. Only 34 percent of consumers surveyed are aware of data collection and knowledgeable of name removal mechanisms at the same time (Milne, & Rohm, 2000). Consumers possess insufficient knowledge about direct marketing practices, for which privacy concerns are caused (Nowak, & Phelps, 1992). Additionally, Park (2011) found strong predictive influence of the three dimensions on privacy control behavior, meaning that users with a higher level of technical familiarity, institutional surveillance awareness and policy knowledge is more likely to exercise information control. However, consumers perceive information control as something difficult and execute insufficient control over their personal information (Madden, 2012; Milne et al., 2004), which might be a result of consumers' underdeveloped digital privacy literacy.

Regarding the insufficiency of privacy literacy, digital literacy initiatives have been called for to educate consumers on privacy issues (Dommeyer, & Gross, 2003; Nowak, & Phelps, 1992; Park, & Jang, 2014). However, little research has responded to the urgent call to investigate privacy education initiatives, which is elaborated more in the last section of the literature review. More importantly, contemporary studies mostly focus on the insufficiency of consumer's digital privacy literacy but seldom look into how the insufficiency can be enhanced through digital literacy campaigns (Dommeyer, & Gross, 2003; Milne, & Rohm, 2000; Nowak, & Phelps, 1992; Park, & Jang, 2014). In other words, most studies detach the intimate relationship between privacy literacy and privacy education. Thus, thesis will not only respond to urgency of digital privacy education but also dive into how those campaigns contribute to the improvement of privacy literacy, with the aim to add new categories, if they are spotted in the analysis of campaigns, to the existing dimensions of digital privacy literacy of Park (2011), Trepte et al. (2015) and Youn (2009).

2.4. Consumer Education on Digital Privacy

With the necessary theoretical foundation of the above three sections, the last section sheds light on relevant research on consumer digital privacy education. This section first discusses general consumer education and then attends to consumer education, specifically on digital privacy.

2.4.1. Consumer Education and Engagement

Consumer education is a broad concept that can be about educating consumers on various issues,

e.g., privacy issues focused on in this thesis. Consumer education concerns empowerment, as it has the aim of "empowering people in their consumer role" (McGregor, 2005, p. 437). The empowerment involves teaching consumers to make better decisions and keeping them informed of their responsibilities and rights (McGregor, 2005). As privacy is recognized as one of those consumer rights, consumer education can also relate to improving consumer privacy literacy (Goodwin, 1991).

Consumer education is important to both the society and the marketplace. The prosperity of the society is increasingly based on consumer education (Adkins, & Ozanne, 2005). As pointed out by Langrehr (1979), consumer education also minimizes people's unfavorable attitudes towards the complicated marketplace, as it leads to the fulfillment of people's needs by teaching them how to navigate the marketplace. Due to the growing importance of consumer education nowadays, numerous studies have centered around the topic. The first type of studies focuses on the "how" of consumer education. Adkins and Ozanne (2005) came up with a critical consumer education framework consisting of tailor-made strategies for educating four different types of consumers, namely "alienated consumers", "conflicted identity managers", "identity exchangers and enhancers" and "savvy consumers". Another type of research focuses on the outcome or effectiveness of consumer education. Xiao et al. (2004) used the Transtheoretical Model of Change (TTM) to analyze participants' change process of the education program called MONEY 2000™. According to Prochaska, Redding and Evers, behavior change includes five stages, a.k.a. precontemplation, contemplation, preparation, action and maintenance (as cited in Xiao et al., 2004, p. 56). Reid and Van Niekerk (2014) studied the cyber security education campaign by South African Cyber Security Academic Alliance and found that the campaign was moderately effective in cultivating a cyber security culture for the South African youth analyzed.

According to Reid and Van Niekerk (2014), educational campaigns, if developed properly, can be effective in enhancing consumer knowledge and raising consumer awareness on certain issues. In the age of Web 2.0 when consumers are increasingly connected online, social media are playing an indispensable role in the success of diverse campaigns (Hanna et al., 2011). "Social media is about creating, influencing, and sharing; and, importantly, it can have a powerful impact on performance" (Hanna et al., 2011, p. 271). The importance of social media to campaigns lies in social media's strength in fostering consumer engagement. The interactive and conversational nature of social media enables various organizations to reach and connect with consumers and to establish close relationships

with them, leading to effective engagement (Sashi, 2012). Waters, Burnett, Lamm and Lucas (2009) studied how non-profit organizations use three main relationship cultivation strategies, a.k.a. “disclosure”, “information dissemination” and “involvement”, on Facebook to facilitate interactions with stakeholders. Those strategies can also be applied to other sectors besides non-profits. As Waters (2007) pointed out, educational non-profits tend to focus on interactive elements in online communication. As the selected digital literacy campaigns or the institutions behind them all use social media, the thesis also looks into how they use social media to spread the outreach of those campaigns and thus maximize their effectiveness. The thesis focuses on not only non-profits but also governmental sectors, with the latter having been untouched by Waters et al. (2009).

2.4.2. Privacy Education and Activism

As mentioned, consumer education can relate to privacy issues (Goodwin, 1991; McGregor, 2005). Consumer privacy education, especially in today’s digital environment, has been generating growing attention due to numerous digital privacy violations discussed above. A considerable number of studies have shed light on the urgency of consumer education on privacy. There has been increasing concern among consumers in terms of privacy invasion, identity theft and Internet fraud online, while consumers either have insufficient knowledge of protecting themselves or perform few protection behaviors, sparking the need for education programs to be developed by different sectors in the society (Milne et al., 2004). Similar to Milne et al. (2004), results of Nowak and Phelps (1992) also show that consumers are concerned about privacy threats online but do not possess proficient digital literacy to tackle privacy threats, for which educational initiatives are highly needed. One of the useful insights from Youn’s (2009) research is the significant influence of perceived vulnerability to privacy risks on privacy concerns among youngsters studied. As a result, it is suggested that privacy education initiatives should attach importance to privacy risks concerning information disclosure so that consumers’ motivations to protect their privacy will be boosted (Youn, 2009). Although educational initiatives to improve consumer digital privacy literacy have been called for by the above studies, little research has responded to the call. The thesis fills the gap through adding to the field of consumer education on digital privacy.

Digital literacy is important in protecting consumer privacy in a sense that digital literacy influences information control behaviors online (Park, 2011). A number of educational initiatives

already exist to protect consumer privacy through improving their digital literacy. Privacy education can be initiated by various actors. Governments in different countries have been playing a crucial role in educating consumers on privacy issues. The privacy education initiatives by governments are usually incorporated in the broader cyber security education initiatives, as mentioned supra. Van Hamel's (2011) Privacy Piece compares digital literacy initiatives that aim to enhance people's privacy competencies in Canada, Britain, Australia, America and Brazil. In the paper, a strong focus was placed on Canadian digital literacy efforts. The key players discussed include governments, industry associations, advocacy groups and so forth, but more emphasis was placed on governmental initiatives. For example, "Get Cyber Safe" was developed by Public Safety Canada, which is a federal government department, to educate Canadian publics on how to protect themselves on the Internet. Most of those public education campaigns backed by governments are cyber security-related but at the same time aim to enhance consumer's privacy competency, meaning that privacy issues are addressed under the discussion of cyber security (Van Hamel, 2011). Additionally, according to Kessler and Ramsay (2013), cyber security, which belongs to the larger concept of information security, is popularly used in governmental sectors. Privacy issues are addressed in the paradigms proposed by Kessler and Ramsay (2013) for cyber security education in the US.

Privacy activism is another way of educating consumers on privacy issues in the digital age through emphasizing privacy violations and advocating the protection of consumer digital privacy. Studies related to privacy activism or scholars serving as privacy advocates shed light on the privacy violations by governments and businesses. Solove (2004) in his book discussed how people's privacy is being harmed by those "digital dossiers" in the information age and how the law should be reformed to safeguard people's digital privacy, stressing that the relationship between consumers and data collectors should be restructured by legislation. Since people's digital privacy has been put under numerous threats by governments and businesses using new technologies, the book by Brunton and Nissenbaum (2015) teaches netizens to fight against the data collection by governments and companies and suggests resorting to the tool of "obfuscation", which means deliberately using confusing information to disturb the surveillance and data collection efforts. The tool of "obfuscation" has something in common with the "fabricate" strategy of Youn (2009), when it comes to providing confusing information. Mendel et al. (2012) not only focused on privacy threats brought by new technologies but also attached great importance to the interplay between Internet privacy and freedom

of expression. Privacy in some cases is considered a precondition of freedom of expression, but the tension between the two has also been witnessed and intensified by the Internet.

There are privacy activism initiatives developed mainly by non-profit organizations to strengthen consumer digital privacy competencies. Bennett (2010) in his book, *The Privacy Advocates,* summarized three types of privacy advocates, namely privacy-centric advocacy groups, civil liberties groups and human rights groups. Those non-profit privacy-centric advocacy groups that have initiated digital literacy campaigns include Privacy International (PI), Electronic Privacy Information Center (EPIC) and so forth. Similar to the above-mentioned scholars who take the activism stand, they focus more on the privacy-intrusive practices, such as surveillance, data collection and others, conducted by governments and businesses (Bennett, 2010). Bennett (2010) has also discovered the strategies used by the privacy advocates. For instance, "promoting change by reporting facts" falls under one of those important strategies, and those facts can be about privacy-related threats or harms (Bennett, 2010).

Although some studies have started paying attention to privacy education initiatives, there is a lack of research that links digital literacy to consumer privacy and compares public education initiatives developed by governments and privacy activism ones by non-profits. The study by Van Hamel (2011) focuses on governmental education programs, while Bennett (2010) focuses on the activism side. Although Van Hamel (2011) mentioned initiatives by advocacy groups in a very limited amount of words, those initiatives were not compared with governmental initiatives. Therefore, there is little research that combines and compares public education campaigns and privacy activism campaigns. The comparison is relevant, timely and valuable not only because it fills the academic blank but also due to the fact that governments and non-profits possess different interpretations towards privacy and thus different institutional aims pertaining to privacy education, demonstrated by the above Apple-FBI dispute. Additionally, there are also insufficient systematic and global studies on digital literacy campaigns that educate consumers on privacy issues. Van Hamel's (2011) report only gives general introductions to numerous initiatives, with strong focus on those in Canada, and is thus considered neither systematic nor global. As a result, the thesis also aims to fill the gap by analyzing digital literacy campaigns from different countries in a systematic and in-depth manner.

3. Methodology

3.1. Approach

3.1.1. Qualitative Methods

In order to answer the research question, the thesis mainly utilizes qualitative content analysis, which belongs to qualitative research methods. Contrary to quantitative research, qualitative research aims to explore “concepts and relationships” in data (Strauss, & Corbin, 1998, p. 11). In other words, it focuses on how certain information or concepts are communicated and meanwhile connected to each other. As the research question of this thesis concerns how digital literacy campaigns educate consumers on privacy issues with the purpose of finding out what those issues are, qualitative methods serve to discover the privacy issues as important concepts and their connections and are thus considered an appropriate choice of method.

Also, qualitative research has an interpretative feature and helps gain detailed insights into the content analyzed (Strauss, & Corbin, 1998). Therefore, by using qualitative methods, the thesis digs deeper into the messages conveyed through the campaigns so as to answer the “how” of privacy education and meanwhile gains better understanding of how the two different types of campaigns vary from each other. Lastly, qualitative methods can be used to discover phenomena which are less known or to explore new findings from what is already known (Strauss, & Corbin, 1998). Qualitative methods precede quantitative ones when the research topic is new, underdeveloped or complex (Ritchie, Lewis, Nicholls, & Ormston, 2013). As already discussed in the theoretical framework, research devoted to privacy education through digital literacy campaigns is insufficient and there are even fewer studies when it comes to comparing different types of campaigns. Therefore, qualitative research methods are the most appropriate for the thesis.

3.1.2. Qualitative Content Analysis

As mentioned, qualitative methods are suitable for the thesis. Specifically, qualitative content analysis as an important qualitative method is utilized to answer the research question. Qualitative content analysis that serves as an important tool for analyzing text data involves subjective interpretation of text data and identification of themes or patterns (Hsieh, & Shannon, 2005). Therefore, through looking for significant themes or concepts within textual data, the method serves

to answer the research question regarding what privacy issues as part of those themes or concepts are heavily communicated in digital literacy campaigns and hence fits the focus of the thesis. Qualitative content analysis aims for the "detail and depth" of text data (Forman, & Damschroder, 2008, p. 41). The method is thus suitable for the question in hand concerning the "how" of privacy education and further for discovering the differences between the two types of digital literacy campaigns.

There are four digital literacy campaigns for qualitative content analysis (see Table 1). The selection of the four campaigns is further discussed in the following part that discusses sampling. For each campaign, three important parts, namely textual educational material, videos and social media (specifically Facebook), are looked into. As most of the information on the website of each campaign is textual educational material, the textual information is the main way through which consumers are educated and thus serves as the focus of the analysis. Another reason is that Van Hamel's (2011) overview of privacy initiatives programs also focuses more on textual information on websites. Besides the textual material, the analysis of videos and social media serve as two extra or supplemental analyses. How each content analysis has been conducted is elaborated in the operationalization section. As mentioned, qualitative content analysis aims to identify themes within text data (Hsieh, & Shannon, 2005). Visual data will not be touched upon due to issues of scope. While feasibility is an issue here, this is also one of the limitations of the thesis.

With qualitative content analysis being used, the thesis resorts to the approach of grounded theory, which means allowing "the theory to emerge from the data" (Strauss, & Corbin, 1998, p. 12), especially considering that there has been little research analyzing digital literacy campaigns for privacy education. The analysis is hence considered inductive, as inductive content analysis is usually adopted where little research has dealt with similar subjects (Elo, & Kyngäs, 2008). With regard to the explorative nature of the thesis, the analysis of textual educational material belongs to conventional content analysis, where coding categories are largely based on the data in hand (Hsieh, & Shannon, 2005). While letting codes emerge from raw material, the theories pertaining to digital privacy and privacy literacy, which are discussed in the theoretical framework, provide starting points into the massive data and serve as important guidance during the analysis. How the coding process is influenced by the existing literature and the codes employed based on the theories in hand are elaborated infra in operationalization and expectations.

3.2. Operationalization

As mentioned, the main qualitative content analysis is conducted on the textual educational material of the selected digital literacy campaigns, with the extra or supplemental analysis of videos and Facebook data. The section sheds light on how the thesis operationalizes the three analyses, with a discussion of sampling before diving into the operationalization.

3.2.1. Sample of Textual Educational Material

Digital literacy campaigns cover a wide range of digital literacy issues beyond privacy competencies, as digital literacy concerns the abilities to use, understand and create with digital media, according to Media Awareness Network (as cited in Van Hamel, 2011, p. 6). As the thesis focuses on the aspect of digital privacy, not all types of digital literacy campaigns are suitable for the research question concerned. Therefore, those campaigns dedicated to digital privacy issues are targeted. Among those targeted campaigns, four of them were selected for the analysis. As mentioned, there are at least two types of digital literacy campaigns, namely public education campaigns and privacy activism campaigns. Since the second sub-question compares the two types of campaigns, two of the four selected campaigns are public education campaigns with heavy involvement of governments, while the other two are privacy activism campaigns solely developed by non-profit organizations. Table 1 summarizes the four campaigns in terms of name, country of origin, initiating institution(s), social media use and type of campaign.

Table 1. *Summary of four selected digital literacy campaigns*

Name	Type	Country	Institution(s)	Social media use
“Get Cyber Safe”	Public education campaign	Canada	Public Safety Canada	Facebook, Twitter, YouTube, Blog, LinkedIn
“STOP. THINK. CONNECT.”	Public education campaign	US	Department of Homeland Security, Anti-Phishing Working Group, etc.	Facebook, Twitter, YouTube, Blog, Instagram
“Me and My Shadow”	Privacy activism campaign	Germany	Tactical Tech	Blog; Tactical Tech has Facebook and Twitter

“Privacy 101”	Privacy activism campaign	UK	Privacy International	Privacy International has Facebook, Twitter and YouTube

The first campaign is “Get Cyber Safe”, a public education campaign developed by the Canadian government (Van Hamel, 2011). The campaign contains comprehensive educational information of privacy-related issues and is the major governmental campaign mentioned in Van Hamel’s (2011) Privacy Piece. Another public education campaign is “STOP. THINK. CONNECT.” developed by the Department of Homeland Security supervising the federal engagement and the Anti-Phishing Working Group which is a public-private partnership (“About STOP. THINK. CONNECT.,” n.d.). The campaign thus has heavy involvement from the US government. It is an important campaign as a great representative from the US, since it was co-launched by government and other organizations as a result of a mandate from Barack Obama’s Cyberspace Policy Review (Goodchild, 2010). The third campaign is a privacy activism campaign called “Me and My Shadow” developed by Tactical Tech, a non-profit organization based in Germany (“About Tactical Tech,” n.d.). The campaign won The Bobs’ best online activism award in the creative and original category held by Deutsche Welle (Bruck, 2013). Another privacy activism campaign is “Privacy 101” developed by Privacy International (PI), a non-profit based in the UK (“About Privacy International,” n.d.). Privacy International is introduced as one of the most important non-profit privacy-centric advocacy groups in Bennett’s (2010) book, with the “Privacy 101” campaign for educating consumers on privacy rights. As the research question concerns privacy education through digital literacy campaigns under the global context, the four campaigns selected come from four different countries.

As for the selection of textual educational material, since there is a huge amount of textual information on each of their websites, not all content is analyzed. As the main content analysis is conducted on textual educational material, on the websites, sections that are not designed for placing educational material, such as “Research & Survey”, “Get Involved”, “App Centre” and others, are firstly excluded. As mentioned, visual educational material is excluded. Sections containing all or most information from external sources, which means the information is not developed by the campaign itself, e.g., “Investigations” (an external project), “Stuff We Like” and others, are also excluded. Although the majority of educational material is retrieved, some information of less

relevance is excluded. For public education campaigns, the sections that are less relevant to the research, such as “Protect Your Business” and “Cyberbullying”, are excluded, as the thesis focuses on consumer education instead of educating businesses as well as on consumer digital privacy that involves control of information and awareness of the handling of personal data (Caudill, & Murphy, 2000). Lastly, material written in other languages is also excluded not only because the English version of the material is provided but also due to the ability of the researcher.

After gathering all necessary textual data for qualitative content analysis, the total word count of the retrieved educational material from all four campaigns reaches around 58,000 (around 31,000 for the two public education campaigns and 27,000 for the two privacy activism campaigns). Although the size exceeds the recommended amount of 18,000 words from the Methodological Guidelines (Janssen, & Verboord, 2015), it is still a manageable size. Although selecting only two campaigns will make the size close to the recommended amount, the number of campaigns is too small to gain broader insights into contemporary digital literacy campaigns. Also, although enlarging the number to six campaigns would be fascinating, it is difficult to gain deeper insights into their educational material and the size is not manageable due to a short time frame. Therefore, four campaigns are considered the most appropriate size for the sample of the analysis.

3.2.2. Content Analysis Operationalization: Textual Educational Material

As mentioned, the qualitative content analysis of the textual educational material gathered serves as the main analysis of the thesis, since those textual data make up most part of the websites. There are two types of digital literacy campaigns, namely public education campaigns and activism campaigns, and they have different institutional purposes (Bennett, 2010; Reid et al., 2014; Van Hamel, 2011). Therefore, the two types of campaigns are expected to have different focuses of privacy issues or different themes. The qualitative content analysis is conducted on the two types of campaigns respectively. In other words, the first content analysis is performed on the two public education campaigns, which is then followed by another analysis on the two privacy activism campaigns. Another reason for doing it separately is that the thesis meanwhile aims to answer the second sub-question concerning the comparison between the two types of campaigns.

As touched upon, grounded theory serves as an important approach for qualitative research (Strauss, & Corbin, 1998) and is used in the analysis of the textual data gathered. Therefore, the

analysis of each type of campaigns goes through three steps coding, namely open coding, axial coding and selective coding (Boeije, 2010). According to Charmaz, during the process of coding, a segment of data is assigned to a code that summarizes the piece of information (Boeije, 2010, p. 95). Therefore, when open coding is conducted, certain segments of the texts in the textual educational material are given those descriptive codes. A segment is not limited to a sentence but can be as short as a phrase or even longer than one sentence. Although not all the texts are coded, the content analysis of the thesis aims to code as much information as possible in case certain codes are needed. Segments that are repeated, emphasized or surprising or have academic relevance are coded (Löfgren, 2013). After open coding, the open codes that are considered important and relevant are merged into axial codes during axial coding (Boeije, 2010; Löfgren, 2013). Relevant axial codes are grouped again into selective codes which are then labeled, ending up with around three themes for each analysis (Boeije, 2010).

As the coding is influenced by the interplay between data and theories, initial codes are drawn from the literature review at the start of the analysis so as to serve as starting points and help generate more meaningful codes. One type of those initial codes concerns digital privacy risks caused by companies, governments and malicious individuals, considering that the emphasis of risks is important in privacy education and it is summarized in the theoretical framework that the above three actors heavily involve in violating consumer privacy. Another type of the codes is related to privacy protection strategies based on Youn (2009), as digital literacy campaigns tend to educate consumers by providing tips or recommendations for enhancing the safety of digital privacy. However, most codes emerge after open coding. Categories and concepts or themes emerge after axial and selective coding respectively. Meanwhile, relationships among those codes, categories and concepts or themes are also examined during the analysis (Boeije, 2010).

3.2.3. Sample of Videos and Facebook Data

Campaigns usually embrace various channels or use different forms of messages in order to maximize their effectiveness (Schooler et al., 1998). Additionally, social media play an important role in the success of diverse campaigns (Hanna et al., 2011). That is why besides diving into textual educational material, the thesis also looks into the videos and social media of the four campaigns. The two public education campaigns has used multiple social media platforms, but the two privacy activism campaigns do not have any social media accounts for themselves, except a blog section of

"Me and My Shadow" (see Table 1). However, the two non-profit organizations that developed the activism campaigns have used social media to deliver messages pertaining to the information from the campaigns. Therefore, it is still valuable to look into their use of social media because, again, social media are a crucial part of nowadays' campaigns (Hanna et al., 2011). To gain deep insights into their social media use, Facebook is chosen as the subject of the study, since the two public education campaigns and two non-profit organizations all have Facebook accounts (see Table 1) and Facebook is considered "a leading social media tool actively used by organizations" and has many engagement features (Cho, Schweickart, & Haase, 2014, p. 565). According to Statista (2016), Facebook is the most popular social networking site with approximately 1,590 million monthly active users as of April 2016. Furthermore, Waters et al. (2009) also studied how non-profit organizations use Facebook for engagement. However, the analysis of videos and Facebook data must be regarded as two supplementary analyses due to the feasibility and the fact that textual educational material constitutes most information of the website of each campaign.

As for the selection of videos, the two privacy activism campaigns have six videos in total (one from "Me and My Shadow" and five from "Privacy 101"), and the videos are from the campaigns themselves instead of outside sources. On the other hand, the public education campaigns have a greater number of videos. Some of them are from the campaigns themselves, while others are from outside sources. Also, some of them are privacy related, while others are less relevant to consumer digital privacy or not for education purposes, such as videos about protecting businesses or stop hating online and those on promoting the campaigns or about activities held. As the videos from the campaigns themselves instead of outside sources and the relevant ones are only considered, twelve videos from the public education campaigns are extracted (seven from "Get Cyber Safe" and five from "STOP. THINK. CONNECT."). It is also seen that the two public education campaigns use videos more actively for educating consumers.

As for Facebook analysis, the Facebook profile and 20 posts of each campaign are analyzed, which is based on the research of Waters et al. (2009) that analyzes how non-profit organizations use Facebook for engagement. The 20 posts are the latest posts as of May 13, 2016, excluding non-English posts and those about changing cover photos, as the analysis was conducted on May 14, 2016, and the thesis aims to discover the most recent engagement and education of the four campaigns through Facebook.

3.2.4. Content Analysis Operationalization: Videos and Facebook Data

As for analyzing videos, each video is summarized using one or two sentences, which is based on the research of Houghton and Joinson (2010) that also summarizes interview transcripts to have a general view on privacy violations reported by respondents. After the summary process, the summary and title of each video is content analyzed to see if the themes emerging from the textual data are repeated. As two content analyses are conducted on the two types of campaigns respectively, themes from public education and privacy activism campaigns are applied to their videos correspondingly. The analysis is not conducted on the whole video instead of its summary and title due to the feasibility and the fact that it only serves as a supplemental analysis. However, the analysis of educational videos from the campaigns serves to add to the richness of the main textual content analysis, with the discussion of its results incorporated into the discussion of results of the textual content analysis.

As for content analysis of Facebook profiles and posts, relationship cultivation strategies from Waters et al. (2009) are resorted to in order to answer the third sub-question concerning how social media are used to engage with consumers. The strategies consist of “disclosure”, “information dissemination” and “involvement”. The majority of the table containing elements under each strategy from the research of Waters et al. (2009) is used (see Table 6). The only adjustment made is that “volunteer opportunities” and “donate”, both of which concern taking actions, are changed to the element of “call for actions”, considering the educational purposes of the campaigns that hardly involve in asking people to volunteer or donate. It is looked into whether each element of relationship cultivation strategies is presented in the extracted Facebook profiles and posts.

3.3. Method of Analysis

This section will provide detailed description of the content analysis process, with strong focus on the main analysis of textual educational material. The software called “ATLAS.ti” is used for the main content analysis. After sampling, the selected textual educational data of each campaign is put into four different Word documents and then imported into ATLAS.ti. Before the coding procedure, it is important to get familiar with the data set in hand and read through it at least once (Braun, & Clarke, 2006). Considering the huge amount of the textual data analyzed, the data set is read through carefully twice before the start of coding. During the content analysis in ATLAS.ti, open coding, axial coding

and selective coding are conducted one by one (Boeije, 2010). In open coding, as mentioned, segments are given codes that summarize the information concerned. Some codes are adjusted during the coding, if new perspectives emerge (Boeije, 2010). The open coding is done repeatedly, so most information is revisited. According to Braun and Clarke (2006), "analysis involves a constant moving back and forward between the entire data set" (p. 15). After the open coding, the data set and open codes are revisited again, and the axial coding creates categories combing open codes, with some codes adjusted or left (Boeije, 2010). At the same time, relationships and distinctions between categories are examined. Afterwards, the categories are merged into concepts, with core concepts determined, in light of theories and the research question, during the selective coding. Those core concepts serve as themes aiming to answer mainly the first and second research question, while their relationships are established (Boeije, 2010).

Although the content analysis is considered qualitative, the frequency of themes and their axial codes are looked into and presented, using ATLAS.ti. According to Strauss and Corbin (1998), some data could be quantified in qualitative analysis, "but the bulk of the analysis is interpretative" (p. 11). The purpose is to explore which themes or axial codes are more prevalent. Prevalence is an important aspect of what counts as a theme (Braun, & Clarke, 2006). It is not only for determining themes but also for making distinctions between different themes. The frequency of a theme concerns the number of quotations it has in total.

As for analyzing videos, the researcher watches each video three times before writing a summary for the video, as familiarizing with the data in hand is important (Braun, & Clarke, 2006). Only the summary and title of each video are content analyzed. However, the details of those videos will be touched upon in the results section if necessary. Afterwards, each video is attributed to one or more themes emerging from the textual educational material. It is important to notice that the themes from public education campaigns are applied to the videos of those campaigns, and it is the same for privacy activism campaigns. As for Facebook analysis, the profile of each campaign is first scanned through carefully to see if the elements of relationship cultivation strategies are presented. Afterwards, the 20 latest Facebook posts as of May 13, 2016 from each campaign are screenshot and then imported into ATLAS.ti for content analysis. The analysis of 20 posts from each campaign serves to see if the rest of the elements of relationship cultivation strategies are presented. At the same time, similar to analyzing the videos' summaries and titles, each post is looked into if themes from the

textual educational material are repeated and thus attributed to one or more of those themes. If the content in a Facebook post does not relate to those themes, it is labeled either “other privacy issues” or “other issues unrelated to privacy”. The reason for doing so is that the thesis aims to see the prevalence or “repeatedness” of the themes across channels and also to answer the third sub-question that not only concerns engagement but also looks into their education through social media.

4. Results and Discussion

4.1. Expectations

As already touched upon in the above methodology section, the reason for conducting two separate content analyses on public education and privacy activism campaigns is that the two types of campaigns have different institutional purposes (Bennett, 2010; Reid et al., 2014; Van Hamel, 2011). Therefore, themes emerging from the two types of campaigns are expected to vary from each other to a certain extent, although a small number of similarities are also expected, as they all belong to digital literacy campaigns for privacy education. This results section first discusses about themes from the two types of campaigns respectively and then turns to comparison, followed by discussion of results of extra analyses on videos and Facebook.

Since privacy education initiated by governments has a strong focus on cyber security issues (Reid et al., 2014; Van Hamel, 2011), themes of public education campaigns are expected to be cybersecurity-related. For another, privacy activism educates consumers while advocating privacy rights and promoting the cause of privacy protection (Bennett, 2010). Therefore, themes from activism campaigns are expected to focus on helping consumers protect privacy rights against abuses and on calling for changes towards privacy protection. According to Culnan and Bies (2003), the activist perspective opposes companies' access to consumer information, and meanwhile, privacy advocates oppose FBI's request (Solove, 2002b; The New York Times, 2016). Therefore, privacy activism campaigns will also stand against companies and governments by demonstrating their violations. For public education campaigns with huge involvement of governments, they are expected to stand for governments. Additionally, as the US has the sectoral level of privacy regulation, while Germany and the UK have the omnibus level and more advanced data protection legislation (Bellman, Johnson, Kobrin, & Lohse, 2004; Bennett, 2010). The two types of campaigns might also vary from each other due to different countries of origin.

As for the types of digital privacy issues communicated through the digital literacy campaigns, the campaigns are expected to focus on communicating various digital privacy risks posed on consumers, according to Youn's (2009) suggestion on emphasizing privacy risks in privacy education initiatives. The emphasis of those risks helps trigger more privacy concerns among consumers, especially younger ones, and those concerns can then lead to their adoption of privacy protection

behaviors (Youn, 2009). According to Trepte et al. (2015), digital privacy literacy contains factual and procedural knowledge. Park's (2011) three dimensions of digital privacy literacy, namely "familiarity with technical aspects of the Internet", "awareness of common institutional practices", and "understanding of current privacy policy", would be considered factual knowledge. Therefore, the campaigns will educate consumers with the aim to strengthen the three dimensions mentioned. Youn's (2009) two types of privacy management strategies, a.k.a. approach and avoidance strategies, would be regarded as procedural knowledge. The campaigns are thus expected to provide recommendations or tips regarding the strategies.

As for the extra analysis of Facebook, Waters et al. (2009) has used relationship cultivation strategies to analyze Facebook accounts of non-profits and found that they use "disclosure" the most often. Therefore, it is expected that the two Facebook accounts of two non-profits in this thesis also tend to use the disclosure strategy compared to the other two strategies, namely "information dissemination" and "involvement". For the analysis of videos, it is expected that themes from the textual educational material campaigns will be repeated, as those videos are also incorporated as an important part of the campaigns, besides the textual material.

4.2. Public Education Campaigns

The two digital literacy campaigns discussed in this part are two public education campaigns, namely "Get Cyber Safe" and "STOP. THINK. CONNECT.". "Get Cyber Safe" is led by Public Safety Canada, which is a federal government department, while "STOP. THINK. CONNECT." has huge involvement of the Department of Homeland Security from the US government (see Table 1). Three main themes emerge from the content analysis of textual educational material (see Table 2). Therefore, this part is divided into three sub-sections accordingly. Within each theme, important sub-themes are shed light on. Also, how the three themes are repeated in the analyzed videos (with titles and summaries) is presented in Table 3.

Table 2. *Themes and axial codes (italicized) of public education campaigns*

Theme	Frequency
Theme 1: Cyber security risks on digital privacy	185
Axial codes:	
• *Growth of cyber security risks*	*29*

• *Risks caused by malware*	*52*
• *Risks caused by scams or frauds*	*46*
• *Risks caused by other malicious individuals*	*58*
Theme 2: Tactics used by malicious individuals	73
Axial codes:	
• *Tactic of faking*	*19*
• *Use of "benefits"*	*19*
• *Use of "threats"*	*11*
• *Other tactics*	*26*
Theme 3: Privacy protection strategies	409
Axial codes:	
• *Devices and information protection measures*	*243*
• *Avoidance strategies*	*115*
• *Approach strategies*	*42*
• *Attention to Terms and Conditions and privacy policy*	*9*

Table 3. *Tiles, summaries and themes of videos of public education campaigns*

Campaign	Title (italicized) and summary	Theme(s)
"Get Cyber Safe"	*Helping your child stay safe online* Parents are supposed to teach their children how to control information posted online and protect their devices that contain a huge amount of personal information.	Theme 3: Privacy protection strategies
	Easy Ways to Stay Safe on Public Wi-Fi WiFi networks give cyber criminals the chance to steal your personal information. It is thus important to use firewall and anti-virus software, double-check the address of the network, watch out for "shoulder surfers" and remember to log out after using public WiFi.	Theme 1: Cyber security risks on digital privacy Theme 3: Privacy protection strategies
	Easy Ways to Stay Safe on Your Mobile Cyber criminals try every means to get access to data in your mobile. To safeguard information on mobile, users need to adopt a five-step privacy protection strategy, which contains using auto-lock, going to trustworthy sites, thinking twice before clicking, turning off Bluetooth connection and updating on time.	Theme 1: Cyber security risks on digital privacy Theme 3: Privacy protection strategies
	Easy Ways to Stay Safe on Social Networks Cyber criminals are casting dangers to information on social media, so it is time to go through five tips for staying safe on social networks, namely never clicking suspicious links, being careful about posting, adjusting privacy settings, being careful about "friending" and thinking twice before downloading and clicking.	Theme 1: Cyber security risks on digital privacy Theme 3: Privacy protection strategies

	Secure Websites The “https”, padlock and green information in the address bar all together make a website a secure place for sending private and sensitive information.	Theme 3: Privacy protection strategies
	Secure Passwords A strong password combining upper and lower case letters, numbers and special characters is an important lock for your information, keeping cyber criminals away.	Theme 3: Privacy protection strategies
	Phishing Scams Phishing scams are causing loss of your information and usually impersonate real organizations. Being careful about suspicious emails and installing anti-phishing software are important protection strategies.	Theme 1: Cyber security risks on digital privacy Theme 2: Tactics used by malicious individuals Theme 3: Privacy protection strategies
“STOP. THINK. CONNECT.”	*Get Ahead With the Digital Spring Cleaning Checklist* A checklist containing tips on improving the security of your account and protecting digital files is introduced.	Theme 3: Privacy protection strategies
	STOP. THINK. CONNECT.: Top Online Privacy Tips Personal information is valuable, so it is important to limit your information posted online and who can have access to your information.	Theme 3: Privacy protection strategies
	2 Steps Ahead: Protecting Your Digital Life Two-factor authentication is important in protecting your online account and information.	Theme 3: Privacy protection strategies
	How to Get Two Steps Ahead on Your LinkedIn Account The step-by-step on how to turn on two-factor authentication on LinkedIn account is demonstrated.	Theme 3: Privacy protection strategies
	How to Get Two Steps Ahead on Your Tumblr Account The step-by-step on how to turn on two-factor authentication on Tumblr account is demonstrated.	Theme 3: Privacy protection strategies

4.2.1. Cyber Security Risks on Digital Privacy

The public education campaigns attach importance to cyber security risks on digital privacy. This theme of cyber security risks encapsulates how malicious individuals or cyber criminals threaten consumer digital privacy in various ways. It contains four sub-themes or axial codes, namely “growth of cyber security risks”, “risks caused by malware”, “risks caused by scams or frauds” and “risks caused by other malicious individuals”.

Growth of cyber security risks addressed by the two public campaigns relates to the trend that online privacy threats are increasing with the growing adoption of new technologies. For instance,

speaking of mobile devices that people are increasingly relying on nowadays, “Get Cyber Safe” directly points out that risks associated with those devices, such as smartphones, are becoming common and thus not limited to physical loss but also exposed to a wide range of malware. In order to stress the issue, “STOP. THINK. CONNECT.” even cites statistics from Telesign’s consumer report in 2015, saying that “40 percent of respondents had experienced security incidents (such as hacked accounts, password theft or notices that their personal information had been compromised) in the past year”. The growth of risks has also led to increasing concern of consumers. The report also found that 80 percent of respondents surveyed expressed worry towards online security. Besides the fact that the quantity of privacy risks is rising, the growth of cyber security risks is also reflected by the increasingly harmful consequences of the risks. Both campaigns have touched upon the severity of recent cyber security risks. For one thing, those risks not only do harm to a person per se but also involve other people around that person. “Get Cyber Safe” highlights that malicious individuals are able to “use your computer to hack other computers” and use malware to “infect your entire digital network of friends, family and associates”. For another, cyber security risks also have a negative impact on businesses, besides consumers. According to “Get Cyber Safe”, worms, as a type of malware, can damage the function of the Internet and cause a severe loss of money for businesses. With regard to the growth of digital privacy risks stressed by both campaigns, Houghton and Joinson (2010) have already pointed out that the development and ubiquitousness of new technologies have brought growing threats to digital privacy, in spite of certain benefits delivered to consumers.

The risks addressed by the two public education campaigns are cybersecurity-related. Specifically, they are the risks mainly caused by malware and scams or frauds. *Risks caused by malware* refer to the way through which various malicious software developed by malicious individuals poses threats to consumer digital privacy. With respect to malware, “Get Cyber Safe” introduces different types of malicious software. Three types of malware, namely viruses, Trojan horses and spyware, are frequently emphasized in the campaign. For viruses, “Get Cyber Safe” describes how their infectiousness threatens consumer digital privacy through compromising and damaging personal information. “Mobile viruses and malware won’t just compromise your information, OS, email and Internet connection. They can also destroy contact info, calendar entries and send infected MMS and SMS messages to your contact list.” At the same time, “STOP. THINK. CONNECT.” repeats four times the sentence, “along with computers, smartphones, gaming systems

and other web-enabled devices also need protection from viruses and malware", in order to call for attention to the danger of viruses. Additionally, according to "Get Cyber Safe", Trojan horses violate digital privacy through recording information consumers enter on websites, while spyware poses risks on digital privacy by gathering consumers' personal data without informing them and provides those data for third parties. The information flow to third parties facilitated by spyware constitutes "information dissemination" that belongs to Solove's (2006) four groups of privacy violations. The information communicated in the two campaigns aligns with the point that consumer digital privacy is under the potential risk of malware infection initiated by malicious individuals (Aimeur et al., 2010).

Risks caused by scams or frauds, as another major type of cyber security risks, are associated with scammers or fraudsters. They are malicious individuals who deceive consumers to attain their confidential information. Their objective is "to try to scam you into providing information, like your username and password, so they can gain access to your personal information", according to "Get Cyber Safe". The unwanted information solicitation by scammers constitutes "privacy invasion" (Wang et al., 1998). When it comes to those dangerous scams, the campaign also categorizes them into five main groups of scams, namely email scams, phishing and smishing scams, contest scams, online dating scams and social networking scams. It gives introductions to those current scams and discusses privacy risks related to them. Among the five types of scams, phishing scams are emphasized in both campaigns. For example, "STOP. THINK. CONNECT." warns consumers of the danger of suspicious emails and social media posts or fake websites that try to "lure" consumers into providing their confidential information like financial information. Pharming or spoofing scams that are quite similar to phishing scams redirect your access from a legitimate website to an illegitimate one, through which your devices or personal data are at risk, according to "Get Cyber Safe". The campaign also highlights that the abundant information posted online by users lays ground for potential scams, especially when it comes to social networking scams. That is why online consumers are asked to limit information posted online, which is elaborated in "approach strategies" under the third theme of privacy protection strategies.

Risks caused by other malicious individuals refer to other cyber security threats posed by malicious individuals, except the two above-mentioned types of risks caused by malware and scams or frauds respectively. Among those risks, identity theft is frequently mentioned in both campaigns. "Get Cyber Safe" introduces identity thieves as individuals who steal and use people's personal

information or identities online for different purposes without informing those people. The misuse of identities stolen can include shopping, downloading and gambling online, opening credit cards, receiving government benefits and so forth. Therefore, the risks can be both online and offline, causing consumers' loss of control of their personal information. As the ability to control personal information is one of the two dimensions of consumer privacy, the loss of that ability constitutes a violation towards consumer privacy (Caudill, & Murphy, 2000). Additionally, both campaigns have been constantly asking consumers to be cautious of cyber criminals and strangers, as words like "cyber criminals" and "strangers" have been frequently used. For instance, "Get Cyber Safe" warns that on social media, "your personal information could be stolen by a cyber criminal, putting your identity and accounts at risk", while "STOP. THINK. CONNECT." stresses that posting information on social networking sites can mean giving out personal details to strangers. Those cyber criminals and strangers are described as persons with malicious intentions of stealing and gathering consumers' personal information.

Based on the discussion of the four axial codes, it is seen that the first theme "cyber security risks on digital privacy" concerns privacy violations initiated by malicious individuals instead of businesses or governments. Although businesses and governments have been criticized for violating privacy, the two public education campaigns do not blame them for any wrongdoing. They even try to stand for businesses by showing that they also suffer loss due to malware. As seen from Table 3, four out of twelve videos in the two campaigns have repeated the first theme by emphasizing how malicious individuals threaten consumer digital privacy in public Wi-Fi, mobile devices, social networks and emails. Part of the privacy violations of Solove's (2006) and Wang et al. (1998) are communicated through the campaigns. With existing studies focusing on violations per se, the findings shift the focus towards the communication of those violations. Under this theme, the campaigns have shed light on the growth of cyber security risks by demonstrating that their quantity is increasing and relevant problems are getting severer. Therefore, Youn's (2009) suggestion on emphasizing privacy risks in privacy educational material is reflected in the two public education campaigns.

4.2.2. Tactics Used by Malicious Individuals

The second theme emerging from the textual educational material of public education campaigns concerns tactics used by malicious individuals, encapsulating the types of techniques or the steps

through which malicious individuals attain consumers' personal information. In the first theme, the two campaigns educate consumers by demonstrating privacy risks. The second theme, "tactics used by malicious individuals", addresses how those risks are generated. Knowing the tactics helps consumers determine what protection strategies they should turn to, and those protection strategies constitute the third theme infra. As a result, the second theme serves as a bridge between the first and third theme. It is composed of four axial codes, namely "tactic of faking", "use of 'benefits'", "use of 'threats'" and "other tactics".

Tactic of faking used by malicious individuals refers to the scheme of impersonating a legitimate organization, website or service. Both campaigns have addressed this common technique and thus ask consumers to verify the person or business they are dealing with. For example, according to "Get Cyber Safe", cyber criminals might send you fake emails or messages or create fake websites or profiles to trick you into providing confidential information. All those emails and messages seem to come from a trustworthy and well-know source, and all those websites and profiles are made similar to legitimate and authentic ones. "Get Cyber Safe" emphases again in the video named "Phishing Scams" (see Table 3) that malicious individuals usually mimic real organizations in order to "fool you into handing over sensitive information, like account numbers, passwords, and PIN numbers". "STOP. THINK. CONNECT." also warns consumers of fraudulent apps that "masquerade" as well-known and popular ones when they are downloading apps on mobile devices. As consumers' privacy literacy on mobile has been found to be insufficient (Park, & Jang, 2014), "STOP. THINK. CONNECT." seems to tackle the insufficiency by demonstrating the techniques malicious individuals are using to compromise consumers' personal information and digital devices.

Use of "benefits" concerns how malicious individuals tap into people's greed for small advantages. Cyber criminals promise that something good will happen to users if they hand over certain information or click on certain links that might damage their devices and thus their valuable personal information inside. In order to show how those malicious individuals use some benefits or bonuses to trick consumers, it is repeated several times in "STOP. THINK. CONNECT." that consumers should be suspicious of communication that "offers something that looks too good to be true". Meanwhile, "Get Cyber Safe" also keeps people aware of "too-good-to-be-true" offers that fool them into clicking links or entering personal details. According to "Get Cyber Safe", in health-related scams, "the promise of a 'magic' diet pill or quick weight loss can be tempting enough for some

people to click on a link and see what it's about". Therefore, the use of "benefits" is another common tactic used by malicious individuals. As seen in Table 2, the tactic of faking and the use of "benefits" are the two most frequently mentioned tactics.

Use of "threats" is also emphasized in both campaigns as a malicious technique concerning threatening people if they fail to take actions immediately. Cyber criminals usually claim that some problems exist so that the targeted consumers are asked to take immediate actions through which their personal information is compromised. Similar to how the use of "benefits" is emphasized in "STOP. THINK. CONNECT.", it is also repeated several times that consumers should be careful about any communication that "implores you to act immediately". "Get Cyber Safe" provides an example of the use of "threats" which is about pop-up messages saying there is a security problem with the computer of a targeted consumer. If the person takes the measures suggested in the messages, they will lose control over their computers and hence their sensitive personal information.

Other tactics refer to the rest of methods used by malicious individuals, excluding the three above-mentioned ones. They can be the tactics cyber criminals use to take control of people's computers and gain access to their personal information. For instance, "Get Cyber Safe" describes how hackers, who try to break into computers, gain access to consumers' information. Firstly, hackers can spot weak points of security settings and "exploit" them so that they have access to personal data. Secondly, hackers can also install a Trojan horse in people's computers, which provides "a back door for hackers to enter and search for your information". Additionally, both campaigns also warn that cyber criminals might use "shoulder surfing", which means watching over people's shoulders when they are typing or entering personal details in public places, to record and collect people's confidential information. Therefore, the information tracking can occur in the offline world and then lead to online privacy risks. However, the blame for the privacy violations is still placed on persons with malicious intentions instead of businesses or governments.

From the above discussion, it is seen that both campaigns educate consumers on privacy issues by communicating various tactics adopted by malicious individuals. Those tactics include the scheme of mimicking, use of benefits and threats and other techniques like "shoulder surfing". Their emphasis on those tactics might be due to the fact that knowing the "how-it-works" of risks is important for consumers to choose corresponding strategies. As seen in Table 2, although the theme "tactics used by malicious individuals" serves as a transitional theme between the first and third theme, it has the least

frequency in the public education campaigns, compared with the other two themes. Similarly, there is only one video (out of twelve) touching upon those tactics. However, the theme should add to Youn's (2009) suggestion on communication of risks, as it is also necessary to communicate the mechanisms behind those risks.

4.2.3. Privacy Protection Strategies

As mentioned, consumers' knowledge of malicious tactics is important in determining what types of privacy protection strategies they are going to adopt. That is why tips pertaining to privacy protection usually come after the description of those tactics in the two campaigns. "Privacy protection strategies" is the third and the most frequently mentioned theme of public education campaigns. It encapsulates tips or recommendations given by the campaigns on how to better safeguard personal information of consumers so as to protect their digital privacy. The four axial codes under this theme are "devices and information protection measures", "avoidance strategies", "approach strategies" and "attention to Terms and Conditions and privacy policy".

Devices and information protection measures refer to technical safety-strengthening actions or steps suggested for improving the protection of consumers' digital devices and personal information. Those measures can be taken to protect consumers' devices, such as computers and smartphones, so essential information stored inside those devices is safeguarded. For instance, both campaigns stress the importance of updates and provide useful tips on how to update. According to "STOP. THINK. CONNECT.", making sure that the software, browsers and operating systems are all up-to-date is the "best defense against online threats" to consumer information. "Get Cyber Safe" further suggests three tips on updating mobile operating systems, which are about checking the availability of updates regularly, never modifying control software and never "jailbreaking" through which future upgrades are disabled. Both campaigns also recommend having security software installed in consumers' devices. There are various types of security software suggested that usually begins with "anti". For example, anti-virus, anti-spyware, anti-spam and anti-theft software are all mentioned. The tips on updates and the ones on security software are sometimes merged together. For instance, both campaigns emphasizes many times that not only should consumers install security software but the software should also be in the latest version.

Meanwhile, both campaigns have been heavily stressing the importance of strong passwords.

Passwords prevent people with malicious intentions from having access to not only their devices but also their online accounts, especially social media accounts. In terms of how to set up strong passwords, “STOP. THINK. CONNECT.” advises consumers to “combine capital and lowercase letters with numbers and symbols to create a more secure password”. Additionally, changing passwords regularly and never using the same password for all accounts are both suggested by the two campaigns. In order to help consumers better protect their accounts, both campaigns introduce a new function called two-factor authentication using password and another separate channel, such as sending a message to a cellphone, to verify the person who is trying to log in is the real owner of the account. There are three videos touching upon this new function (see Table 3). Besides devices and accounts, the campaigns also provide measures consumers can take to better safeguard their sensitive information online. The importance of “https” is emphasized and repeated in both campaigns. For instance, a website with “https” instead of “http” and also the padlock and green information in the address bar, according to the video “Secure Websites” in Table 3, is a secure place where consumers can enter sensitive information, such as financial information when shopping and paying online. The suggested devices and information protection measures are mostly related to the technical aspect of privacy protection. According to Park (2011), “familiarity with technical aspects of the Internet” belongs to the three dimensions of digital privacy literacy. Therefore, the campaigns seem to enhance consumer digital privacy literacy by communicating the privacy protection measures.

Avoidance strategies are suggested approaches concerning refraining from exposing sensitive information and avoiding taking immediate actions on impulse without thinking twice. According to Youn (2009), avoidance strategies are used by consumers to withhold personal information or reject certain services or requests, with the purpose of better managing their privacy online. As for strategies about refraining information, both campaigns have been constantly asking consumers to limit the amount of information posted online as well as who can have access to the information. “STOP. THINK. CONNECT.” sheds light on the stay-forever nature of online content by emphasizing “once posted, always posted”. The information posted also has the possibility to be searched and used not only by future employers but also by such malicious individuals as identity thieves. That is why “Get Cyber Safe” asks consumers to keep in mind that “before you share personal information, consider carefully what you’re putting out there through email and social networking sites”. “STOP. THINK. CONNECT.” also suggests adjusting privacy settings on social media to limit who can see your

information. Another aspect of avoidance strategies concerns refusing suspicious services or requests. Both campaigns have been repeatedly warning consumers of the danger of links or attachments from unknown sources. Clicking those links or opening those attachments might harm consumers' devices and thus cause loss of their personal information. Therefore, the campaigns suggest ignoring or never replying to those links and attachments.

Approach strategies refer to the approaches to seek help from trustworthy organizations or people and provide false information so that consumers' real identities are hidden. According to Youn (2009), approach strategies have two aspects, namely seeking help and fabricating information. As for the aspect of "seek", both campaigns recommend turning to governmental agencies when consumers encounter issues pertaining to digital privacy or suffer from cyber crimes that are putting their privacy in danger. With regard to those problems, "Get Cyber Safe" suggests the Office of the Privacy Commissioner in Canada which provides resources for safeguarding people's privacy and protecting them from online threats. Moreover, both campaigns also stress that consumers can turn to service providers or companies for assistance. For instance, "STOP. THINK. CONNECT." mentions that if consumers come across information they do not want to associate with when searching for themselves on the Internet, they could ask the websites or ISPs to delete or alter that piece of information. Therefore, it is seen that the campaigns do not blame companies or governments for any wrongdoing, as mentioned supra, and even ask consumers to seek help from them. As for another aspect of "fabricate", both campaigns suggest using a virtual private network (VPN) to hide people's real identities, and the network offers safe connections and encrypts data. The main use of VPN they suggest is for protecting consumers' information from malicious persons who try to track consumers in public WiFi. Additionally, "STOP. THINK. CONNECT." asks consumers to retain certain anonymity through avoiding using their actual names or pictures for profiles.

Attention to Terms and Conditions and privacy policy concerns the strategy that consumers should attach importance to online agreements in order to better maintain their digital privacy. "Understanding of current privacy policy" serves as one of the three dimensions of digital privacy literacy (Park, 2011). Therefore, to enhance consumer digital privacy literacy, both campaigns have been repeatedly calling consumers' attention to Terms and Conditions and privacy policies. For example, they ask consumers to "read" and "understand" those agreements before they take further steps. According to "Get Cyber Safe", "sometimes the wording can be confusing and you may allow

the site to use your information without realizing it". Although the campaign criticizes those confusing agreements and that misuse of information is involved, it does not specify if the website is developed by companies or malicious individuals. Additionally, the effort of the campaigns is only limited to calling for attention to those agreements but does not provide detailed information regarding Terms and Conditions and privacy policy.

To summarize, privacy protection strategies address approaches or tips consumers can use to safeguard their digital privacy. According to Youn (2009), approach strategies and avoidance strategies are two dimensions of privacy-related risk-coping approaches. Both types of strategies are reflected in the two public education campaigns. The communication of those strategies is therefore incorporated into the privacy education driven by governments. Also, the two campaigns aim to strengthen consumer digital privacy literacy by focusing on the dimension of "familiarity with technical aspects of the Internet" and "understanding of current privacy policy", but the aspect of "awareness of common institutional practices" is missed out (Park, 2011). As seen in Table 2, it is the most frequent theme. Meanwhile, all the twelve videos analyzed discuss about privacy protection strategies, with eight of them paying major attention to the theme (see Table 3). Thus, privacy protection strategies serve as the focal theme of public education campaigns.

4.3. Privacy Activism Campaigns

This section focuses on the two privacy activism campaigns initiated by non-profit organizations. The first campaign is "Me and My Shadow" developed by Tactical Tech based in Germany, while the second one is "Privacy 101" developed by Privacy International based in UK (see Table 1). As seen in Table 4, three main themes emerged from the content analysis. Accordingly, this section is thus composed of three sub-sections. Significant axial codes are discussed within each theme. How the three themes are repeated in the analyzed videos is presented in Table 5.

Table 4. *Themes and axial codes (italicized) of privacy activism campaigns*

Theme	Frequency
Theme 1: Privacy risks posed by companies and governments	163
Axial codes:	
• *Growth of privacy risks*	*19*
• *Privacy risks posed by companies*	*82*

• *Privacy risks posed by governments*	*48*
• *Company-government relation and Terms and Conditions*	*14*
Theme 2: Privacy protection strategies	154
Axial codes:	
• *Devices and information protection measures*	*129*
• *Approach strategies*	*14*
• *Avoidance strategies*	*11*
Theme 3: Call for increasing protection of privacy	112
Axial codes:	
• *Status of privacy protection*	*62*
• *Demand for strengthening regulation and protection*	*50*

Table 5. *Tiles, summaries and themes of videos of privacy activism campaigns*

Campaign	Title (italicized) and summary	Theme(s)
"Me and My Shadow"	*What are digital traces?* Digital traces are created once we are online and let a considerable number of data stored in data centers worldwide. They reveal a detailed story of our own.	Theme 1: Privacy risks posed by companies and governments
"Privacy 101"	*Big Data* Companies and governments have been collecting a huge amount of data that construct big data and use them for proper or improper purposes. Therefore, we need stronger privacy laws and more access and understanding of how our data are used.	Theme 1: Privacy risks posed by companies and governments Theme 3: Call for increasing protection of privacy
	Communications Surveillance Mass communications surveillance conducted by governments contains network, tactical and centralized monitoring and poses threats to human rights.	Theme 1: Privacy risks posed by companies and governments
	Data Protection Data protection laws are deigned for protecting people's information and restricting its abuse, but contemporary laws should be improved with independent regulators needed.	Theme 3: Call for increasing protection of privacy
	Metadata Metadata are the "data about data" which reveal a detailed story of a person and are being collected by companies and governments. The circumstantial nature of metadata collected by governments can put you in danger by placing you within the network of a suspect.	Theme 1: Privacy risks posed by companies and governments
	What is Privacy? The right to privacy allows you to maintain control over your information, but it was hampered by the monitoring of governments and companies.	Theme 1: Privacy risks posed by companies and governments

4.3.1. Privacy Risks Posed by Companies and Governments

The two privacy activism campaigns shed light on privacy risks posed by companies and governments instead of the ones by malicious individuals that are the focus of the public education campaigns. The theme encapsulates how companies and governments pose threats to consumer digital privacy through information tracking, collection and so forth. It is comprised of four sub-themes or axial codes, a.k.a. “growth of privacy risks”, “privacy risks posed by companies”, “privacy risks posed by governments” and “company-government relation and Terms and Conditions”.

Growth of privacy risks refers to the tendency that the scale of risks posed by companies and governments on consumer digital privacy is enlarging. An important reason for the rise is the development of new technologies. Firstly, the increase of government surveillance is stressed. “Privacy 101” warns consumers that “the technologies of mass surveillance are becoming more prevalent, and as resource limitations disappear, the capabilities for governments become endless”. Therefore, not only is surveillance becoming increasingly commonplace, but governments are also getting more powerful. Secondly, the amount of data being collected and mined is rising. “Privacy 101” continues to emphasize that governments and companies are aggregating and analyzing a large amount of personal data from consumers, which is constructed as big data, and the data mining with the decision-making based on those data is expanding. Not only are governments and companies collecting personal information, but the digital traces that consumers leave every single day also cause the growth of data being tracked and collected. “With so many points of data available to be selected and analysed, the digital trail that we generate and our devices make available, taken together all the pieces give a more accurate picture of our lives than even we may be aware of”, according to “Privacy 101”. The campaign also stresses that more metadata tools are being developed and sold to governments and companies, which constitutes another reason for the rise of data collection.

Privacy risks posed by companies are associated with privacy violations conducted by companies, including marketers and Internet service providers, through their inappropriate handling of consumer information. Both campaigns have covered all four types of privacy violations of Solove (2006) concerning information collection, storage, dissemination and invasion. “Me and My Shadow” frequently mentions that when consumers use certain Internet services or products, their personal data end up in the hands of the businesses that offer those services or products. Those commercial

companies have a business model possibly involving in collecting and selling consumer data. “If the service itself is free, how does the company make money?” the campaign asks consumers. Both campaigns also highlight that companies analyze consumer information and engage in profiling meaning building profiles of consumers. Through using cross-referencing, they can create “a detailed picture” of a consumer, according to “Privacy 101”. Afterwards, companies can use the data for advertising or marketing purposes and even sell it for money to other companies or governments besides advertisers. Additionally, “Me and My Shadow” attaches importance to the location tracking by companies. Location information is being constantly tracked by mobile devices providers when consumers are using mobiles or by ISPs when consumers are using social media platforms, either of which violates “privacy of location and space” (Finn et al., 2013). As pointed out by Park and Jang (2014), consumer digital privacy literacy in terms of location-related knowledge in mobile use is considered inadequate. Thereby, the campaign’s focus on location tracking seems to be tailored to that insufficiency. As seen in Table 4, the axial code concerning digital privacy risks caused by companies is the most frequently mentioned sub-theme.

Privacy risks posed by governments relate to threats to consumer privacy casted by governments through their improper handling of consumer information. Similar to the risks caused by companies, both campaigns also cover all four types of privacy violations of Solove (2006), namely information collection, processing, dissemination and invasion. Both campaigns have pointed out that governments have access to consumer information and use it for different purposes. However, the major criticism on the wrongdoing of governments comes from “Privacy 101”. The campaign first agrees that it is understandable for governments to collect and analyze consumer data because they need the information for investigating crimes or countering terrorism. Nevertheless, the problem lies in the fact that the collection is expanding beyond merely collecting the information of suspects. In the video “What is Privacy” (see Table 5), it is stressed that “governments are not just watching terrorists”, and “they are watching all of us”. The video “Communications Surveillance” (see Table 5) further states that governments are trying to “collect it all”. Therefore, the campaign questions the honesty of governments in safeguarding consumer information by saying they “ignore” the fact that “what they are doing is a violation of their legal obligations”. The campaign even repeatedly conveys the message that surveillance of governments empowers the governments themselves but disempowers consumers. According to “Privacy 101”, “such (surveillance) equipment gives

governments a frightening amount of access to people's lives, allowing them to listen to phone calls, read emails, SMS messages, social networking messages and to extract data without a user's knowledge". Therefore, consumer's right to privacy is threatened by governments in the digital era.

Company-government relation and Terms and Conditions refer to information flows between companies and governments, which is mainly granted by Terms and Conditions and privacy policies. The two campaigns emphasize that companies and governments maintain close relationships with each other. Sometimes, governments do not have to collect consumer information by themselves. They can "directly access communications and metadata" from companies, such as "undersea cable companies, telephone companies and internet service providers", according to "Privacy 101". In the video "Communications Surveillance" (see Table 5), companies provide "unlimited unchecked access" to consumer information for governments. However, information flows between governments and private sectors are enabled by Terms and Conditions and privacy policies. Not only do they allow information flows between companies and consumers, but they also grant governments' access to the data collected by private sectors (Hoback et al., 2013; Solove, 2002b). With respect to those online agreements, the two campaigns are not limited to only asking consumers to read them or calling for their attention like what the two public education campaigns have done. They further criticize that those agreements are uncommunicative by saying they are "long" and "confusing" and they allow abuse of consumer information. Moreover, "Me and My Shadow" provides consumers with detailed introductions to privacy policies of LinkedIn, Facebook, Twitter, Instagram, Google and Whatsapp.

Based on the discussion of four axial codes, the first theme concerns how companies and governments are posing threats to consumer digital privacy through inappropriate handling of consumer information, with attention also paid to the information flows granted by Terms and Conditions between the two sides. Different from the two public education campaigns focusing on risks posed by malicious individuals, the privacy activism campaigns pay attention to those posed by companies and governments. Moreover, as seen from Table 5, the theme "privacy risks posed by companies and governments" has the most videos (five out of six) of the two campaigns. As it is also the most frequently mentioned theme compared to other two (see Table 4), both the educational material and videos have placed emphasis on this theme concerning privacy risks. It thus reflects Youn's (2009) advice on communicating privacy risks in privacy education, with little research examining the adoption of such a suggestion. The communication of risks posed by companies and

governments is also able to strengthen consumer digital privacy literacy, as “awareness of common institutional practices” is an important component of digital privacy literacy (Park, 2011).

4.3.2. Privacy Protection Strategies

As various threats to consumer digital privacy are presented, it is then important for the two privacy activism campaigns to help consumers cope with those privacy issues. Therefore, the second theme is about privacy protection strategies which encapsulate different tips or recommendations provided for protecting personal information and enhancing digital privacy. It contains three sub-themes, namely “devices and information protection measures”, “approach strategies” and “avoidance strategies”.

Devices and information protection measures relate to step-by-steps or tools consumers can use to better safeguard their digital devices and maintain their information online. The majority of these measures come from “Me and My Shadow”. Similar to the two public education campaigns, “Me and My Shadow” suggests keeping operating systems, software and apps up-to-date while setting strong passwords so that devices and online accounts of consumers are safeguarded from various harms on the Internet. It also stresses the importance of “https” and recommends using two-factor authentication to further protect their information and accounts. More than that, the campaign advises on turning to “alternative tools and platforms” instead of mainstream ones, such as Gmail, WhatsApp and so forth, which are owned by commercial companies. Three types of alternative tools suggested include email services, mobile chat apps and Google products. Those alternative tools, such as “Riseup”, “DuckDuckGo”, etc., are open-sourced and thus offer better protection of consumers’ data and do not keep track of their records, according to “Me and My Shadow”. It also suggests using tools or add-ons for blocking trackers, such as “Ghostery” and “Adblock Plus”, instead of security software beginning with “anti” recommended by public education campaigns. Additionally, the campaign also provides detailed step-by-step guides on how to adjust privacy settings on three platforms, namely Firefox, Chrome and Twitter, as default settings usually have the lowest privacy protection. For example, consumers are asked to check “content settings” on Chrome through clicking on “settings”, “show more advanced settings” and “privacy” one by one. Therefore, the above protection measures concern the technical aspect of privacy protection and are designed to raise consumer digital privacy literacy, considering that “familiarity with technical aspects of the Internet” is a crucial component of

digital privacy literacy (Park, 2011).

Approach strategies refer to approaches consumers can take to provide false or confusing information. Although approach strategies contain two aspects, namely "seek" and "fabricate" (Youn, 2009), only the latter aspect is reflected in the two activism campaigns. The aim of fabricating is to hide consumers' real identities and thus avoid being tracked by Internet service providers. Both campaigns strongly recommend using a virtual private network (VPN), as "Me and My Shadow" points out that it is an important method to "obfuscate" personal information. The same suggestion is also communicated in the two public education campaigns, but their aim differs from the one of privacy activism campaigns. The public education campaigns stress that consumers can use VPNs to protect themselves from malicious individuals when using public WiFi, while the privacy activism campaigns ask consumers to use VPNs so as to hide "part of your messages metadata, your location (IP address) and unique fingerprints of your device, from your internet service provider and others who have access your communication", according to "Privacy 101", meaning that the privacy activism campaigns target not only malicious individuals but also governments and companies like ISPs mentioned. The tool of "obfuscation" concerning using confusing information to disturb governments' and companies' information monitoring efforts is thus reflected in the activism campaigns (Brunton, & Nissenbaum, 2015). Both campaigns also communicate the importance of online anonymity. "Me and My Shadow" has step-by-step guides on creating anonymous accounts on Twitter by going through the following steps, "go to your browser → register with a pseudonym and an anonymous email account → skip the steps that require personal data".

Avoidance strategies refer to the recommended approaches that are about withholding sensitive information posted online. According to Youn (2009), avoidance strategies can be used for tackling digital privacy risks. "Me and My Shadow" advises consumers to refrain sharing information online and to limit who can have access to their personal information. Regarding that respect, the campaign suggests changing discoverability and limiting who can follow or make friends with consumers on social media platforms. The advice concerning limiting personal information posted online and who can see the information is also communicated in public education campaigns. Therefore, the four campaigns all regard the tips of "limit" or avoidance strategies as essential digital privacy protection measures. However, in the privacy activism campaigns, avoidance strategies are the least frequent privacy protection strategies (see Table 4).

From the description of three axial codes, it is seen that privacy protection strategies concern useful suggestions, both technical and non-technical ones, on helping consumers protect themselves from privacy risks online. From Table 4, devices and information protection measures are the most frequent axial code, while avoidance strategies are the least one. Therefore, the two campaigns focus more on the technical aspect of privacy protection. Also, the theme "privacy protection strategies" is not presented in any of the six videos from the two campaigns (see Table 5), even though it is not the least frequently mentioned theme (see Table 4). Based on the first and second theme, Youn's (2009) two approaches for coping with privacy risks and Park's (2011) three dimensions of privacy literacy are all covered in the privacy education driven by non-profits.

4.3.3. Call for Increasing Protection of Privacy

Call for increasing protection of privacy as the third theme encapsulates the need to increase and strengthen the insufficient protection of consumer digital privacy. While privacy protection strategies, which are the second theme, are suggested to tackle privacy risks posed by companies and governments, which are the first theme, call for increasing protection of privacy, which is the third theme, serves as another way to cope with the increasing digital privacy risks mentioned. The third theme consists of two axial codes, namely "status of privacy protection" and "demand for strengthening regulation and protection".

Status of privacy protection summarizes the recent legal protection of digital privacy by laws as well as the current nature of privacy protection maintained by governments and companies, both of which engage in data collection. It is stressed that legal protection of consumer privacy nowadays is considered insufficient. One of the main reasons for the insufficiency is attributed to the different pace of legal and technological development, with the development of technologies outpacing the modification of existing laws to adapt to the change. For instance, as pointed out by "Privacy 101", "laws governing communications surveillance have become outdated in the face of powerful new technologies", while "the greatest problem is that communications surveillance technology is not waiting around for legislation to catch up and reach those minimum standards". "Privacy 101" also provides a detailed introduction to data protection law designed to safeguard people's right to privacy through preventing their information from being abused. Although the law is coming into being and accepted by most countries, those countries "have not yet developed comprehensive data protection

law that applies to all business sectors and to government". Meanwhile, "Me and My Shadow" mentions the existence of the "right of access" in the EU that grants consumers permission to the data having been collected by companies and governments, but other countries might not recognize this right due to different legal nature of privacy in different countries or areas. Therefore, the inadequacy of current legal protection of data has been emphasized.

Next to the legal aspect of privacy protection, companies and governments that involve in collecting and monitoring consumer information also have the responsibility to safeguard consumer privacy and not to abuse consumer information. However, companies and governments not only fail to inform consumers of the collection and the use of their data but also show reluctance to better protect their digital privacy, according to "Privacy 101". For one thing, information about consumers is being tracked and flows of the information among different sectors are being generated "even without your knowledge". If consumers are not well informed about data collection and information use, the misconducts of those institutions constitute a violation of privacy, as being informed about information handling serves as an important dimension of consumer privacy (Caudill, Murphy, 2000). Thereby, "Privacy 101" describes the violation of privacy rights of consumers without their awareness as "perhaps the most significant challenge to privacy". For another, the campaign criticizes that companies and governments "have shown repeatedly that unless rules restrict their actions, they will endeavour to collect it all, mine it all, keep it all, while telling us nothing at all". Additionally, the video "What is Privacy" (see Table 5) states that those institutions "push hard against the law".

Demand for strengthening regulation and protection refers to the requests asking for better regulation of information collection and stronger protection of consumer digital privacy rights, with the call mostly coming from "Privacy 101". The campaign first stresses the importance of the right to privacy by describing it as a "fundamental right" that many other human rights are established upon and that builds "boundaries" to prevent others from intruding people's communications and accessing their information. The campaign is thus calling for increasing protection of the important right held by consumers. It claims that consumers should be "protected against arbitrary interference with their right to communicate privately" and further warns that "it must only be done in accordance with clear and transparent law", when governments are planning to collect their data and monitor their communications. Another call is placed on regulating data collection and aggregation practices and limiting the power of companies and governments. For instance, due to the rapid development and

popularity of big data, there is a lack of regulations surrounding big data. Because of the considerable amount and the confidential nature of those data, institutions that capture consumer information need to "be held to account for how they collected the information, how they put this information to use, and how individuals are affected by the use of this information, and whether individuals were granted the opportunity to engage with the system", according to "Privacy 101". When it comes to the growing power of companies and governments, it should be guaranteed that those institutions "don't abuse laws and loopholes to invade your privacy".

To summarize, the third theme concerning call for increasing protection of privacy demonstrates that the current digital privacy protection is insufficient and thus needs to be strengthened. Through requesting better protection of consumer digital privacy, the campaigns seem to spark actions from consumers. Not only do they need the privacy protection strategies, but they are also supposed to force regulations to move forward so that the regulations are able to better adapt to technological changes and thus better protect consumer privacy rights. Although the third theme from the two privacy activism campaigns is the least frequent theme in educational material (see Table 4), there are two videos (out of six) shedding light on the topic (see Table 5), compared to zero video on the second theme that ranks second in terms of frequency in textual educational material.

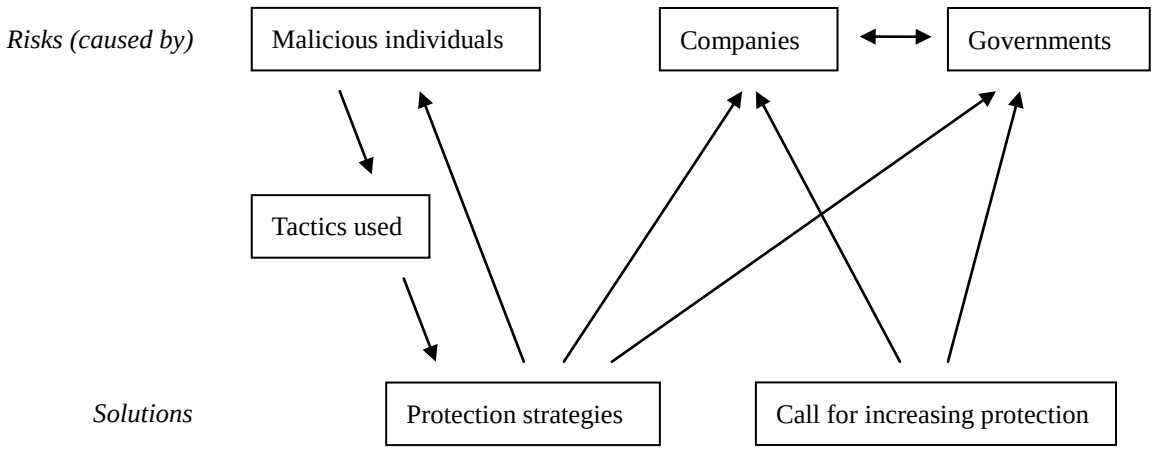
4.4. Comparison between Public Education and Privacy Activism Campaigns

Three themes from the public education campaigns and three from the privacy activism campaigns were discussed respectively in the last two sections. Figure 1 maps out the relationships among the themes, outlining the nature of the studied digital literacy campaigns. Firstly, digital literacy risks are communicated, with public education campaigns focusing on the ones caused by malicious individuals and privacy activism campaigns on those by companies and governments. The information flows between companies and governments are stressed by the two activism campaigns.

Secondly, regarding the increasing digital privacy risks, the campaigns provide solutions for consumers to tackle the privacy threats. For dealing with cyber security risks posed by malicious individuals, consumers are first offered the information concerning the common tactics used by malicious individuals. Knowing those tactics helps consumers better understand the risks and more importantly decide what protection strategies to use later. That is why the square of "tactic used" is placed between the square of risks caused by malicious individuals and the square of privacy

protection strategies. After showing those tactics, the public education campaigns provide protection strategies for consumers, which contain information and devices protection measures, avoidance and approach strategies as well as paying enough attention to Terms and Conditions and privacy policies. Similarly, in terms of tackling privacy risks posed by companies and governments, the privacy activism campaigns also offer protection strategies including information and devices protection measures and avoidance and approach strategies. Next to providing protection strategies, the activism campaigns also call for strengthening the insufficient protection of consumer digital privacy through regulating data handling practices and limiting the growing power of companies and governments, which is also considered another solution to the privacy risks.

Figure 1. *Relationships of themes in digital literacy campaigns*



During the above discussion, some similarities and differences between the two types of digital literacy campaigns were already touched upon but lack in-depth discussion. With respect to that, this section focuses on the comparison between the two types of campaigns in order to answer the second sub-question concerning how public education campaigns with huge involvement from governments differ from privacy activism campaigns solely developed by non-profits. Attention is first paid to the commonalities, and then differences are discussed.

4.4.1. Commonalities of Digital Literacy Campaigns

The two types of digital literacy campaigns share a certain degree of similarity in terms of the growth of digital privacy risks and some aspects of privacy protection strategies.

Firstly, the first themes of the two types of campaigns both focus on risks posed on consumer digital privacy. Both types of campaigns attach importance to the growth of privacy threats in the digital era. As seen in Table 2 and Table 4, the first axial codes of their first themes both concern the "growing" nature of privacy risks. According to "Get Cyber Safe", one of the two public education campaigns, the quantity of malware that can comprise consumers' devices and personal information is "growing exponentially". From the activism campaigns, "Privacy 101" stresses that as new technologies, not only the devices used by consumers but also the technologies used for tracking and monitoring information, are evolving, and "we move towards 'smart' devices and cities" with an increasing amount of consumers' activities and data being collected and aggregated. It is thus seen that with the advancement of modern technologies, consumer digital privacy is being placed under increasing danger, and the right to privacy can be threatened by anyone who has access to those technologies. The message concerning the growth of privacy risks is communicated through both types of campaigns, possibly with the purpose of letting consumers realize the severity of problems and take immediate actions to better manage their online privacy. As pointed out by Youn (2009), privacy risks can trigger privacy concerns of consumers and then lead to their privacy protection behaviors. Therefore, the communication of growing risks serves to enhance consumers' motivations in safeguarding their digital privacy.

Secondly, the two types of campaigns both provide privacy protection strategies for consumers to better safeguard their personal information online. From Table 2 and Table 4, the public education campaigns cover more strategies than the activism campaigns, but there are some overlapping strategies that are communicated by both. In terms of devices and information protection measures, they both stress the importance of updates, strong passwords, "https" and two-factor authentication while offering tips in relation to those aspects. Those tips are of great importance in protecting consumers' digital devices, online accounts and personal information. Both types of campaigns also regard deleting or cleaning information as an essential tip for managing digital privacy. For instance, in Chrome, "Get Cyber Safe" asks consumers to "go to the wrench icon in the top right hand corner"

and click on “Clear Browsing Data” under the Bonnet. Meanwhile, “Me and My Shadow” offers a similar routine, “Chrome → history and recent tabs → history → clear browsing data → select the beginning of time and check: all the items you want to be cleared → clear browsing data”.

When it comes to avoidance strategies, both types of campaigns demonstrate that it is important for consumers to refrain from sharing much personal information, especially sensitive and identifiable details, on the Internet and to limit the scope of people who can have access to their personal data. Regarding that respect, consumers are recommended to think twice before posting information on social media and to adjust their privacy settings to narrow the access to their information. The “refrain” strategies by Youn (2009) are thus communicated in both types of digital literacy campaigns.

Lastly, two types of campaigns both shed light on Terms and Conditions and privacy policies. They try to attract the attention of consumers to those online agreements. For example, “STOP. THINK. CONNECT.” asks consumers to “review” those Terms and Conditions and privacy policies and to “understand” how their data will be “accessed and shared”. Similarly, “Me and My Shadow” also emphasizes the need to read and understand those agreements by asking the question, “What did you actually ‘agree’ to?” Nevertheless, “Me and My Shadow” is doing more than just calling for attention, since it also provides further introductions to privacy policies from five mainstream platforms, namely LinkedIn, Facebook, Twitter, Instagram, Google and Whatsapp.

As mentioned, devices and information protection measures are mostly associated with technical aspects of privacy protection. Therefore, within the discussion of privacy protection strategies and Terms and Conditions, both types of campaigns aim at strengthening digital privacy literacy through focusing on consumers’ “familiarity with technical aspects of the Internet” and “understanding of current privacy policy”, which are two crucial dimensions of privacy literacy (Park, 2011).

4.4.2. Differences between Public Education and Privacy Activism Campaigns

In the former section, the two types of campaigns share some similarities in terms of the growing nature of digital privacy risks and privacy protection strategies. However, certain differences exist between them.

Firstly, although both types of campaigns communicate privacy risks to consumers, the type of privacy risks they focus on varies from each other (see Table 2 and Table 4). The risks addressed by public education campaigns are cyber security-related. Those privacy risks are caused by malware,

scams or frauds or other activities conducted by malicious individuals. They also label those malicious individuals as cyber criminals or strangers who aim at “stealing” personal information of consumers. For example, in terms of Wi-Fi eavesdropping, those malicious individuals can use public or unsecure WiFi to “capture” or “steal your personal information including logins and passwords”, according to “Get Cyber Safe”. The public education campaigns do mention information tracking, but the subjects who conduct it are malicious individuals, e.g., those who might use malware to “record usernames, passwords and other personal information”, instead of businesses or governments. On the other hand, the privacy risks posed by companies and governments, which are missed by public education campaigns, are just the focus of the two activism campaigns. As seen in the axial codes of the first theme in those two campaigns, privacy risks caused by companies and governments and their information flows are heavily addressed. Those risks cover Solove’s (2006) four types of privacy violations containing information collection, processing, dissemination and invasion. For example, “Privacy 101” points out the development of technologies has made it “possible for companies and governments to monitor every conversation we conduct, each commercial transaction we undertake, and every location we visit”. Thereby, the subjects who exercise privacy violations are different in the two types of campaigns, with malicious individuals targeted in public education campaigns and companies and governments addressed in activism campaigns.

Secondly, although both types of campaigns have the theme “privacy protection strategies”, there is a certain degree of difference in terms of the scope they cover. As for devices and information protection measures, both types of campaigns have recommendations on updates, passwords, two-factor authentication and others, but the difference comes from the safety-enhancing software or tools they suggest. The public education campaigns advise consumers to install security software that usually starts with “anti”, such as anti-virus, anti-spyware, etc. Most of the security software is used for tackling malware or malicious activities. However, “Me and My Shadow”, one of the activism campaigns, recommends using “alternative tools and platforms” to replace mainstream services, e.g., Google services, offered by commercial companies. It further suggests using add-ons to block trackers placed by companies, especially after cookies are accepted. Therefore, based on the tools they suggest, the public education campaigns aim to fight against malicious individuals, while the activism campaign against commercially-owned companies.

In terms of approach strategies, there are two dimensions, namely “seek” and “fabricate” (Youn,

2009). The aspect of “seek”, meaning turning to trustworthy agencies or people for help, is covered by the public education campaigns but not emphasized in the privacy activism campaigns. As for another aspect of “fabricate” concerning providing confusing information, both types of campaigns recommend using a virtual private network (VPN). The difference lies in that consumers are advised to use VPNs to prevent themselves from the scrutiny of malicious individuals in the public education campaigns; however, the activism campaigns suggest using VPNs to hide “part of your messages metadata, your location (IP address) and unique fingerprints of your device, from your internet service provider and others who have access your communication”. With malicious individuals targeted in the public education campaigns, the activism campaigns target companies and possibly governments or other individuals who are able to access consumers’ communications.

For avoidance strategies, although two types of campaigns both advise consumers to limit the information posted online and the access to their information, the public education campaigns cover broader scope of the strategies. For example, they ask consumers to avoid clicking on suspicious links or attachments. According to “STOP. THINK. CONNECT.”, “links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer”. This respect is not covered in the activism campaigns.

Additionally, as for Terms and Conditions, both types of campaigns have called for consumers’ attention to those agreements. The public education campaigns are only limited to the action of calling, such as asking consumers to read them, while the activism ones are doing more than that. They further make consumers aware of the negative consequences of clicking “agree”. For instance, “Me and My Shadow” mentions those consequences include “entrusting our email provider with a lot of personal information - think about all the things that go through your inbox on a daily basis”, while “Privacy 101” stresses that “once it is in a company's hands through a contractual agreement, they can do what they want with it, whether that it malicious or harmless”. The public education campaigns have not reached this step to highlight the dark side of Terms and Conditions.

Thirdly, the activism campaigns, especially “Privacy 101”, engage in calling for social changes, which can be shown in their third theme “calling for increasing protection of privacy”. The campaigns have realized the importance of the right to privacy as a fundamental human right and the insufficient protection by laws and powerful institutions. Through communicating the message that privacy rights are important with more privacy protection needed, the activism campaigns are seemingly calling

consumers to take actions for social changes, especially considering that the word “we” is used frequently. For example, “Privacy 101” states that “we should be able to have access to our information, and we must have the right to challenge the information held and to seek its deletion, rectification, completion or modification”, and “we believe that in order for individuals to participate in the modern world, developments in laws and technologies must strengthen and not undermine the ability to freely enjoy this right”. It is also regarded as another away to tackle the privacy risks posed by companies and governments, next to privacy protection strategies. However, the calling for changes in the society is missed out in the public education campaigns. Moreover, the activism campaigns seem to contain more legal information. Not only does “Me and My Shadow” bring up the “right of access” in the EU, but “Privacy 101” also introduces data protection laws and some legal progress in protecting consumer privacy. For instance, in spite of the increase in surveillance, “courts and civil society have been making efforts address some of the dated ideas of communications surveillance”. However, the public education campaigns mention little information regarding the legal aspect except for asking consumers to turn to governmental agencies for help.

Based on the above discussion of differences, it is also detected where the two types of campaigns stand in the consumer-company and consumer-government relationship (Culnan, & Bies, 2003). The public education campaigns represent the for-company and for-government perspective. For one thing, the campaigns do not touch upon the privacy risks posed by companies and governments, although they involve in various privacy violations pointed out by the activism campaigns. For another, the public education campaigns suggest turning to companies like ISPs or governmental agencies like the Office of the Privacy Commissioner in Canada for help if consumers are in trouble. They further point out that cyber security risks caused by malware not only pose threats to consumer digital privacy but also have a negative impact on businesses. While the campaigns are standing for companies and governments, it is confusing to say they are against consumers, as they are educating consumers through the campaigns per se.

On the other hand, the two privacy activism campaigns represent the for-consumer perspective and are meanwhile against companies and governments. For one thing, although it is acceptable for governments and companies to collect and analyze consumer data for legitimate reasons, the campaigns point out that they “collect it all” and use those data for more purposes beyond merely investing crimes and countering terrorism. Therefore, in the dispute between national security and

individual privacy, the campaigns support the for-privacy perspective and thus stand for consumers. For another, the campaigns focus on digital privacy risks specifically posed by companies and governments and provide privacy protection strategies for consumers to safeguard themselves from data tracking by companies and governments, while actively calling for regulating and limiting the power of those institutions. They even question the honesty of those institutions. For instance, “Me and My Shadow” asks, “Most companies claim that they don’t identify you by name when they hand over a profile of you - but what does that really mean, when you can be identified easily through all the other information included?” Meanwhile, “Privacy 101” blames governments for overlooking that “what they are doing is a violation of their legal obligations, and placing the burden on individuals”. Therefore, the activism campaigns stand against companies and governments.

Besides where they are situated in the consumer-company and consumer-government relationship, it is also found how the two types of campaigns interpret digital privacy differently. As mentioned, the activism campaigns cover a considerable amount of legal information. For example, the “right of access” is brought up in “Me and My Shadow”, while data protection laws are introduced in “Privacy 101”. With regard to that respect, the campaigns tend to regard consumer privacy as a human right, compared to the public education campaigns. For example, privacy is considered as a “fundamental right” in “Privacy 101”. The conceptualization of privacy as a human right, the “right to be let alone”, has been recognized by Warren and Brandeis (1890).

Additionally, the public education and activism campaigns both attach importance to the protection of electronic devices and consumer data in those devices as well as online, since both have the axial code of devices and information protection measures (see Table 2 and Table 4). Therefore, in terms of seven types of privacy by Finn et al. (2013), “privacy of data and image” referring to information of consumers has been emphasized by both types of campaigns. However, consumer privacy is not merely limited to the information they have. Privacy activism campaigns cover privacy issues beyond the privacy of consumer information and thus include “privacy of communication” and “privacy of association” (Finn et al., 2013). Under the theme “privacy risks posed by companies and governments”, the activism campaigns point out that communications surveillance, such as “UK’s Tempora program”, violates consumer’s right to privacy, specifically the “privacy of communication”. According to “Privacy 101”, “communications surveillance is a significant interference with this fundamental need to communicate”. Regarding “privacy of association”, the campaign highlights that

communication surveillance intrudes “individuals’ private lives and associations”. The video “Big Data” also points out that with the relationships and communications among consumers being analyzed, any of them can be “wrongly identified as terrorists”. Therefore, based on how the two types of campaigns address privacy issues, it is seen that they have different interpretation regarding the concept of privacy, with the activism campaigns tending to consider privacy as a human right and focusing on more aspects of privacy than the public education campaigns. The results drive the field of study from general interpretations of privacy towards the comparison of nuanced interpretations held by different institutions.

As the four campaigns come from four different countries with more or less different ecologies, the country of origin can also affect the scope of privacy issues those campaigns focus on. “STOP. THINK. CONNECT.” from the US focuses on cyber security risks caused by malicious individuals and hardly criticizes privacy threats posed by companies or governments. In the Apple-FBI dispute, the US government seemed to take its access to San Bernardino shooter’s smartphone for granted. As the campaign has heavy involvement of the US government, it makes sense for the campaign not to criticize the government. Also, the US only has the sectoral level of privacy regulation, which is between the level of no regulation and the omnibus level (Bellman et al., 2004), showcasing that privacy violations conducted by companies and governments might receive weaker oppositions from consumers. That could be another reason why risks caused by malicious individuals are emphasized instead. On the other hand, Germany and the UK have the omnibus level of privacy regulation (Bellman et al., 2004). According to Bennett (2010), European countries tend to have better data protection legislation. The power of companies and governments is thus more restrained, making any wrongdoing on their side more unacceptable for consumers. That could be the reason why “Me and My Shadow” and “Privacy 101” developed by two non-profits based in Germany and the UK respectively have stressed the risks caused by companies and governments.

4.5. Social Media Use of Digital Literacy Campaigns

After discussing how the digital literacy campaigns educate consumers on privacy issues through textual educational material and videos on the websites, it is important to shed light on how those campaigns create outreach and engage with their audiences through social media, as social media are crucial to the success of diverse campaigns (Hanna et al., 2011). Since Facebook as an important

social networking site is focused on in the analysis, the current section explores how the four campaigns make use of the platform. The use of Facebook for engagement through relationship cultivation strategies is first discussed, followed by the discussion of what types of themes are communicated through the Facebook posts analyzed.

4.5.1. Social Media Engagement

Three main relationship cultivation strategies, namely "disclosure", "information dissemination" and "involvement", from Waters et al. (2009) are examined, in terms of how the campaigns or institutions behind use Facebook. There are different elements under each strategy. Table 6 summarizes whether those elements are presented on the Facebook profiles and the analyzed posts.

Table 6. *Relationship cultivation strategies used on Facebook*

	"Get Cyber Safe"	"STOP. THINK. CONNECT."	Tactical Tech ("Me and My Shadow")	Privacy International ("Privacy 101")
Disclosure				
Description	yes	yes	yes	yes
History	yes	yes	yes	yes
Mission statement	yes	yes	yes	yes
URL	yes	yes	yes	yes
Logo	yes	yes	yes	yes
Administrators listed	no	no	no	no
Information dissemination				
News links	yes	yes	yes	yes
Photo posted	yes	yes	yes	yes
Video files	yes	yes	yes	yes
Audio files	no	no	no	no
Posted announcements	yes	yes	no	no
Discussion wall	no	no	no	no
Press releases	no	no	yes	no
Campaign summaries	yes	yes	yes	yes
Involvement				
E-mail to organization	no	yes	yes	yes
Phone number	yes	no	no	yes
Message board used	yes	no	yes	yes
Calendar of events	yes	yes	yes	no
Call for actions	yes	yes	yes	yes
Store	no	no	no	no

The first relationship cultivation strategy is “disclosure”. As shown in Table 6, the two public education campaigns both have description, history, mission statement, URL (to the campaign’s website) and logo of the campaigns. Similarly, the two non-profits that developed the two privacy activism campaigns respectively also have the five elements, namely description, history, mission statement, URL and logo of the organizations. However, administrators are not listed in any of the four Facebook accounts. Therefore, the four campaigns or institutions behind have all the elements of “disclosure”, except a listing of administrators.

As for strategy of “information dissemination”, the first three elements, a.k.a. news links, photos and videos, and the last one, campaign summaries, are all presented across the four Facebook accounts. On the contrary, the element of audio files and discussion wall are absent across all the accounts. The rest of the elements within the strategy are partly presented. For posted announcements, which are usually located on the left side on a Facebook page, the two public education campaigns have adopted the function, while the two non-profits do not use the function. Lastly, for links to press releases, only Tactical Tech has used those links in the analyzed posts, while the rest of the accounts do not include those links. For example, Tactical Tech has four Facebook posts containing the links to press releases on its website, and one of those posts concerns digital security practices of human rights defenders and contains a link to an article regarding the topic on the newsroom of its website.

The last strategy is “involvement”. Only the element of “call for actions” is presented in all the Facebook accounts. It is an important element of “involvement”, as it calls audiences to take actions and participate in certain activities. For instance, “Get Cyber Safe” asks young people to speak out by posting “youth can play an important role in stopping cyberbullying by telling others it’s not OK”, while “STOP. THINK. CONNECT.” has a post asking audiences to take part in an event on protecting online accounts and personal information through two-factor authentication. For non-profit organizations, Tactical Tech calls for joining its project named “That’s Not Privacy” concerning changing the misleading name of “privacy policy”, while Privacy International posts one of its projects called “Don’t Spy on Us” about fighting against authoritarian surveillance. Therefore, the four campaigns or institutions behind actively engage with audiences through calling for actions. Based on how the two types of campaign call for actions on social media, it is also seen that the activism campaigns are aiming at causing social changes.

On the other hand, “store” is not found in any of the Facebook accounts. The remaining elements

are partly presented among the four Facebook accounts. All the accounts, except the one of "Get Cyber Safe", have included email in their Facebook profiles. For phone number, the account of "Get Cyber Safe" and the one of Privacy International both have provided the number, while "STOP. THINK. CONNECT." and Tactical Tech do not have the element. In terms of message board, only "STOP. THINK. CONNECT." does not use this interactive function. Lastly, all Facebook accounts, except the one of Privacy International, use calendar of events on their profiles.

Based on the above discussion, all four Facebook accounts have adopted three relationship cultivation strategies, namely "disclosure", "information dissemination" and "involvement", to varying degrees. As for the two accounts of non-profit organizations, the majority of elements of "disclosure" are presented, which further confirms the finding of Waters et al. (2009) that non-profits adopt the disclosure strategy the most often. In the research of Waters et al. (2009), none of the studied non-profit organizations in the sphere of education use "audio files" under "information dissemination" and "store" under "involvement". The same results are also reflected in this thesis, as "audio files" and "store" are not found in the accounts of both non-profit organizations. As for public education campaigns, the majority of elements of "disclosure" are also found in their Facebook accounts, compared to the other two strategies. Therefore, the two campaigns together with the two non-profit organizations use the disclosure strategy more actively.

4.5.2. Education through Social Media

The profile and twenty posts of each Facebook account were analyzed to discover the use of relationship cultivation strategies. Meanwhile, what types of content are communicated through the analyzed Facebook posts were also looked into. As mentioned in the methodology, it is explored how the four Facebook accounts communicate the themes that emerge from the textual educational material (see Table 7).

Table 7. *Types of content communicated through Facebook posts*

Campaign	Theme	Frequency
"Get Cyber Safe"	Theme 1: Cyber security risks on digital privacy	2
	Theme 3: Privacy protection strategies	11
	Other privacy issues	2
	Other issues unrelated to privacy	5

"STOP. THINK. CONNECT."	Theme 1: Cyber security risks on digital privacy	1
	Theme 2: Tactics used by malicious individuals	1
	Theme 3: Privacy protection strategies	7
	Other privacy issues	3
	Other issues unrelated to privacy	8
Tactical Tech ("Me and My Shadow")	Theme 1: Privacy risks posed by companies and governments	3
	Theme 2: Privacy protection strategies	5
	Other privacy issues	3
	Other issues unrelated to privacy	9
Privacy International ("Privacy 101")	Theme 1: Privacy risks posed by companies and governments	8
	Theme 3: Call for increasing protection of privacy	11
	Other issues unrelated to privacy	1

In the twenty analyzed Facebook posts of "Get Cyber Safe", most posts (11 out of 20) are associated with privacy protection strategies. Specifically, among the eleven posts about the theme, most of them concern information and devices protection measures, such as enhancing password security, turning to multi-factor authentication, adjusting browser's security settings, keeping devices up-to-date and so forth. One of those posts touches upon the avoidance strategies by warning consumers not to download anything suspicious. "Cyber security risks on digital privacy" is another theme communicated through the analyzed posts (2 out of 20). The two posts are related to the danger of mobile viruses and location tracking of cyber criminals on mobile devices.

As for the Facebook account of "STOP. THINK. CONNECT.", seven out of twenty posts are related to privacy protection strategies. Specifically, all of them are about information and devices protection measures, such as password security, two-factor authentication, updates, etc. Only one post relates to the theme of cyber security risks, and the risk mentioned is conducted by a "cyber intruder" who "broke into a database" that contains a huge amount of information. Similarly, there is also only one for the theme "tactics used by malicious individuals", with the tactic mentioned associated with the use of "threat" where scammers claim that "your email has been hacked" and they will "take legal action against you" if they are not allowed to fix the problem.

In terms of privacy activism campaigns, Tactical Tech has five (out of twenty) posts about privacy protection strategies. They are mostly about taking control of personal information, with a "Privacy Pocket" and workshops regarding controlling data recommended. Three posts shed light on privacy risks posed by companies and governments. One of the three posts shares an outside post

about Big Brother's watching, while one concerns "fitness trackers", the information tracking in personal trainers. Another one is about a project called "That's Not Privacy" concerning changing the misleading name of "privacy policy". However, while three out of twenty posts are about other privacy issues, the majority of the analyzed posts (9 out of 20) are unrelated to privacy issues.

As for Privacy International, there are eleven out of twenty posts about the third theme, "call for increasing protection of privacy", while eight posts are about the first theme, "privacy risks posed by companies and governments". For the posts about calling for increasing protection of privacy, most of them concern the status of privacy rights and surveillance practices in several countries, such as Ireland, Thailand, Tanzania and others. Meanwhile, two of those posts are about a project called "Don't Spy on Us" that calls for limiting surveillance practices. For posts about privacy risks, most of them concern the discussion of controversial Investigatory Powers Bill that can potentially pose risks towards people's privacy. It is seen that most of the posts analyzed have repeated the themes that emerged from textual educational material.

To sum up, in the two Facebook accounts of public education campaigns, "privacy protection strategies" is the main theme, compared to the other two themes of public education campaigns, although there are quite some posts concerning issues outside of the three themes. As "privacy protection strategies" is also the most frequently mentioned theme in the analyzed educational material and videos, the theme serves as the focal theme across three channels. For privacy activism campaigns, the analyzed Facebook posts of Tactical Tech and Privacy International have only one theme in common that is "privacy risks posed by companies and governments", in terms of the three themes of privacy activism campaigns. Privacy International seems to actively engage in driving social changes, as most of the posts are about the theme of "call for increasing protection of privacy" with two of them about the project "Don't Spy on Us". Tactical Tech has also engaged in causing social changes to some extent, since there is a post about the project named "That's Not Privacy".

5. Conclusion

5.1. Discussion and Conclusion

The thesis studies four digital literacy campaigns from four countries. Two campaigns are public education campaigns, while the other two are privacy activism campaigns. Based on the discussion of two sets of themes emerging from the textual educational material of the two types of campaigns respectively, it is concluded that contemporary digital literacy campaigns communicate various digital privacy risks and meanwhile provide solutions to the risks consumers are encountering. As the communication of those themes is further strengthened through videos and social media, the campaigns also create their outreach and engage with consumers on Facebook using relationship cultivation strategies.

In order to answer the first sub-question concerning the nature of contemporary digital literacy campaigns, Figure 1 already maps out the types of digital privacy issues addressed by the four campaigns studied. First of all, the digital literacy campaigns studied communicate digital privacy risks to consumers. Those privacy risks are caused by three main actors, namely malicious individuals, companies and governments. The two public education campaigns demonstrate that malicious individuals threaten consumer digital privacy mainly in the form of malware and scams or frauds online. The activism campaigns stress that companies and governments violate consumer digital privacy through information collection, processing, dissemination and invasion and through information flows between the two institutions. While communicating the privacy risks, the four digital literacy campaigns also convey the message about the growth of those risks. The dissemination of information on digital privacy risks and their growing nature responds to Youn's (2009) recommendation on emphasizing risks in privacy education, concerning that the emphasis can contribute to the adoption of privacy protection behaviors. The findings further reveal the application of such a recommendation in contemporary privacy education through digital literacy campaigns.

To educate consumers on how to tackle the digital privacy risks, the digital literacy campaigns provide privacy protection strategies that include information and devices protection measures and avoidance and approach strategies. The tactics used by malicious individuals mediate the relationship between privacy risks caused by malicious individuals and privacy protection strategies (see Figure 1), as understanding those tactics helps determine the strategies to be used. At the same time, the activism

campaigns demand that the protection of consumer digital privacy should be enhanced, serving as another solution to the digital privacy risks specifically posed by companies and governments. While asking for any changes in terms of legal protections and on the side of companies and governments, they also seem to mobile consumers to become part of the advocacy cohort so as to make those changes happen. Additionally, privacy protection strategies serve as the focal theme in both the textual educational material and videos of the public education campaigns, while the activism campaigns communicate privacy risks caused by companies and governments the most in both their textual educational material and videos.

The nature of and the digital privacy issues addressed in the four digital literacy campaigns show that the campaigns aim to enhance the factual and procedural knowledge of consumers in terms of digital privacy literacy, connecting with the privacy literacy studies of Park (2011), Trepte et al. (2015) and Youn (2009). Park's (2011) three dimensions of digital privacy literacy would serve as the factual knowledge concerning "knowing that". The information and devices protection measures offered by the digital literacy campaigns mostly relate to "familiarity with technical aspects of the Internet", while the communication of violations of consumer digital privacy conducted by businesses and governments serves to raise consumers' "awareness of common institutional practices", as those violations concern data handling practices of the two types of institutions. Meanwhile, the call for attention to Terms and Conditions and privacy polices by the campaigns aims to increase consumers' "understanding of current privacy policy". As for the procedural knowledge concerning "knowing how", it is intertwined with Youn's (2009) two types of privacy risks coping strategies, namely approach strategies and avoidance strategies. Both types of strategies emerged as axial codes under the theme "privacy protection strategies". The digital literacy campaigns communicate approach and avoidance strategies to consumers by asking them to provide confusing information and refraining from sharing much personal information online.

More importantly, the campaigns also aim to raise consumers' awareness of tactics used by cyber criminals and their abilities to facilitate social changes pertaining to better privacy protection by laws and such institutions as businesses and governments. Since the two aspects have not been covered by the above-mentioned digital privacy literacy studies, the findings add "awareness of tactics used by cyber criminals" and "abilities to facilitate social changes" to the existing dimensions of digital privacy literacy.

Within the digital literacy campaigns, public education campaigns and privacy activism campaigns are compared. With regard to the second sub-question concerning the comparison, the two types of campaigns differ from each other to certain extent, although some similarities concerning the growing nature of privacy risks and part of privacy protection strategies are shared. In terms of the consumer-company relation, the public education campaigns represent the for-company perspective by portraying companies as victims of cyber security risks and asking consumers to seek help from companies. On the contrary, the privacy activism campaigns stand against companies through emphasizing their violations of privacy rights due to their inappropriate handling of consumer data, which is in line with the activist perspective pertaining to the consumer-company relation (Culnan, & Bies, 2003). As for the consumer-government relation, the public education campaigns are shown to stand on the government side, while activism campaigns are against governments by citing their wrongdoings. Another sign of the opposition towards governments by the activism campaigns is that they stand for individual privacy in the security-privacy debate through demonstrating their disbelief of governments' data collection for merely countering crimes and terrorism. Their perspective is hence for-privacy, aligning with the view of privacy advocates in the Apple-FBI dispute.

Furthermore, the two types of digital literacy campaigns imply that governments and non-profits as advocacy groups have different interpretations of consumer digital privacy. The privacy activism campaigns tend to regard privacy as a fundamental human right. As pointed out by Bennett (2010), privacy activism involves in advocating the right to privacy. On the other hand, the public education campaigns tend to see privacy as consumer information, e.g., personal data and images. The different interpretations and different focus on digital privacy risks could be related to the difference in terms of country of origin. As the US has a different level of privacy regulation and data protection legislation from Germany and the UK, it might influence how privacy is interpreted in the two types of campaigns and the scope of privacy risks they focus on. However, the further examination, especially quantitatively, of how the factor of country of origin influences the communication of privacy issues in digital literacy campaigns is suggested for future research.

To answer the third sub-question concerning engagement and education through social media, Facebook was selected as the platform of analysis. The Facebook accounts of the four campaigns or institutions behind use "disclosure" more actively than "information dissemination" and "involvement" in terms of relationship cultivation strategies, although all four accounts engage in

calling for actions of consumers and asking them to participate in relevant activities. The finding that the disclosure strategy is mostly used by Tactical Tech and Privacy International further confirms the finding of Waters et al. (2009) that non-profits use “disclosure” the most often. Furthermore, the themes of textual educational material are communicated through the Facebook posts analyzed to varying degrees. For public education campaigns, “privacy protection strategies” is the most frequently mentioned theme not only in the textual educational material and videos but also in the Facebook posts, and therefore it serves as the focal theme across all three channels. For activism campaigns, “privacy risks posed by companies and governments” is the focal theme across three channels.

In conclusion, the digital literacy campaigns from four countries educate consumers on privacy issues through communicating the digital privacy risks posed mainly by malicious individuals, companies and governments while offering solutions for consumers to tackle those risks, using the website as a main platform and social media for engagement and further education. While providing avoidance and approach strategies for consumers to improve their procedural knowledge, the campaigns also aim to strengthen consumers’ factual knowledge concerning familiarity with technical privacy protection strategies, knowledge of institutional practices and attention to Terms and Conditions. Next to that, the campaigns are also found to improve their “awareness of tactics used by cyber criminals” and “abilities to facilitate social changes”, and these two newly spotted aspects are added to the existing dimensions of digital privacy literacy. The thesis uncovers that the Youn’s suggestion of actively communicating risks in privacy education has been applied by contemporary digital literacy campaigns, while confirming Waters et al. (2009) when it comes to the heavy use of “disclosure” strategy in Facebook engagement of non-profits.

Lastly, based on the above conclusion, the thesis further provides a model for the future development of a comprehensive digital literacy campaign for privacy education. Two indispensable elements, namely “privacy risks” and “risk-coping solutions”, should be taken into account. Firstly, the campaign needs to covey the most recent privacy risks and violations. To maintain a neutral tone, it should cover the risks caused by various actors. Therefore, not only should malicious individuals and cyber criminals be focused on, but it is also important to communicate the violations by businesses and governments. The campaign should then attach importance to the mechanisms behind those risks, e.g., approaches and tactics used by the above three actors to harm consumers’ digital

privacy, when introducing different types of privacy risks. Secondly, a comprehensive campaign is supposed to recommend practical solutions to the privacy risks at hand. Those solutions can include technical protection measures (e.g., step-by-steps on how to set up strong passwords or how to adjust privacy settings) and strategies that concern refraining from sharing detailed information online and providing confusing information if necessary. In other words, the themes spotted in this research serve to provide implications and construct an alternative pattern for future digital privacy education. Additionally, social media like Facebook should be used to create outreach and facilitate engagement so that the education and communication can be more effective. With the disclosure strategy used more often by the studied campaigns, future campaigns should place more emphasis on the involvement strategy that has more interactive features.

5.2. Limitations

The thesis analyzed four digital literacy campaigns from four different countries. As the thesis aims to gain insights into contemporary campaigns rather than to generalize findings, the selection of the four campaigns is not based on scientific sampling or random sampling. Due to the feasibility and a limited time frame, only four campaigns were chosen. However, if more campaigns could be analyzed, a broader insight into the nature of contemporary digital literacy campaigns would be achieved. Also, the four campaigns come from Canada, the US, Germany and the UK, all of which are considered western or developed countries. The thesis did not choose any campaigns from non-western or developing countries because some of them have not developed comprehensive digital literacy campaigns or some do not provide English versions even though they have relevant campaigns. Therefore, future research that can dive into campaigns from non-western or developing countries to see what types of digital privacy issues they focus on and how they are communicated is highly suggested.

As the thesis mainly focuses on textual educational material that constitutes most part of the website of each campaign, another limitation is the lack of analysis of visual education material in pictures and videos as well as the lack of the depth concerning two extra analyses which are the video analysis and Facebook analysis. Visuals can be powerful in persuasive communication and thus are able to increase effectiveness of privacy education through digital literacy campaigns. However, due to the feasibility and issues of scope, visual data were not analyzed. Also, each video is analyzed

based on only its title and summary instead of the whole video. For social media analysis, only Facebook was chosen, although the four campaigns or institutions behind also have other platforms in common, such as Twitter. However, it must be remembered that the textual educational material is the major information on the websites, and the videos and Facebook analysis both serve as two superficial or supplemental analyses.

5.3. Future Research

In response to the above-mentioned limitations, certain suggestions for future studies are provided in this section. As mentioned, the thesis only pays attention to digital literacy campaigns from western or developed countries. Future research focusing on campaigns from non-western or developing countries is recommended. Also, in the discussion supra, it is suggested that future research can examine the effect of country of origin on the communication of privacy issues in digital literacy campaigns, either quantitatively or through combining quantitative and qualitative analysis. Since the nature of privacy rights and protection is already different within western or developed countries and can be more different between western and non-western countries or between developed and developing countries, it is also suggested that future research can compare digital literacy campaigns from the two types of countries. Additionally, studies can look into how digital literacy campaigns make use of visuals to better educate consumers and even combine the analysis of textual and visual material, as visual data was not touched upon in this research.

Lastly, the above discussion of limitations and future research mostly concerns the “how” of privacy education and communication of privacy issues through digital literacy campaigns. As discussed in the theoretical framework, there are two types of research pertaining to consumer education, with one about the “how” and the other on the “outcome”. Therefore, future research can study the effectiveness of the four campaigns in the thesis or probably other campaigns outside of the four to see how much effect the contemporary digital literacy campaigns have on consumers’ knowledge and behaviors, especially the changes in their understanding and behaviors. Focus groups or experiments can be a possible research method for finding out the effectiveness of those campaigns.

References

About Privacy International. (n.d.). Retrieved from https://www.privacyinternational.org/node/5

About STOP. THINK. CONNECT. (n.d.). Retrieved from https://www.stopthinkconnect.org/about

About Tactical Tech. (n.d.). Retrieved from https://tacticaltech.org/about

Adkins, N. R., & Ozanne, J. L. (2005). Critical consumer education: Empowering the low-literate consumer. *Journal of Macromarketing, 25*(2), 153-162.

Aimeur, E., Gambs, S., & Ho, A. (2010, February). Towards a privacy-enhanced social networking site. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on* (pp. 172-179). IEEE.

Aïmeur, E., & Schőnfeld, D. (2011, July). The ultimate invasion of privacy: Identity theft. In *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on* (pp. 24-31). IEEE.

Altman, I. (1976). Privacy: "A conceptual analysis". *Environment and Behavior, 8*(1), 7.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*(2), 107-123.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).

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), 313-324.

Bennett, C. J. (2010). *The privacy advocates.* Mit Press.

Berson, I. R., & Berson, M. J. (2006). Children and their digital dossiers: Lessons in privacy rights in the digital age. *International Journal of Social Education, 21*(1), 135-147.

Boeije, H. (2010). *Analysis in qualitative research.* London: Sage (pp. 93-121).

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

Bruck, J. (2013, May 7). The Bobs announce winners of online activism award. *Deutsche Welle*. Retrieved from http://www.dw.com/en/the-bobs-announce-winners-of-online-activism-award/a-16794236

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: A user's guide for privacy and protest.*

Cambridge: MIT Press.

Byford, K. S. (1998). Privacy in cyberspace: Constructing a model of privacy for the electronic communications environment. *Rutgers Computer & Tech. LJ, 24*, 1.

Bygrave, L. A. (2015). A right to be forgotten?. *Communications of the ACM, 58*(1), 35-37.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7-19.

Cho, M., Schweickart, T., & Haase, A. (2014). Public engagement with nonprofit organizations on Facebook. *Public Relations Review, 40*(3), 565-567.

Clarke, R. (2006). *Introduction to dataveillance and information privacy, and definitions of terms.* Canberra: Xamax Consultancy Pty Ltd. Retrieved from: http://www.rogerclarke.com/DV/Intro.html

Coiro, J., Knobel, M., Lankshear, C., & Leu, D. J. (Eds.). (2014). *Handbook of research on new literacies.* Routledge.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing, 9*(2), 10-19.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323-342.

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing, 17*(2), 34-51.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46*(4), 81-83.

Erlandsson, F., Boldt, M., & Johnson, H. (2012, September). Privacy threats related to user profiling in online social networks. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)* (pp. 838-842). IEEE.

Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia, 13*(1), 93-107.

Eurobarometer. (2010). *Attitudes on data protection and electronic identity in the European Union.* Brussels: European Commission.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In *European data protection: coming of age* (pp. 3-32). Springer Netherlands.

Forman, J., & Damschroder, L. (2008). Qualitative content analysis. *Empirical Research for Bioethics: A Primer. Oxford, UK: Elsevier Publishing,* 39-62.

Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing,* 106-119.

Franzak, F., Pitta, D., & Fritsche, S. (2001). Online relationships and the consumer's right to privacy. *Journal of Consumer Marketing, 18*(7), 631-642.

Gindin, S. E. (2009). Nobody reads your privacy policy or online contract: Lessons learned and questions raised by the FTC's action against Sears. *Nw. J. Tech. & Intell. Prop., 8,* 1.

Goodchild, J. (2010, October 7). 'Stop.Think.Connect.' campaign launched to curtail risky online behavior. *CSO.* Retrieved from http://www.csoonline.com/article/2126025/security-awareness/-stop-think-connect---campaign-launched-to-curtail-risky-online-behavior.html

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing,* 149-166.

Hanna, R., Rohm, A., & Crittenden, V. L. (2011). We're all connected: The power of the social media ecosystem. *Business Horizons, 54*(3), 265-273.

Hans, G. S. (2012). Privacy policies, Terms of Service, and FTC enforcement: Broadening unfairness regulation for a new era. *Mich. Telecomm. & Tech. L. Rev., 19,* 163.

Hoback, C. (Producer & Director), Ramos, J. (Producer), & Khanna, N (Producer). (2013). *Terms and Conditions may apply* [Motion picture]. United States: Hyrax Films.

Houghton, D. J., & Joinson, A. N. (2010). Privacy, social network sites, and social relations. *Journal of Technology in Human Services, 28*(1-2), 74-94.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288.

Janssen, S., & Verboord, M. (2015). *Methodological guidelines thesis research.* Department of Media & Communication. Erasmus School of History, Culture and Communication. Erasmus University Rotterdam, Netherlands

Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. *Project MAC: MIT Project on*

Mathematics and Computing, 1, 1-76.

Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education, 2*, 35.

Klitou, D. (2014). *Privacy-invading technologies and privacy by design.* TMC Asser Press.

Langrehr, F. W. (1979). Consumer education: Does it change students' competencies and attitudes?. *Journal of Consumer Affairs, 13*(1), 41-53.

Leu, D. J., Kinzer, C. K., Coiro, J. L., & Cammack, D. W. (2004). Toward a theory of new literacies emerging from the Internet and other information and communication technologies. *Theoretical Models and Processes of Reading, 5*(1), 1570-1613.

Löfgren, K. (2013, May 19). *Qualitative analysis of interview data: A step-by-step guide* [Video file]. Retrieved from https://www.youtube.com/watch?v=DRL4PF2u9XA

Madden, M. (2012). Privacy management on social media sites. *Pew Internet Report*, 1-20.

Madden, M. (2015a). *Privacy and cybersecurity: Key findings from Pew Research.* Retrieved from http://www.pewresearch.org/key-data-points/privacy/

Madden, M. (2015b). *Why some Americans have not changed their privacy and security behaviors.* Retrieved from http://www.pewresearch.org/fact-tank/2015/04/14/why-some-americans-have-not-changed-their-privacy-and-security-behaviors/

McGregor, S. (2005). Sustainable consumer empowerment through critical consumer education: A typology of consumer education approaches. *International Journal of Consumer Studies*, *29*(5), 437-447.

Melber, A., Hartzog, W., & Selinger, E. (2013, May 22). Fighting Facebook, a campaign for a people's Terms of Service. *The Nation.* Retrieved from http://www.thenation.com/article/fighting-facebook-campaign-peoples-terms-service/

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., & Torres, N. (2012). *Global survey on internet privacy and freedom of expression.* UNESCO.

Milne, G. R., & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing, 19*(2), 238-249.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and

identity. *Journal of Consumer Affairs, 38*(2), 217-232.

Moje, E. B. (2009). Standpoints: A call for new research on new and multi-literacies. *Research in the Teaching of English, 43*(4), 348-362.

Nowak, G. J., & Phelps, J. (1992). Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing, 6*(4), 28-39.

Palmer, D. (2016, May 6). Ransomware is now the biggest cybersecurity threat. *ZDNet.* Retrieved from http://www.zdnet.com/article/ransomware-is-now-the-top-cybersecurity-threat-warns-kaspersky/

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research,* 0093650211418338.

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior, 38*, 296-303.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Phillips, J. T. (2002). Privacy vs. cybersecurity. *Information Management, 36*(3), 46.

Pidaparthy, U. (2011). What you should know about iTunes' 56-page legal terms. *CNN.* Retrieved from http://edition.cnn.com/2011/TECH/web/05/06/itunes.terms/

Plester, B., & Wood, C. (2009). Exploring relationships between traditional and new media literacies: British preteen texters at school. *Journal of Computer-Mediated Communication, 14*(4), 1108-1129.

Reid, R., & Van Niekerk, J. (2014). Towards an Education Campaign for Fostering a Societal, Cyber Security Culture. In *HAISA* (pp. 174-184).

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (Eds.). (2013). *Qualitative research practice: A guide for social science students and researchers.* Sage.

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online, 64*, 88.

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business ethics, 46*(2), 111-126.

Sashi, C. M. (2012). Customer engagement, buyer-seller relationships, and social media. *Management Decision, 50*(2), 253-272.

Schooler, C., Chaffee, S. H., Flora, J. A., & Roser, C. (1998). Health campaign channels tradeoffs

among reach, specificity, and impact. *Human Communication Research, 24*(3), 410-432.

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. *Online Information Review, 28*(3), 224-234.

Smith, O. (2013). Facebook terms and conditions: Why you don't own your online life. *The Telegraph.* Retrieved from http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html

Smithers, R. (2011). Terms and conditions: Not reading the small print can mean big problems. *The Guardian.* Retrieved from http://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems

Solove, D. J. (2002a). Conceptualizing privacy. *California Law Review*, 1087-1155.

Solove, D. J. (2002b). Digital dossiers and the dissipation of fourth amendment privacy. Southern *California Law Review, 75*.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. NyU Press.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 477-564.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review, 44*, 745.

Solove, D.J. (2008). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Sophos (2011). *Sophos Security Threat Report reveals increase in social networking security threats.* Retrieved from https://www.sophos.com/en-us/press-office/press-releases/2011/01/threat-report-2011.aspx

Statista. (2016). *Leading social networks worldwide as of April 2016, ranked by number of active users (in millions).* Retrieved from http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research. Techniques and procedures for developing grounded theory.* London: Sage (pp. 3-25).

Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine*, 95.

Summey, D. C. (2013). *Developing digital literacies: A framework for professional learning.* Thousand Oaks, CA: Corwin Press. doi: http://dx.doi.org/10.4135/9781483387901

Terms of service. (n.d.). In *Encyclopedia PC Magazine*. Retrieved from http://www.pcmag.com/encyclopedia/term/62682/terms-of-service

The New York Times. (2016). Breaking down Apple's iPhone fight with the U.S. government. *The New York Times.* Retrieved from http://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html?_r=0

Thuraisingham, B. (2002). Data mining, national security, privacy and civil liberties. *ACM SIGKDD Explorations Newsletter, 4*(2), 1-5.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In *Reforming European data protection law* (pp. 333-365). Springer Netherlands.

Van Alsenoy, B., Verdoodt, V., Heyman, R., Ausloos, J., Wauters, E., & Acar, G. (2015) From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms (v1.1). *Leuven/Brussel: ICRI-CIR & iMinds-SMIT,* 61.

Van Hamel, A. (2011). The privacy piece: Report on privacy competencies in digital literacy programs in Canada, Britain, Australia, America, and Brazil. University of Ottawa. https://www.priv.gc.ca/information/research-recherche/2011/hamel_201111_e.pdf

Wang, H., Lee, M. K., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63-70.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193-220.

Waters, R. D. (2007). Nonprofit organizations' use of the internet: A content analysis of communication trends on the internet sites of the philanthropy 400. *Nonprofit Management and Leadership, 18*(1), 59-76.

Waters, R. D., Burnett, E., Lamm, A., & Lucas, J. (2009). Engaging stakeholders through social networking: How nonprofit organizations are using Facebook. *Public Relations Review, 35*(2), 102-106.

Weintraub, J., & Kumar, K. (1997). *Public and private in thought and practice: Perspectives on a grand dichotomy*. University of Chicago Press.

Xiao, J. J., O'Neill, B., Prochaska, J. M., Kerbel, C. M., Brennan, P., & Bristow, B. J. (2004). A

consumer education programme based on the transtheoretical model of change. *International Journal of Consumer Studies, 28*(1), 55-65.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389-418.

Zephoria. (2016). *The Top 20 Valuable Facebook Statistics.* Retrieved from https://zephoria.com/top-15-valuable-facebook-statistics/

Appendix A: Content Analysis of Textual Educational Material

A.1. Overview of raw materials collected in selected campaigns

Name	Website link	Sections where materials are retrieved
"Get Cyber Safe"	http://www.getcybersafe.gc.ca/index-en.aspx	- "Cyber Security Risks": All - "Protect Yourself": All
"STOP. THINK. CONNECT."	https://www.stopthinkconnect.org/	- "Tips & Advice": All tip sheets in English - "Campaigns": All sub-sections ("Two Steps Ahead", "Own Your Online Presence", "Keep a Clean Machine")
"Me and My Shadow"	https://myshadow.org/	- "Home": What are digital traces? - "Tracking": All (except the content of privacy policies of six websites) - "Control Your Data": All
"Privacy 101"	https://www.privacyinternational.org/privacy-101?type=2	- "Explainers": All "Privacy 101 Texts"

A.2. Axial codes and open codes of public education campaigns outputted from ATLAS.ti

Code Families

Code Family: 1.1 Growth of cyber security risks
Created: 2016-05-10 23:25:08 (Super)
Codes (6): [Growing cyber security risks] [Harms to other people besides you] [Increasing sophistication of new invaders] [Increasing sophistication of scams and fraud] [Negative impact on businesses or governments] [Severity of risks]
Quotation(s): 29

Code Family: 1.2 Risks caused by malware
Created: 2016-05-10 22:26:44 (Super)
Codes (17): [Attention to viruses and malware] [Change your computer without informing you] [Infectiousness of viruses] [Information flowed to third parties] [Information lost due to malware] [Introduction (101) to Trojan Horses] [Introduction (101) to viruses] [Introduction to spyware and adware] [Introduction to worms] [Malware of malicious individuals] [Malware threatens your mobile device] [Negative impact of malware] [Ransomware (under malware) of malicious individuals] [Risks associated with Trojan horses] [Spyware of malicious individuals] [Tactics used in ransomware] [Viruses developed by malicious individuals]
Quotation(s): 52

Code Family: 1.3 Risks caused by scams or frauds

Created: 2016-05-10 22:36:15 (Super)
Codes (7): [Information on social media helps scammers] [Information solicitation by scammers] [Personal information lost because of scams] [Pharming (or spoofing) of malicious individuals] [Phishing of malicious individuals threatens privacy] [Risks associated with fraudulent calls (under scams and fraud)] [Risks associated with scams or frauds]
Quotation(s): 46

Code Family: 1.4 Risks caused by other malicious individuals
Created: 2016-05-10 23:12:11 (Super)
Codes (20): [Data sniffing of malicious individuals] [Eavesdropping of malicious individuals] [Growing of identity theft] [Hacking by malicious individuals] [Identity theft on social media] [Information lost due to identity theft] [Information lost due to offline risks] [Information lost to strangers] [Information on social media is easily used by malicious individuals] [Information posted online can be misused by malicious individuals] [Information stolen by cyber criminals] [Information tracking by malicious individuals] [Introduction to identity theft] [Malicious individuals use your computer to conduct other harms] [Misuse of information by identity thieves] [Monitor your behaviors by malicious individuals] [Negative impact of identity theft] [Offline risks cause online information threats] [Risks associated with identity theft] [Spam of malicious individuals]
Quotation(s): 58

Code Family: 2.1 Tactic of faking
Created: 2016-06-19 16:37:20 (Super)
Codes (1): [Tactics of mimicing (or posing or faking) by malicious individuals]
Quotation(s): 19

Code Family: 2.2 Use of “benefits”
Created: 2016-06-19 16:38:40 (Super)
Codes (1): [Benefits are used for tricking people]
Quotation(s): 19

Code Family: 2.3 Use of “threats”
Created: 2016-06-19 16:39:20 (Super)
Codes (1): [Threats are used for tricking people]
Quotation(s): 11

Code Family: 2.4 Other tactics
Created: 2016-05-10 21:20:09 (Super)
Codes (6): [Tactics of Phishing] [Tactics of physical tracking ("shoulder surfing") used by malicious inviduals] [Tactics of spoofing] [Tactics used by cyber criminals to get your password]

[Tactics used by malicious individuals] [Tactics used in identity theft]
Quotation(s): 26

Code Family: 3.1 Devices and information protection measures
Created: 2016-05-10 22:04:06 (Super)
Codes (42): [Call for attention to privacy settings] [Danger of jailbreak] [Danger of public wifi] [Good consequences of enhancing protection] [Importance of "https" and padlock] [Importance of backing up] [Importance of deleting and cleaning information] [Importance of encryption] [Importance of firewall] [Importance of locking] [Importance of password] [Importance of two-factor authentication] [Importance of updates] [Information collection in open networks (wifi)] [Information lost due to physical (device) lost] [Information tracking in public wifi and bluetooth] [Introduction to two-factor authentication] [Keeping attention to your devices] [Risks associated with (not having) firewall] [Risks associated with password] [Risks associated with weak security settings] [Risks caused by weak password] [Risks to your information without encryption] [Step-by-step guides on switching on firewalls] [Step-by-step on deleting and cleaning] [Step-by-step on how to update] [Tips on (strong) password] [Tips on adjusting default settings] [Tips on backing up] [Tips on changing password regularly] [Tips on firewall] [Tips on hiding your devices] [Tips on increasing the protection features] [Tips on locking your devices] [Tips on managing device remotely] [Tips on not using automatic login or fill features] [Tips on privacy setting] [Tips on protecting your computer] [Tips on turning to safety-strengthening tools] [Tips on using public wifi safely] [Tips on using security (anti-) softwares] [Tips on using two-factor authentication]
Quotation(s): 243

Code Family: 3.2 Avoidance strategies
Created: 2016-05-10 21:37:05 (Super)
Codes (20): [Danger of links, tweets and posts from unknown source] [Importance of knowing the business or people you are dealing with before further steps] [Importance of limiting information online] [Importance of reviews and comments (about sites)] [Importance of trustworthiness of source] [Information online can be easily stolen] [Information online can lead to offline threats] [Information online used for employment] [Location information can cause privacy risks] [Reputation of services or organizations is important] [Stay-forever nature of online content] [Tips of "avoiding"] [Tips on being careful about friending] [Tips on being careful about of physical tracking ("shoulder surfing")] [Tips on giving out information about others] [Tips on hiding or withholding sensitive or confidential information] [Tips on limiting information to other individuals] [Tips on limiting who can see your information] [Tips on limiting your information posted online] [Tips on withholding certain information]
Quotation(s): 115

Code Family: 3.3 Approach strategies
Created: 2016-05-10 21:30:29 (Super)
Codes (8): [Importance of being anonymous online] [Recommendation on using VPN] [Tips of

"seeking help"] [Tips on seeking help from other organizations] [Tips on seeking help from parents] [Tips on seeking help from service providers] [Tips on turning to governmental agencies for help] [Tips on turning to law]
Quotation(s): 42

Code Family: 3.4 Attention to Terms and Conditions and privacy policy
Created: 2016-05-10 22:17:21 (Super)
Codes (4): [Call for attention to the ToS and privacy policy] [Importance of knowing information use on ToS and privacy policy] [Misuse of information by sites granted by privacy policy] [Privacy policy is confusing]
Quotation(s): 9

A.3. Axial codes and open codes of privacy activism campaigns outputted from ATLAS.ti

Code Families

Code Family: 1.1 Growth of privacy risks
Created: 2016-05-11 15:57:23 (Super)
Codes (9): [Concerns over information collection expressed by people] [Digital traces reveal detailed story (about a person)] [Expanding of data mining] [Growing infromation being collected] [Growing of surveillance] [Growing tools for analyzing data] [New opportunities for data collection] [Severity of monitoring] [Ubiquitousness of information tracking]
Quotation(s): 19

Code Family: 1.2 Privacy risks posed by companies
Created: 2016-05-11 12:23:18 (Super)
Codes (25): [Access to information by companies] [cross-platform tracking by companies] [Dark side of mainstream commercial services] [Dishonesty of companies] [Increasing data given to service providers] [Information aggregation by service providers] [Information analyzed by companies] [Information collected by companies reveals detailed story] [Information collection by companies] [Information storing by service providers] [Information tracking by companies] [Information used for advertising purposes] [Information used for profiling (by companies)] [Location information is analyzed by companies] [Location is tracked by service providers] [Loss of control in front of companies] [Metadata is collected by service providers] [Misuse of data collected by companies] [Monitoring by companies] [Plentiness of information analyzed by companies] [Plentiness of information collected by service providers] [Plentiness of information tracked by companies] [Selling of your information by companies] [Use of tracking technologies by websites] [Weakened privacy by (mainstream) service providers (e.g. Google)]
Quotation(s): 82

Code Family: 1.3 Privacy risks posed by governments
Created: 2016-05-11 12:33:27 (Super)
Codes (19): [Access to information by governments] [Big data used by govenments for investigating crimes] [Communications surveillance by governments] [Dishonesty of governments] [Information analyzed by governments] [Information collection by governments] [Location information used by governments] [Mass surveillance is not legitimate] [Misconduct of governments in surveillance] [Misuse of data collected in surveillance by governments] [Monitoring by governments] [Nagative impact of mass surveillance] [Plentiness of information collected by governments] [Surveillance (equipment) empowers governments but dispowers citizens] [Surveillance equipment is used for counter-terrorism] [Surveillance on global level] [Threats of surveillance equipments used by governments to privacy] [Threats to privacy by mass surveillance] [Threats to privacy of monitoring by governments]
Quotation(s): 48

Code Family: 1.4 Company-government relation and Terms and Conditions
Created: 2016-05-11 13:42:17 (Super)
Codes (6): [Call for attention to ToS and privacy policy] [Company-government information flow] [Dark side of ToS] [Importance of understanding privacy policy] [Information flow granted by ToS] [Uncommunicative feature of privacy policy]
Quotation(s): 14

Code Family: 2.1 Devices and information protection measures
Created: 2016-05-11 12:01:01 (Super)
Codes (27): [Alternative service (email)] [Alternative service (mobile chat apps)] [Alternative service (to Google)] [Benefits of using alternative tools] [Importance of deleting and cleaning] [Importance of encryption] [Importance of https] [Importance of strong passwords] [Importance of updates] [Importance of using open-source tools] [Increased control granted by alternative tools] [Limitations of alternative tools] [Limitations of privacy enhancing tools] [Step-by-step on changing privacy settings] [Step-by-step on deleting wifi history] [Step-by-step on limiting tracking] [Strengthened privacy by alternative tools] [Strengthened privacy by privacy enhancing tools] [Tips on blocking trackers] [Tips on changing default settings] [Tips on deleting browsing history] [Tips on passwords] [Tips on stopping spying or unwanted ads] [Tips on turning to alternative tools] [Tips on turning to privacy enhancing tools] [Tips on using "two-factor" authentication] [Tools that block trackers]
Quotation(s): 129

Code Family: 2.2 Approach strategies
Created: 2016-05-11 13:41:06 (Super)
Codes (6): [Importance of being anonymous online] [Recommendation on using VPN] [Step-by-step on being anonymous "fabricate"] [Tips of "fabricate"] [Tips of "obfuscate"] [Tips on being anonymous]

Quotation(s): 14

Code Family: 2.3 Avoidance strategies
Created: 2016-05-11 12:16:29 (Super)
Codes (5): [Importance of limiting information posted online] [Tips of "refraining" information] [Tips on hiding information for service providers] [Tips on limiting who can see your information] [Tips on limiting your information posted online]
Quotation(s): 11

Code Family: 3.1 Status of privacy protection
Created: 2016-05-11 15:37:38 (Super)
Codes (16): ["Right of access"] [Awareness of data mining by people] [Data protection laws regulate organizations that collect data] [Different privacy nature in different countries] [Insufficiency of limiting governments' power] [Insufficiency of protection by law] [Introduction to data protection laws] [Lack of consent of users] [Little knowledge of information collection] [Little knowledge of the use of data by people] [Opposition to privacy protection by companies and governments] [People are not well informed] [Progress in protecting privacy right] [Reluctance to better protect privacy rights] [Reluctance to stop collecting information by governments and companies] [Status of privacy protection laws]
Quotation(s): 62

Code Family: 3.2 Demand for strengthening regulation and protection
Created: 2016-05-11 13:31:05 (Super)
Codes (17): [Call for controlling data collection] [Call for increased privacy rights] [Call for increased protection of privacy rights] [Call for increased security of information] [Call for limiting information collection] [Call for regulating data use] [Call for regulating practices around big data] [Call for regulating surveillance equipment (through export controls)] [Call for transparency of data use] [Criticism of data collection by companies and governments] [Governments and companies should be limited] [Importance of data protection laws] [Importance of individual human right] [Importance of privacy rights] [Question about compliance of data holders] [Use of technologies for data protection] [Warning governments to comply with law]
Quotation(s): 50

Appendix B: Video Analysis

Overview of videos analyzed

Campaign	Title	Link
"Get Cyber Safe"	Helping your child stay safe online	http://www.getcybersafe.gc.ca/cnt/rsrcs/vds/sty-sf-nlne/index-en.aspx
	Easy Ways to Stay Safe on Public Wi-Fi	http://www.getcybersafe.gc.ca/cnt/rsrcs/vds/scr-pblc-wf-en.aspx
	Easy Ways to Stay Safe on Your Mobile	http://www.getcybersafe.gc.ca/cnt/rsrcs/vds/sty-sf-mbl-en.aspx
	Easy Ways to Stay Safe on Social Networks	http://www.getcybersafe.gc.ca/cnt/rsrcs/vds/scl-ntwrkng-en.aspx
	Secure Websites	http://www.getcybersafe.gc.ca/cnt/rsrcs/vds/scr-wbsts-en.aspx
	Secure Passwords	http://www.getcybersafe.gc.ca/cnt/rsrcs/vds/scr-pssrds-en.aspx
	Phishing Scams	http://www.getcybersafe.gc.ca/cnt/rsrcs/vds/phshng-en.aspx
"STOP. THINK. CONNECT."	Get Ahead With the Digital Spring Cleaning Checklist	https://www.youtube.com/watch?v=NtemO0uAx4M
	STOP. THINK. CONNECT.: Top Online Privacy Tips	https://www.youtube.com/watch?v=CIcIswUkqiY
	2 Steps Ahead: Protecting Your Digital Life	https://www.youtube.com/watch?v=vC8qbff_U4o
	How to Get Two Steps Ahead on Your LinkedIn Account	https://www.youtube.com/watch?v=SjFQDMV4uAM
	How to Get Two Steps Ahead on Your Tumblr Account	https://www.youtube.com/watch?v=gcW__rMTS88
"Me and My Shadow"	What are digital traces?	https://myshadow.org/
"Privacy 101"	Big Data	https://www.privacyinternational.org/node/572
	Communications Surveillance	https://www.privacyinternational.org/node/569
	Data Protection	https://www.privacyinternational.org/node/570
	Metadata	https://www.privacyinternational.org/node/573
	What is Privacy?	https://www.privacyinternational.org/node/568

Appendix C: Facebook Analysis

C.1. Coding system adjusted from Waters et al. (2009)

Relationship cultivation strategies:

Disclosure

Description: Description of or general introduction to the campaign or organization concerned

History: Information about campaign or organizational history

Mission statement: Stating missions in Facebook page info

URL: Link to the website of the campaign or organization concerned

Logo: Whether logo appears in profile picture or cover photo

Administrators listed: A listing of the administrators of the profile

Information dissemination

News links: Links to news items

Photo posted: Posting photos on the page

Video files: Posting videos on the page

Audio files: Posting audios on the page

Posted announcements: Posting announcements or notes on the page (usually placed on the left side)

Discussion wall: Whether the discussion wall function is enabled

Press releases: Providing links to press releases in posts

Campaign summaries: Summaries of campaign(s) developed by the organization

Involvement

E-mail to organization: Whether email is provided as contact information

Phone number: Whether phone number is provided as contact information

Message board used: Enabling the message board function (bottom right corner of cover photo) to make it possible for audiences to message the organization or campaign on Facebook

Calendar of events: Having the events section on the page

Call for actions: Asking audiences to take actions and participate in certain activities held by the organization or campaign

Store: Presence of an e-commerce store

C.2. Overview of Facebook data (profiles and posts)

"Get Cyber Safe"

Facebook link: https://www.facebook.com/GetCyberSafe/timeline

Facebook profile (screenshot taken on May 14, 2016):

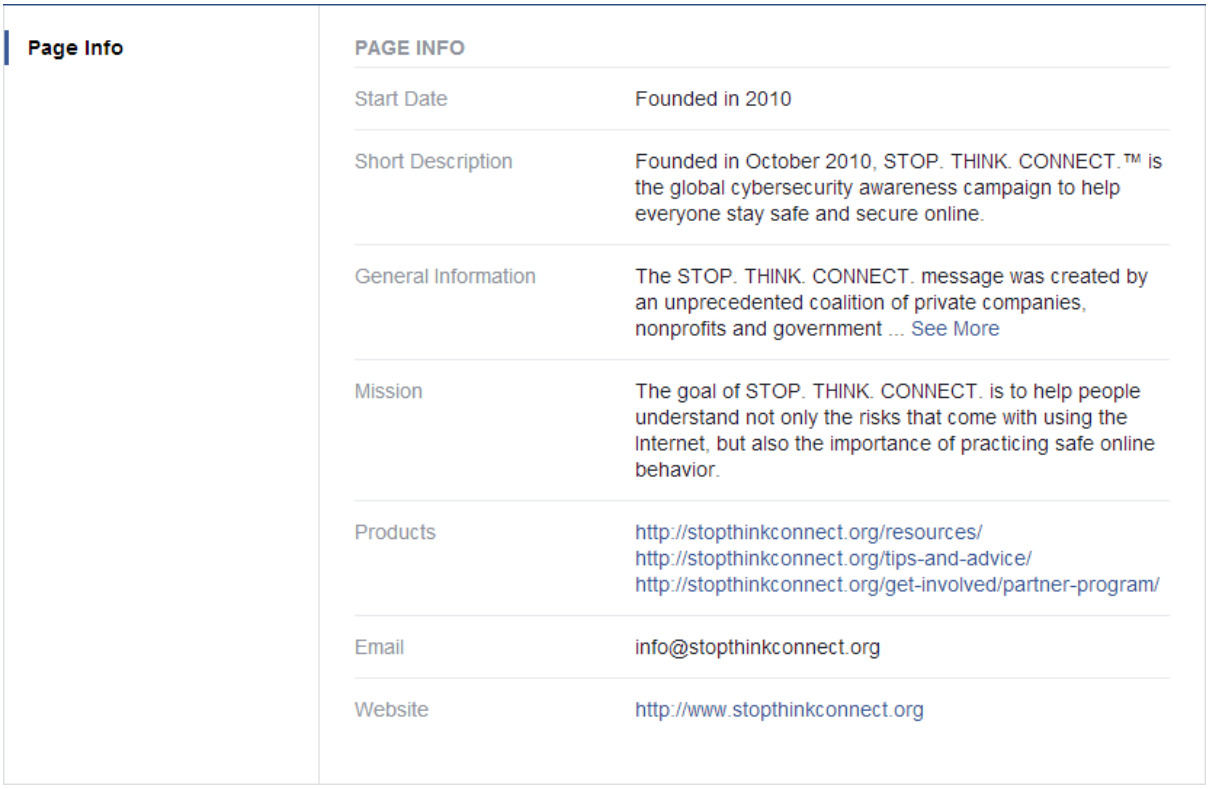
Facebook posts: 20 latest posts as of May 13, 2016 (excluding non-English posts and posts about changing cover photos); see Table 7 for types of content communicated in the posts and their

frequencies

“STOP. THINK. CONNECT.”

Facebook link: https://www.facebook.com/STOPTHINKCONNECT/

Facebook profile (screenshot taken on May 14, 2016):

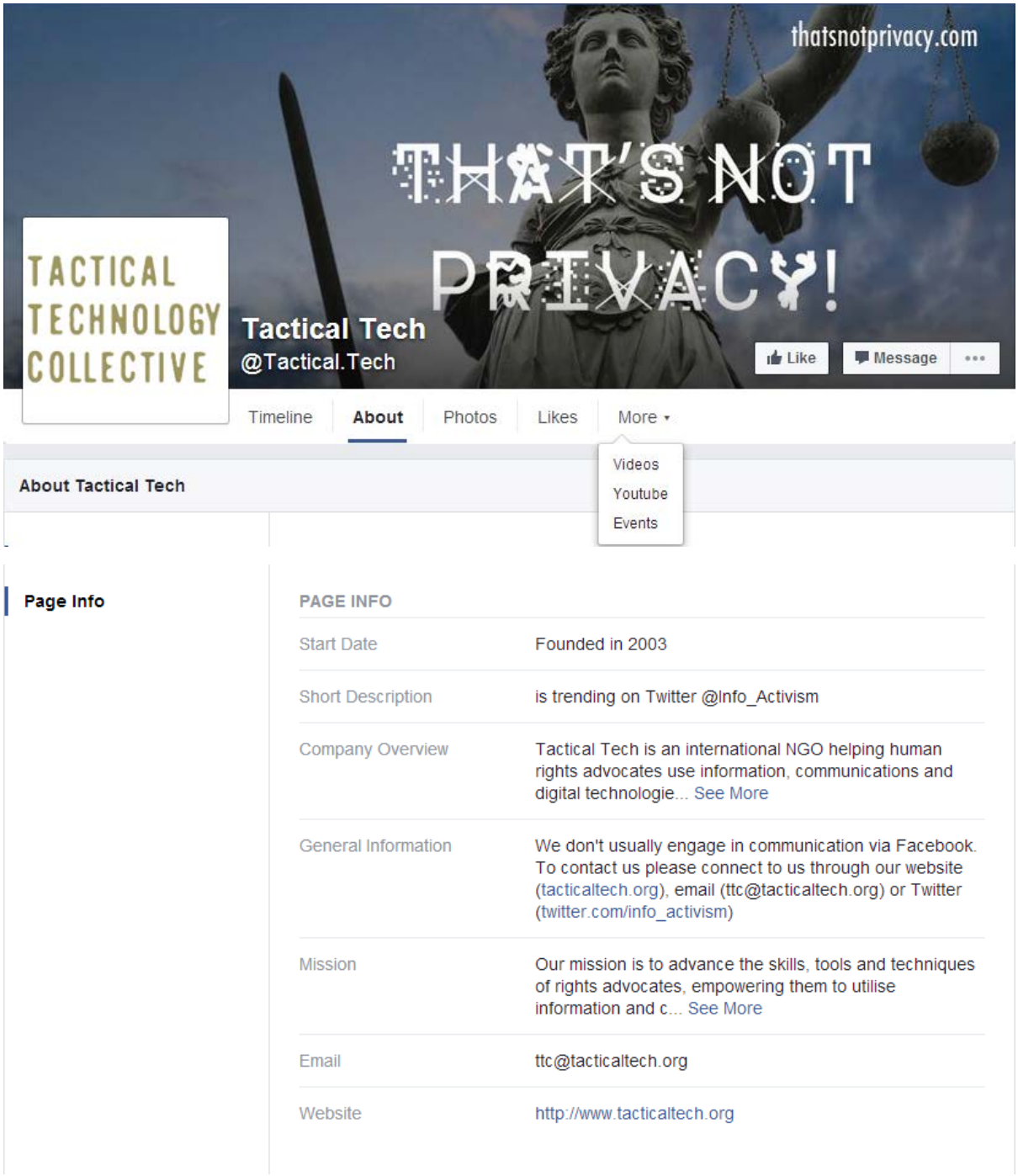


Facebook posts: 20 latest posts as of May 13, 2016 (excluding non-English posts and posts about changing cover photos); see Table 7 for types of content communicated in the posts and their frequencies

Tactical Tech, "Me and My Shadow"

Facebook link: https://www.facebook.com/Tactical.Tech/timeline

Facebook profile (screenshot taken on May 14, 2016):

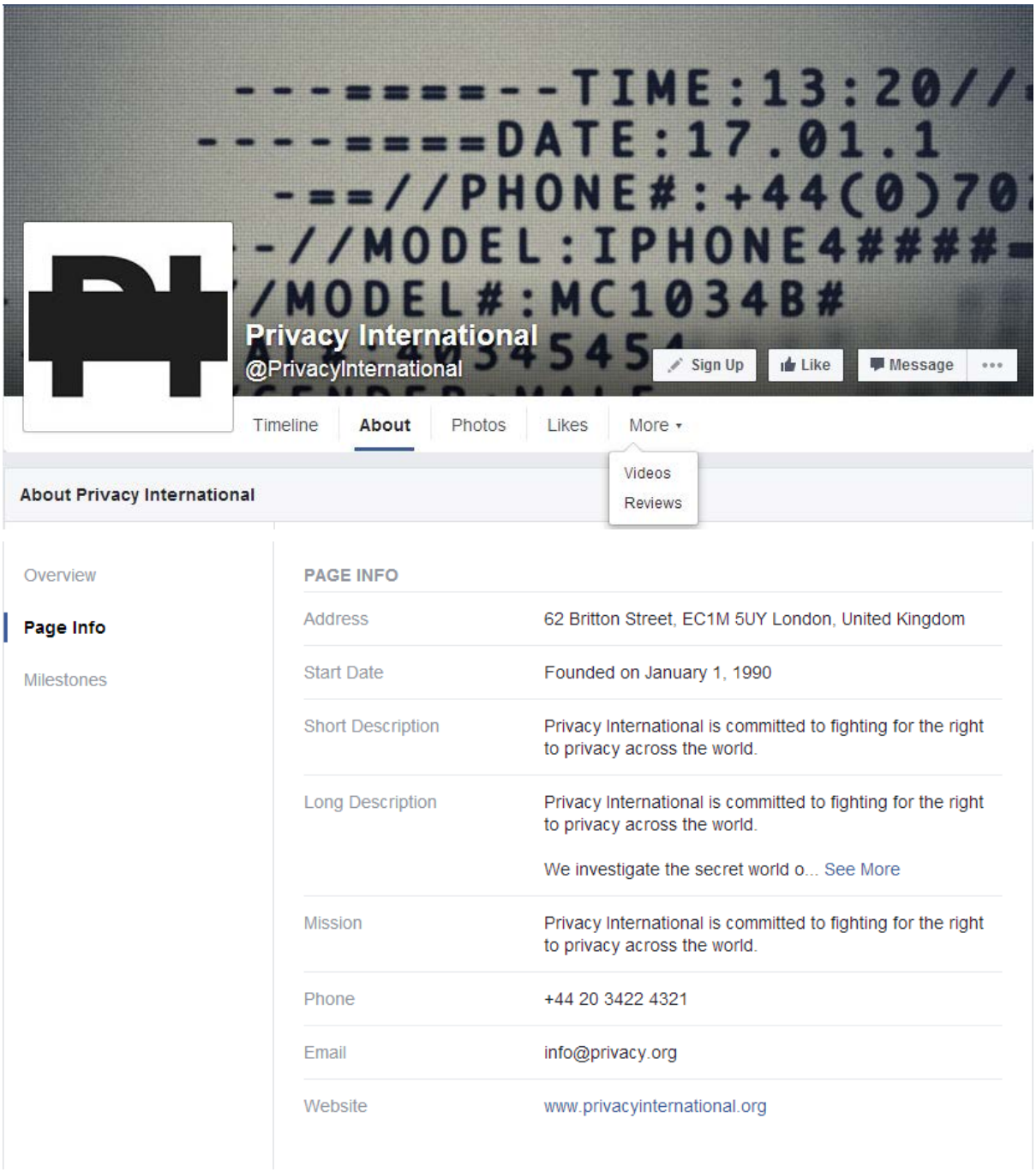


Facebook posts: 20 latest posts as of May 13, 2016 (excluding non-English posts and posts about changing cover photos); see Table 7 for types of content communicated in the posts and their frequencies

Privacy International, "Privacy 101"

Facebook link: https://www.facebook.com/PrivacyInternational/timeline

Facebook profile (screenshot taken on May 14, 2016):



Facebook posts: 20 latest posts as of May 13, 2016 (excluding non-English posts and posts about changing cover photos); see Table 7 for types of content communicated in the posts and their frequencies